CSU, Chico
Information Resources

Information Security
Laws & Regulations
March 2019
March 2019

Campus Community:

On behalf of the Office of Information Resources, please find enclosed the following policies, procedures, standards, and best practice guidelines that guide information technology security practices.

The organization is guided by Chico’s Strategic Plan, CSU, Chico’s Academic Plan, CSU’s ICSUAM section 8000, audits by various external agencies, and routine audits by CSU’s Audit and Advisory Services based on IT best practices. Please review the enclosed information.

- Information Security Laws and Regulations
- CSU ICSUAM 8000 Standards
- State of California Technology Standards
- NIST – Security Framework
- Gartner – Best Practices
- CSU Accessibility Guidelines
- CSU, Chico Information Security Plan
- CSU, Chico Incident Management Plan
- CSU, Chico Security Policies & Standards

Thank you.

[Signature]

Michael Schilling
Vice Provost, Information Resources
Chief Information Technology Officer and CISO
California State University, Chico
Office (530) 898-6212
Voice mail (530) 898-6209
Information Security Laws & Regulations

Follow the links below to learn more about how federal and state laws impact information security and the use of computers.

Breach Notification Laws

Notification of Disclosure of Private Data

- SB 1386 Personal Information Privacy [http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200120020S1386]

California General Security Standard for Businesses

- CA AB 1950 [http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200920100S20]

California OPP Recommended Practices on Notification of Security Breach

- SB 20 Personal Information privacy [http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200920100S20]

Security Breach Notice

- CV 1798.29 [http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CV&sectionNum=1798.29&searchStr=1798.82]

Data Destruction

- California Civil Code sections 1798.80 - 1798.81 and 1798.84 [http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CV&division=3&title=1.81&part=4&chapter=4&articles]

Healthcare Privacy

Health Insurance Portability and Accountability Act (HIPAA)


Public health

- AB 211 [http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200720060AB211]

• Civil, criminal, and monetary penalties for browsing, selling, or unlawfully accepting Healthcare and Psychiatric records. This is a modification to Civil Code 56. January 2009.

Health Information Technology for Economic and Clinical Health (HITECH) Act
• HITECH [PDF](http://www.hhs.gov/sites/default/files/ocr/privacy/hipaasecurity/hitechact.pdf)
  • Provides penalties for healthcare information breaches for HIPAA covered entities. Physicians will be eligible for $40,000 to $65,000 for showing that they are meaningfully using health information technology such as through reporting of quality measures.

California Constitution Declaration of Rights
• Article 1, section 10[PDF](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CON&sectionNum=SECTION%2010&art=11)
  • The state Constitution gives each citizen an "inalienable right" to pursue and obtain "privacy."

Computer Misuse and Abuse: Criminal Sanctions
• Penal Code section 502[PDF](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEL&sectionNum=502)
  • In general, this section makes it a crime to knowingly access and, without permission, use, misuse, abuse, damage, contaminate, disrupt or destroy a computer, computer system, computer network, computer service, computer data or computer program. Depending on the particular violation, this section can support a variety of fines as well as remedies recoverable in civil actions.

PCI DSS

The Payment Card Industry Data Security Standard
• PCI DSS[PDF](https://www.pcisecuritystandards.org/policy-maintaining-payment-security)
  • The PCI Data Security Standards help protect the safety of that data. They set the operational and technical requirements for organizations and processing or receiving payment transactions, and for software developers and manufacturers of applications used in those transactions.

Credit Card or Check Payment
• Civil Code sections 1725 & 1747.08[PDF](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CMV&sectionNum=1725&1747.08)
  • Any person accepting a check in payment for most goods or services at retail is prohibited from recording a purchaser's credit card number or requiring that a credit card be shown as a condition of accepting the check (Section 1725[PDF](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CMV&sectionNum=1725)). Any person accepting a credit card in payment for most goods or services is prohibited from writing the cardholder's personal information on forms associated with the transaction (Section 1747.08[PDF](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CMV&sectionNum=1747.08)).

Credit/Debit Card Number Truncation
• California Civil Code section 1747.09[PDF](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CMV&sectionNum=1747.09)
  • No more than the last five digits of a credit card or debit card number may be printed on the customer copy of electronically printed receipts.

Credit Card "Skimmers"
• Penal Code section 502.6[PDF](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEL&sectionNum=502.6)
  • The knowing and willful possession or use, with the intent to defraud, of a device designed to scan or re-encode information from or to the magnetic strip of a payment card (a "skimmer") is punishable as a misdemeanor. The devices owned by the defendant and possessed or used in violation may be destroyed and various other computer equipment used to store illegally obtained data may be seized.

Eavesdropping, Spying, Unauthorized Pictures

Eavesdropping or Skimming RFID
• Civil Code section 1758.79 and following[PDF](http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CMV&division=3&title=17.81&part=4&chapter=art1&article=)
  • This law makes it a misdemeanor to intentionally remotely read or attempt to read another person's identification document that uses radio frequency identification (RFID), without the person's knowledge or consent. It also makes it a misdemeanor to reveal the operational system keys used in a contactless identification document. Both crimes are punishable by a jail term of up to one year and/or a fine of up to $1,500.

Electronic Eavesdropping
• Penal Code sections 630-638[PDF](http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEL&division=15&part=1&chapter=15&article=)
  • Among other things, this law prohibits, with exceptions, electronic eavesdropping on or recording of private communications by telephone, radio, cellular radio telephone, cable or any other device or in any other manner.

Electronic Eavesdropping by State Law Enforcement Officials
• Penal Code sections 629.50-629.84[PDF](http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEL&division=15&part=1&chapter=15&article=)

With the approval of a Superior Court Judge, specified law enforcement officials can intercept specifically described wire, electronic pager, or electronic cellular telephone communications. The law prescribes a procedure that requires officials to present to a Superior Court Judge requests for authority to record, catalogue, maintain and report about recordings of all communications intercepted (except legally privileged communications). The law also requires authorities to notify the parties to such intercepted communications about the facts of the wiretapping activities, no later than 90 days after the termination of the activities or after the denial of an application seeking wiretapping authority. This law will expire on January 1, 2012.

Telecommunications Customer Privacy

- Public Utilities Code sections 2891-2894.10 [http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PU&division=1&title=8&part=2&chapter=10&article=3]
  - This law bars telecommunications companies from disclosing the calling patterns, personal financial information or other specified personal information of residential subscribers without first getting written consent of the subscriber. There are some exceptions, including disclosure for the purpose of debt collection, in response to a 911 call, and as required by legal process. It also requires, among other things, that telephone companies must give annual notice to subscribers that calling an 800 or 900 number may result in the disclosure of the subscriber's telephone number to the called party.

Telephone Record "Pretexting"

- Penal Code section 638 [http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=638]
  - This law prohibits the purchase or sale of any telephone calling pattern record or list without the written consent of the subscriber.

Wireless Network Security

- Business and Professions Code sections 22948.5-22948.7 [http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BP&division=8&title=2&part=3&chapter=34&article=1]
  - This law requires devices that include an integrated and enabled wireless access point that are manufactured on or after October 1, 2007, to include a warning that advises consumers about how to protect their personal information and mitigate unauthorized use of their Internet access, and provide other specified protection measures.

Physical & Constructive Invasions of Privacy

- Civil Code section 1708.4 [http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&division=5&title=3&part=3&chapter=18&article=1]
  - This law defines physical invasion of privacy in terms of trespassing in order to capture an image, sound recording or other impression in certain circumstances. It also defines constructive invasion of privacy as attempting to capture such an impression under circumstances in which the plaintiff had a reasonable expectation of privacy.

General Laws

California Constitution

- Article 1, section 1 [http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS&sectionNum=SECTION%201_article=1]
  - The state Constitution gives each citizen an "inalienable right" to pursue and obtain "privacy."

Computer Misuse and Abuse: Criminal Sanctions

  - In general, this section makes it a crime to knowingly access and, without permission, use, misuse, abuse, damage, contaminate, disrupt or destroy a computer, computer system, computer network, computer service, computer data or computer program. Depending on the particular violation, this section can support a variety of fines and imprisonment in criminal actions as well as remedies recoverable in civil actions.

The Identity Theft and Assumption Deterrence Act of 1998

  - This law makes identity theft a federal crime.

Locking Mail Boxes in Residential Hotels

  - Effective July 1, 2008, all residential hotels must provide each residential unit with a locking mail receptacle, acceptable for mail delivery by the U.S. Postal Service. Failure to comply is a basis for considering a residential unit un-tenantable. The law also authorizes cities and counties to make and enforce ordinances that provide greater protections and penalties.

Public Records Act

  - This law applies to state and local government. It gives members of the public a right to obtain certain described kinds of documents that are not protected from disclosure by the Constitution and other laws. This law also provides some specific privacy protections.

https://www.csuchico.edu/isec/policies/privacy.htm

4/4/2019
Public Record Exemption for Sex Offense Victims
  - These laws prohibit the disclosure of the names and addresses of victims of specific sex-related crimes in documents provided in response to requests for records, including responses provided under the California Public Records Act.

Employment of Offenders
  - Prison and county jail inmates may not have jobs that give them access to personal information. The same prohibitions apply to offenders performing community service in lieu of a fine or custody.

Family Educations Rights and Privacy Act
  - FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Larceny
  - The complete text of the Penal Code of the State of California, Sections 502 and 502.01, which details the scope of computer crime and its penalties. It describes the protection afforded to individuals, businesses, and governmental agencies against tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.

Wayne Shredding Bill
- State Civil Code 1798.80-89 [http://www.leginfo.ca.gov/cgi-bin/displayCode?section=cy&group=0100-0200&file=1798.80-1798.84].
  - Requires that sensitive information be unreadable before disposing of either electronic or paper documents.

Security of Personal Information
- Civil Code section 1798.81.5 [http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CV&division=3&title=1.81&part=4&chapter=&article=].
  - This law requires specified businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus SSN, driver's license/state ID, financial account number) and to contractually require third parties to do the same. It does not apply to businesses that are subject to certain other information security laws.

The Digital Millennium Copyright Act (DMCA)
- Public Law 105-304 [https://www.copyright.gov/legislation/pl105-304.pdf].
  - Signed into law on October 28, 1998, amended the copyright law to provide limitations for service provider liability relating to material online. CSU, Chico complies with the provision of the Digital Millennium Copyright Act and encourages the university community to respect copyright laws.

Information Resources
Meriam Library, Room 338
www.csuchico.edu/ires
Support Our College
Contact Us

More in our division
- Computing & Communication Services [https://www.csuchico.edu/ccsv]
- Creative Media & Technology [https://www.csuchico.edu/cmt]
- Enterprise Applications & Data Services [https://www.csuchico.edu/eads]
- Information Security [https://www.csuchico.edu/isc]
- IRES Administrative Service [https://www.csuchico.edu/ires]
- IT Support Services [https://www.csuchico.edu/its]
- Institutional Research [https://www.csuchico.edu/ir]
CSU Information Security Policy Obligations

100 Introduction
The Board of Trustees of the California State University (CSU) is responsible for protecting the confidentiality, integrity and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which the CSU must protect from unauthorized access.
- Integrity and availability of information stored on or processed by CSU information systems.
- Compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection.

The CSU Information Security Policy and Standards are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the CSU’s core mission and campus academic and administrative goals.

200 Scope
The CSU Information Security policy shall apply to the following:

- All campuses.
- Central and departmentally-managed campus information assets.
- All users employed by campuses or any other person with access to campus information assets.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.
Auxiliaries

Auxiliaries, external businesses and organizations that use campus information assets must operate those assets in conformity with the CSU Information Security Policy.

The CSU retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CSU. The CSU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.
CSU

ICSUAM
Section 8000
Information Security
**Table of Contents**

<table>
<thead>
<tr>
<th>Section Code</th>
<th>Section Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8000.00</td>
<td>Introduction and Scope</td>
<td>3</td>
</tr>
<tr>
<td>8005.00</td>
<td>Policy Management</td>
<td>4</td>
</tr>
<tr>
<td>8010.00</td>
<td>Establishing an Information Security Program</td>
<td>5</td>
</tr>
<tr>
<td>8015.00</td>
<td>Organizing Information Security</td>
<td>6</td>
</tr>
<tr>
<td>8020.00</td>
<td>Information Security Risk Management</td>
<td>7</td>
</tr>
<tr>
<td>8025.00</td>
<td>Privacy of Personal Information</td>
<td>9</td>
</tr>
<tr>
<td>8030.00</td>
<td>Personnel Information Security</td>
<td>11</td>
</tr>
<tr>
<td>8035.00</td>
<td>Information Security Awareness and Training</td>
<td>12</td>
</tr>
<tr>
<td>8040.00</td>
<td>Managing Third Parties</td>
<td>13</td>
</tr>
<tr>
<td>8045.00</td>
<td>Information Technology Security</td>
<td>14</td>
</tr>
<tr>
<td>8050.00</td>
<td>Configuration Management</td>
<td>15</td>
</tr>
<tr>
<td>8055.00</td>
<td>Change Control</td>
<td>16</td>
</tr>
<tr>
<td>8060.00</td>
<td>Access Control</td>
<td>17</td>
</tr>
<tr>
<td>8065.00</td>
<td>Information Asset Management</td>
<td>18</td>
</tr>
<tr>
<td>8070.00</td>
<td>Information Systems Acquisition, Development and Maintenance</td>
<td>19</td>
</tr>
<tr>
<td>8075.00</td>
<td>Information Security Incident Management</td>
<td>20</td>
</tr>
<tr>
<td>8080.00</td>
<td>Physical Security</td>
<td>21</td>
</tr>
<tr>
<td>8085.00</td>
<td>Business Continuity and Disaster Recovery</td>
<td>22</td>
</tr>
<tr>
<td>8090.00</td>
<td>Compliance</td>
<td>23</td>
</tr>
<tr>
<td>8095.00</td>
<td>Policy Enforcement</td>
<td>24</td>
</tr>
<tr>
<td>8100.00</td>
<td>Electronic and Digital Signatures</td>
<td>25</td>
</tr>
<tr>
<td>8105.00</td>
<td>Responsible Use Policy</td>
<td>26</td>
</tr>
</tbody>
</table>

**Glossary**
8000.00  |  Introduction and Scope

Effective Date: 4/19/2010  |  Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction for managing and protecting the confidentiality, integrity and availability of CSU information assets. In addition, the policy defines the organizational scope of the CSU information Security Policy.

POLICY STATEMENT

100 Introduction
The Board of Trustees of the California State University (CSU) is responsible for protecting the confidentiality, integrity and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which the CSU must protect from unauthorized access.
- Integrity and availability of information stored on or processed by CSU information systems.
- Compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection.

The CSU Information Security Policy and Standards are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the CSU’s core mission and campus academic and administrative goals.

200 Scope
The CSU Information Security policy shall apply to the following:

- All campuses.
- Central and departmentally-managed campus information assets.
- All users employed by campuses or any other person with access to campus information assets.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

Auxiliaries, external businesses and organizations that use campus information assets must operate those assets in conformity with the CSU Information Security Policy.

The CSU retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CSU. The CSU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.
**8005.00 | Policy Management**

**Effective Date:** 4/19/2010  |  **Revised Date:** 4/19/2010

**POLICY OBJECTIVE**

The CSU Information Security policy defines the CSU Information Security Policy review process.

**POLICY STATEMENT**

The CSU Information Security Management Department shall be responsible for overseeing a documented annual review of this policy and communicating any changes or additions to appropriate CSU stakeholders. The CSU Information Security policy shall be updated as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations.

The policy may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by each campus.

Policies, standards, and implementation procedures referenced in the CSU Information Security policy must be developed by each campus through consultation with campus officials and key stakeholders.
POLICY OBJECTIVE

The CSU Information Security policy defines minimum requirements for CSU Information Security Programs.

POLICY STATEMENT

Each campus President and the Assistant Vice Chancellor for Information Technology Services are responsible for the establishment and implementation of an information security program that contains administrative, technical and physical safeguards designed to protect campus information assets. Each campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The campus information security program reviews must be documented. The campus program must:

- Document roles and responsibilities for the information security program.
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic).
- Develop risk management strategies to identify and mitigate threats and vulnerabilities to level 1 and level 2 information assets as defined in the CSU Data Classification Standard.
- Establish and maintain an information security incident response plan.
- Maintain ongoing security awareness and training programs.
- Comply with applicable laws, regulations, and CSU policies.
POLICY OBJECTIVE

The CSU Information Security policy provides guidance for defining the governance structure of CSU Information Security Programs.

POLICY STATEMENT

Each campus must develop, implement, and document the organizational structure that supports the campus' information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program. The governance structure must be reviewed at least annually. Review of the campus organizational structure that support the information security program must be documented.

Each President (or President-designee) and the Assistant Vice Chancellor for Information Technology Services (or the Vice Chancellor's designee) must appoint a campus information security officer (ISO). The Assistant Vice Chancellor for Information Technology Services (or the designee of the Chancellor) is responsible for the systemwide Information Security Management program and may organize the responsibilities as appropriate.
8015.S000 Information Security Roles and Responsibilities

Implements: CSU Policy #8015
Policy Reference: 8015.00 Organizing Information Security

Introduction
The CSU Information Security policy provides guidance for defining the governance structure of CSU Information Security Programs.

a) Each campus must develop, implement, and document the organizational structure that supports the campus' information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program. The governance structure must be reviewed at least annually.

b) Each President (or President-designee) and the Assistant Vice Chancellor for Information Technology Services (or the Vice Chancellor's designee) must appoint a campus information security officer (ISO). The Assistant Vice Chancellor for Information Technology Services (or the designee of the Chancellor) is responsible for the systemwide Information Security Management program and may organize the responsibilities as appropriate.

1.0 Campus President

1.1 Each CSU campus President must establish an information security program which is compliant and consistent with the CSU information security policy and standards. The details of each campus program are left to the President (or designee) to determine, with the exception of items identified in the CSU information security policy and standards; these items are meant to provide some degree of consistency of approach and application.

1.2 The President (or President's designee) must identify the specific duties and responsibilities for the ISO, which, at a minimum, include those items identified below. While the role of the Information Security Officer (ISO) may be an additional duty, the President must ensure the appointee has sufficient time to carry out the assigned duties and responsibilities.

1.3 The President may assign additional roles and responsibilities appropriate to the campus.

1.4 Each President must review information security risks at least annually.

2.0 Campus Chief Information Officer (CIO)

In addition to other duties as defined within the CSU, each campus CIO must:

a) Work with the campus ISO to develop procedures and processes which implement the CSU information security policy and standards as directed by the campus President.

b) Work with the campus ISO to evaluate the risk introduced by any changes to campus operations and systems.

c) Consult with the ISO regarding campus operations and systems to address security.

3.0 Campus Information Security Officer (ISO)

The ISO must:
a) Coordinate the campus information security program on behalf of the President.
b) Advise the President and his/her cabinet on all information security matters.
c) Work closely with campus administrators and executive officers on information security matters.
d) Oversee campus information security risk assessment activities.
e) Inform the President (or President-designee) of significant information security risks as they are identified.
f) Oversee the campus information security incident response program in coordination with appropriate campus personnel.
g) Oversee the campus information security awareness and training program.
h) Provide input to the campus budget process regarding prioritization and required resources for information security risk mitigation activities and inputs regarding information security risks of proposed projects.
i) Respond to information security related requests during an audit.
j) Serve as the campus representative on the CSU Information Security Advisory Committee.
k) Avoid conflicts of interest by not having direct responsibility for information processing or technology operations for campus programs that employ protected information.

4.0 Campus Managers
Technical and program (e.g., human resources, registrars, privacy officers, etc.,) managers are responsible for:

a) Ensuring that information assets under their control are managed in compliance with CSU and campus information security policies and standards.
b) Ensuring that staff and other users of information assets under their control are informed of and comply with CSU and campus information security policies and standards.

5.0 Campus Data Owners

5.1 The data authority/owner must:

a) Classify each information asset for which he or she has ownership responsibility in accordance with CSU and campus policies/standards, or legal, regulatory, or contractual requirements.
b) Work with the ISO to define controls for limiting access to and preserving the confidentiality, integrity and availability of information assets that have been classified as requiring such controls.
c) Authorize access to the information asset in accordance with the classification of the asset and the need for access to the information.
d) Ensure that those with access to the information asset understand their responsibilities for collecting, using, and disposing of the asset in accordance with CSU and campus policies/standards, or legal, regulatory, or contractual requirements.
e) Work with the ISO to monitor and ensure compliance with CSU/campus security policies and procedures affecting the information asset.
f) Work with the ISO to identify an acceptable level of risk for the information asset.
g) Work with the ISO, data user, data custodian/steward, and/or other authorized individuals during the investigation and mitigation of information security incidents/breaches affecting the information asset.

5.2 The ownership responsibilities must be performed throughout the life cycle of the information asset, until its proper disposal. Individuals that have been designated owners of information assets must coordinate these responsibilities with the campus ISO.
6.0 Campus Data Custodian/Steward

The responsibilities of a custodian of an information asset consist of:

a) Complying with applicable law and administrative policy.
b) Complying with any additional security policies and procedures established by the owner of the information asset and the campus ISO.
c) Advising the owner of the information asset and the campus ISO of vulnerabilities that may present a threat to the information and of specific means of protecting that information.
d) Notifying the owner of the information asset and the campus ISO of any actual or attempted violations of security policies, practices, and procedures.

7.0 Campus Data User

The responsibilities of a data user consist of:

a) Ensuring that he or she does not put any University information asset for which he or she has been given access at risk through his or her own actions.
b) Working with the ISO, data authority, data custodian/steward, and/or other authorized individuals during the investigation and mitigation of information security incidents/breaches affecting the information asset.
c) Performing as appropriate other information security duties as required by other CSU and campus policies/standards, the data owner, or the campus ISO.

8.0 Systemwide Chief Information Security Officer

The Systemwide Chief Information Security Officer must:

a) Provide leadership for the overall CSU Information Security Program
b) Conduct an periodic review and update of the CSU security policy and standards
c) Advise the Chancellor and CSU senior management on matters regarding information security
d) Provide support to information security staff at each campus
e) Develop systemwide information security strategies and metrics
### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>5/20/2011</td>
<td>Macklin</td>
<td>Draft Standard</td>
<td>All</td>
</tr>
<tr>
<td>1.1</td>
<td>6/17/2011</td>
<td>Moske</td>
<td>Format draft.</td>
<td>All</td>
</tr>
<tr>
<td>1.2</td>
<td>11/5/2013</td>
<td>Macklin</td>
<td>Updated § 8 to reflect title change, added 8(e) based on feedback from ITAC. Update other section titles to distinguish between campus and systemwide personnel.</td>
<td>All</td>
</tr>
<tr>
<td>New</td>
<td>11/15/13</td>
<td>Moske</td>
<td>Accept Macklin Edits and publish final</td>
<td>All</td>
</tr>
</tbody>
</table>

### Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click here to enter Review Date</td>
<td>Click here to enter Review Date</td>
<td>Click here to enter Review Date</td>
</tr>
<tr>
<td>3/21/2012</td>
<td>ISAC</td>
<td>Reviewed, approved and recommended for CISO review</td>
</tr>
<tr>
<td>6/25/2013</td>
<td>ITAC</td>
<td>Reviewed and approved</td>
</tr>
<tr>
<td>11/5/2013</td>
<td>CISO</td>
<td>Reviewed and approved</td>
</tr>
</tbody>
</table>
POPCY OBJECTIVE

The CSU Information Security policy provides direction and support for the campus information security risk management program.

POICY STATEMENT

100 Information Security Risk Management
Risk management involves the identification and evaluation of risks to information security assets (risk assessment) and the ongoing collection of information about the risk (risk monitoring). Once a risk has been identified, campuses must develop and implement strategies to reduce the risk to acceptable levels (risk mitigation), share or shift the risk to another party (risk transference), or assume the identified risk (risk acceptance).

Campuses must develop risk management processes that identify, assess, and monitor risks to information assets containing level 1 and level 2 data as defined in the CSU Data Classification Standard. Identified risks to these information assets must be actively managed by data owners and/or appropriate administrators in order to prioritize resources and remediation efforts.

200 Information Security Risk Assessment
Risk assessments are part of an ongoing risk management process. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls.

Campuses must document the scope and frequency of the assessment; risk assessment methodology; result of the risk assessment; and, mitigation strategies designed to address identified risks.

300 Information Security Risk Mitigation
Risk mitigation involves prioritizing, evaluating, and implementing appropriate risk-reducing activities recommended as a result of the risk assessment process. Since the elimination of all risk is impossible, campus leadership must balance the cost and effectiveness of the proposed risk-reducing activities against the risk being addressed.

Campuses must select appropriate mechanisms to safeguard the confidentiality, integrity, and availability of information assets containing protected data. Campus mitigation strategies must be commensurate with risks identified by risk assessments. For those risks where the mitigation strategy involves the use of controls, those controls must ensure that risks are reduced to an acceptable level, taking into account:

- Legal and regulatory requirements and compliance.
- Campus operation and policy requirements and constraints.
- Cost of implementation, maintenance, and operation.

Each campus must develop and maintain a process for documenting and tracking decisions related to risk mitigation activities.

400 Information Security Risk Transference
Whenever possible, a risk may be managed by sharing or completely transferring it to another entity. Campuses may transfer risks if the required actions of the receiving entity are deemed to result in an acceptable outcome should the risk be exploited and damage occurs. Risks associated with potential failure to comply with applicable laws, statutes, or regulations can only be transferred if the results will support compliance.

Each campus must develop and maintain a process for documenting and tracking decisions related to risk transference activities.

500 Information Security Risk Acceptance
Risk acceptance occurs when potential risk-reduction activities cannot be found or those identified are determined not to be cost effective (e.g. the protection measures cost more than the potential loss). In the case where resources for the best mitigation strategy are not available, the risk must be addressed to the extent possible using available resources.
Campuses must develop a process for documenting, reviewing and approving accepted risks. Accepted risks must undergo periodic review and approval by appropriate administrators.

600 Information Security Risk Monitoring
Sometimes, when a risk is identified, there may be insufficient or conflicting information regarding its likelihood of occurrence or potential impact. Campuses must monitor risks of this nature and develop a plan to gather sufficient information to judge whether the risk should be mitigated, transferred, or accepted.

700 Reporting Information Security Risks
The Senior Director of Systemwide Information Security Management must complete a risk assessment of information assets containing level 1 data as defined in the CSU Data Classification Standard at least every two years. The report must include a description of the methodology, the results of the risk assessment, and recommended systemwide mitigation strategies for addressing each identified risk. The report must be certified by the systemwide Information Security Steering Committee and presented to the Chancellor (or Chancellor-designee).
8020.S000 Information Security Risk Management – Exception Standard

Implements: CSU Policy #8020.0

Introduction
A campus may decide to allow exceptions to CSU or campus policies, standards or practices. Campuses must develop criteria for determining the organization with authority to approve an exception (i.e. manager, ISO, CIO, data owner, or combination of persons as appropriate). Exceptions may be granted when the campus decides, after risk assessment, that there are adequate compensating controls. When adequate compensating controls do not exist, the campus must follow its risk management process to ensure that the exception is approved by an appropriate Vice-President or other campus administrator with fiscal responsibility for addressing the result of risk acceptance. When a campus grants an exception or accepts a risk, it must comply with the following minimum standards to identify, monitor and periodically review the exception.

1.0 Exception Process
Each campus must develop a process for documenting, reviewing and approving exceptions.

1.1 The campus exception process must include the following:
   a) Required management approval from the requesting organization’s appropriate administrator.
   b) A description of the nature and types of exceptions which must be reviewed by the campus ISO.
   c) A process and timeline for periodic review of granted exceptions in which periodic reviews must be performed at least every three years.
   d) A record documenting the exception process including:
      a. Contact information for individual and/or organization requesting the exception.
      b. The policy, standard or other requirement to which exception is being requested...
      c. Justification for the proposed exception.
      d. Description of any proposed compensating control or mitigating circumstance.
      e. Information security risk analysis using the campus risk assessment methodology.
      f. Designation (i.e. “high”, “medium”) of risk under the campus’ risk assessment methodology.
      g. Appropriate approvals.
   e) Retention of exception review and approval records for at least 3 years after the exception is withdrawn or expired, or as required by applicable records retention schedule.

2.0 Periodic Review of Granted Exceptions
Exceptions must undergo periodic review and approval by appropriate administrators.
2.1 The exception review process must include:
   a) Periodic review as per the schedule established in §1.1(c).
   b) Confirmation from the requestor of whether or not the exception remains necessary.
   c) Review sufficient to determine if controls remain adequate to mitigate risk.
   d) Update of the exception record to reflect changes and record completion of the review including:
      a. Updated approval from changed management or organization.
      b. Any changes in hardware, software, policy or standard relevant to this exception.

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>6/10/2014</td>
<td>Macklin</td>
<td>First draft – ISAC development team</td>
<td>All</td>
</tr>
<tr>
<td>1.1</td>
<td>2/24/15</td>
<td>Macklin</td>
<td>CISO comments/ISAC development team</td>
<td>1.1, Intro</td>
</tr>
<tr>
<td>1.2</td>
<td>3/1/15</td>
<td>Macklin</td>
<td>CISO comments</td>
<td>1.1, Intro</td>
</tr>
<tr>
<td>1.3</td>
<td>3/1/15</td>
<td>Macklin</td>
<td>CISO comments</td>
<td>1.1(c)</td>
</tr>
</tbody>
</table>

Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/2/15</td>
<td>P&amp;S Committee with CISO</td>
<td>CISO comments reviewed and discussed (3/2/15 – 10am). This version includes those comments. Next steps collaborative review.</td>
</tr>
<tr>
<td>3/2/15</td>
<td>Leslie DeCato</td>
<td>Added Draft Watermark. Submitting to ISAC/ITAC for Review.</td>
</tr>
<tr>
<td>3/3/15</td>
<td>Perry</td>
<td>Reviewed and accepted all (track changes). Submitted to DeCato for ISAC/ITAC Review. Review period will be 3/6/15 to 4/10/15.</td>
</tr>
<tr>
<td>6/4/15</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>

Implements: CSU Policy #8020.0

Introduction
A campus must develop a process for assessing risks to its information assets. These assessments must be based on established severity and likelihood criteria and managed through ongoing evaluation and review activities.

1.0 Risk Assessment Criteria
Each campus must use a risk assessment model based on established criteria (see Appendix A). The campus must not alter the severity or likelihood classifications contained in Appendix A, but the campus may add criteria and/or numeric weighting based on its unique environment or circumstance.

2.0 Formal Risk Assessment Process

2.1 Establish Criteria
Each campus must establish and document two forms of formal risk assessment criteria. These criteria must be adequately communicated to campus departments:

- Criteria for situations in which a formal risk assessment must be performed (i.e. HIPAA, PCI, protected level 1 data, etc.).

- Criteria for situations in which a formal risk assessment may be necessary as determined by the ISO. If a project meets this criteria then the ISO must be notified about the proposed information asset change or acquisition. The ISO will determine whether a formal assessment needs to be performed.

2.2 Identify Formal Risk Assessment Methodology
Working with the procurement, project teams, change management groups and others as appropriate, campuses must establish and maintain a process for identifying information assets on which established criteria is used to determine if a formal risk assessment is required.

2.3 Required Elements of Formal Risk Assessment
Recognizing that risk assessment activities may vary depending on the nature of the risk being assessed, the following elements must be included:

a) Review Frequency
Formal risk assessments must identify a review cycle to ensure that risk management remains appropriate and effective. The length of the review cycle must comply with all applicable laws, policies, standards, and contracts. (For example, the length of the review cycle for PCI and HIPAA risk assessments must not exceed two years.) The review cycle for systems which were identified as “critical” must not exceed three years.
b) Risk Exposure
Each formal risk assessment must use the established risk assessment criteria (See Appendix A) to establish a risk exposure for the identified system, process, asset, etc.

c) Documentation and Retention
Written records of the formal risk assessment and supporting materials must contain sufficient detail to facilitate periodic review and must be retained for a minimum of 3 years.

d) Approval
The campus ISO is responsible for approving the formal information security risk assessment.

3.0 Informal Risk Assessment Process

Informal risk assessments may be used for those systems, assets, processes, etc. not considered critical to the organization and/or which fail to meet the criteria for formal risk assessment. Records of informal risk assessments may be in the form of email or other notes and should contain a statement of the dependencies, premises and facts upon which the opinion is based.

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>11/25/14</td>
<td>Macklin</td>
<td>First draft – ISAC development team</td>
<td>All</td>
</tr>
<tr>
<td>0.3</td>
<td>2/6/14</td>
<td>Macklin</td>
<td>Incorporated team comments</td>
<td>2</td>
</tr>
<tr>
<td>.4</td>
<td>3/10/15</td>
<td>Macklin</td>
<td>Incorporated team comments</td>
<td>2</td>
</tr>
<tr>
<td>.5</td>
<td>4/28/15</td>
<td>Luvisi</td>
<td>Incorporated CISO comments</td>
<td>2.3</td>
</tr>
<tr>
<td>.6</td>
<td>4/29/15</td>
<td>DeCato</td>
<td>Made Cosmetic changes like font type and size</td>
<td>All</td>
</tr>
</tbody>
</table>

Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/13/15</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>

Last Revised: 4/29/2015
Severity Scale (derived from SANS)

**Critical** - May allow full access to or control of the application, system, or communication including all data and functionality.

- The attacker is not limited in access after execution, they may be able to escalate privileges.
- Possible disclosure of 500 or more records containing sensitive or confidential information.
- Allows modification or destruction of all critical/sensitive data.
- Total shutdown of a critical service or services.

**High** - May allow limited access to or control of the application, system, or communication including only certain data and functionality.

- The attacker can access the sensitive data or functionality of a user, either limited to a specific piece of data and/or a specific user.
- An outside attacker can execute arbitrary code at the level of the user.
- Ability for a user to access unauthorized functionality.
- Allows limited modification or destruction of critical/sensitive data, either limited to a specific piece of data and/or a specific user.
- Severe degradation of a critical service or services.
- Exposure of sensitive system or application information that provides implementation details that may be used to craft an exploit.
- Breach may be difficult to detect.

**Moderate** - May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified.

- Weaknesses that can be combined with other vulnerabilities to have a higher impact.
- Disclosure of information that could aid an attacker.
- Any vulnerability that can hinder the detection or investigation of higher impact exploit.
- Fines greater or equal to $10,000 and less than $50,000.

**Low** - May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified.

- Deviation from a recommended practice or emerging standard.
- May be the lack of a security process or procedure to govern or manage security related activities.
- No direct exposure of data.
- Fines less than $10,000.
- Would not contribute to the exposure of confidential information.
- Would not enable alteration of stored records.
- Would not impact the availability of critical campus systems.

**Likelihood Scale**

**Very High** - Exposure is apparent through casual use or with publicly available information, and the weakness is accessible publicly on the Internet.

- Can be exploited by large anonymous population (Any Internet host).
- Vulnerability can be exploited from the general Internet.
- Possible with only publicly available information.
- No specific attack skills are required, such as general user knowledge.

**High** - The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

- Can be exploited by extended campus population (students, guests)
- Can be exploited by anyone that can reach the network, no authentication required.
- Vulnerability can only be exploited from related networks to which the organization does not control access (vendors)
- Simple (easily guessable) authentication may be required for exploit.
- Possible with limited knowledge of target configuration.
- Basic attack skills are needed, such as an automated attack (i.e. there exists a metasploit module, or known attack)

**Moderate** - The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

- Can be exploited by a limited and known population.
- Vulnerability can be exploited through the internal company network or client connection only.
- Simple authentication is required for exploit.
- Vulnerability requires a user to be 'tricked' into taking some action (e.g. a targeted phishing message or a request to go to a website and download a file).
- Possible only with detailed internal information or reasonable guessing.
- Expert technical knowledge is needed such as knowledge of available attack tools.

**Low** - The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede the vulnerability from being exercised.

- Threat source is employee
- Vulnerability can be exploited through the internal campus network only.
- Single strong authentication is required for exploit.
- Possible only with a significant amount of guesswork or internal information.
- Vulnerability can be exploited with local physical access only and resources have physical access controls, but are still accessible to a large number of people.
**Negligible** - The threat-source is part of a small and trusted group or controls prevent exploitation without physical access to the target or significant inside knowledge is necessary, or purely theoretical.

- Small and trusted population.
- Vulnerability can be exploited with local physical access only and resources have strong physical access controls.
- A series of strong authentications or multi-factor authentication are required for exploit.
- Possible only with a significant amount of likely detectable guesswork or tightly controlled internal information.
- Attack is theoretical in nature and no known exploit or potential of exploit is currently proven or expected.

---

**Risk Exposure Mapping**

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Critical</td>
</tr>
<tr>
<td>Very High</td>
<td>Critical</td>
</tr>
<tr>
<td>High</td>
<td>Critical</td>
</tr>
<tr>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>Negligible</td>
<td>Low</td>
</tr>
</tbody>
</table>
8025.00 | Privacy of Personal Information

Effective Date: 4/19/2010  | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for protecting the privacy of personal information managed by the CSU and guidance for collecting and accessing personal information.

POLICY STATEMENT

100 Privacy of Personal Information
All users of campus information systems or network resources are advised to consider the open nature of information disseminated electronically and must not assume any degree of privacy or restricted access to information they create or store on campus systems. The CSU is a public university and information stored on campus information systems may be subject to disclosure under state law. No campus information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, the CSU acknowledges its obligation to respect and protect private information about individuals stored on campus information systems and network resources.

200 Collection of Personal Information
To comply with state and federal laws and regulations, campuses may not collect personally identifiable information unless the need for it has been clearly established.

Where such information is collected:

- The campus will use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.
- The campus shall store personally identifiable information only when it is appropriate and relevant to the purpose for which it has been collected.

300 Access to Personal Information
Except as noted elsewhere in CSU policy, information about individuals stored on campus information systems may only be accessed by:

- The individual to whom the stored information applies or his/her designated representative(s).
- Authorized CSU employees with a valid CSU-related business need to access, modify, or disclose that information.
- Appropriate legal authorities.

When appropriate, authorized CSU personnel following established campus procedures may access, modify, and/or disclose information about individuals stored on campus information systems or a user's activities on campus information systems or network resources without consent from the individual. For example, CSU may take such actions for any of the following reasons:

- To comply with applicable laws or regulations.
- To comply with or enforce applicable CSU policy.
- To ensure the confidentiality, integrity or availability of campus information.
- To respond to valid legal requests or demands for access to campus information.

If CSU personnel accesses, modifies, and/or discloses information about an individual and/or his/her activities on campus information systems or network resources, staff will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by CSU policy or applicable laws.

Campuses are advised to consult the CSU Records Access Manual to determine which records must be made available for public inspection under the California Public Records Act.

400 Access to Electronic Data Containing Personal Information
Individuals who access or store protected data must use due diligence to prevent unauthorized access and disclosure of such assets.

Browsing, altering, or accessing electronic messages or stored files in another user's account, computer, or
storage device is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for CSU business reasons. This prohibition does not affect:

- Authorized access to shared files and/or resources based on assigned roles and responsibilities.
- Authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individual’s job duties.
- Access to implicitly publicly accessible resources such as University websites.
- Campus response to subpoenas or other court orders.
- Campus response to a request pursuant to public record disclosure laws.
8030.00 | Personnel Information Security

Effective Date: 4/19/2010  |  Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing personnel information security, defines pre-employment requirements, and provides guidance for managing separations or changes in employment status.

POLICY STATEMENT

100 Personnel Information Security
All users are expected to employ security practices appropriate to their responsibilities and roles. Users who access level 1 or level 2 data as defined in the CSU Data Classification Standard must sign an approved system-wide confidentiality (non-disclosure) agreement.

200 Employment Requirements
Campuses must develop procedures to conduct background checks on positions involving access to level 1 information assets as defined in the CSU Data Classification Standard.

300 Separation or Change of Employment
Campuses must implement procedures to revoke access to information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy and by the data owner. Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

Procedures must be implemented to ensure proper disposition of information assets upon termination. Electronic and paper files must be promptly reviewed by an appropriate manager to determine who will become the data steward of such files and identify appropriate methods to be used for handling the files. If the separating employee is holding resources subject to a litigation hold, the campus must ensure preservation of relevant information until the litigation hold has been revoked, at which point the resource is subject to the normal record retention schedule.

Campuses must verify that items granting physical access such as keys and access cards are collected from the exiting employee. Any access list that grants the exiting employee physical access to a limited-access area on the campus must be updated appropriately to reflect the change in employment status.

Each campus must establish procedures to allow for separated employees to obtain such incidental personal electronic information as appropriate.

Information system privileges retained after separation from the campus must be documented and authorized by an appropriate campus official.
8030.S000 Personnel Security

Implements: CSU Policy #8030.000
Policy Reference: 8030.00 Personnel Information Security

6.0 Personnel Security

6.1 Employment Separations and Position Change

a) Based on established campus procedures, authorized CSU managers must promptly notify the appropriate department(s) responsible for granting and revoking access privileges regarding all employee separations and job changes.

b) If an employee is separating from the University, the employee's access privileges (logical and physical) must be terminated by the employee's last day of employment, unless otherwise approved through proper campus procedures. By the last day of work, an employee must return all campus- and/or CSU-supplied access devices to his or her manager. If an employee has used cryptography on data belonging to the CSU, he or she must provide the cryptographic keys to the manager by the last day of employment.

c) It is the responsibility of the employee's manager to identify and define the access privileges needed by the employee to perform the job. The campus must implement a process to ensure that managers evaluate and approve such access privileges within a reasonable period of time after a change in position, job responsibilities, or management reporting structure.

d) Campuses must implement a process to confirm that logical and physical access privileges have been appropriately revoked or changed after separation or position change.

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/10/2011</td>
<td>T. Macklin</td>
<td>Corrected policy reference URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/21/2012</td>
<td>T. Macklin</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/26/12</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Review</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>

Last Revised: 07/16/13
8035.00 | Information Security Awareness and Training

Effective Date: 4/19/2010  | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for developing and managing information security awareness and training programs.

POLICY STATEMENT

100 Information Security Awareness and Training

Each campus must implement a program for providing appropriate information security awareness and training to employees appropriate to their access to campus information assets. The campus information security awareness program must promote campus strategies for protecting information assets containing protected data.

All employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, information security training must be provided to individuals whose job functions require specialized skill or knowledge in information security.

200 Information Security Awareness

The security awareness program must provide an overview of campus information security policies, and help individuals recognize and appropriately respond to threats to campus information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard.

The program must promote awareness of:

- CSU and campus information security policies, standards, procedures, and guidelines.
- Potential threats against campus protected data and information assets.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information assets.
- CSU and campus notification procedures in the event protected data is compromised.

After receiving initial security awareness training, employees must receive regular updates in policies, standards, procedures and guidelines. The updates should be relevant to the employee’s job function, duties and responsibilities.

300 Information Security Training

When necessary, the campus information security program must provide or coordinate training for individuals whose job functions require special knowledge of security threats, vulnerabilities, and safeguards. This training must focus on expanding knowledge, skills, and abilities for individuals who are assigned information security responsibilities.
8035.S000 Security Awareness and Training

Implements: CSU Policy #8035
Policy Reference: 8035.00 Information Security Awareness and Training

Introduction

Information Security Awareness and Training programs are a key element of the CSU Information Security Program. Establishment of a campus training and awareness program will ensure that people understand their information security responsibilities and help to reduce the number and impact of information security incidents.

1.0 Campus Security Awareness and Training Program

1.1 Each campus ISO will be responsible for overseeing development and coordination of the campus information security awareness and training program. At a minimum, each campus program must include:

a) Annual review of content, and refresh as necessary to address changes in law, policy or present information security threats.

b) Information security awareness training for new employees. This training must be completed within reasonable proximity to employee start date as established by the campus.

c) Annual information security awareness refresher training for all campus employees who interact with protected Level 1 information assets.

d) Periodic information security awareness refresher training for all campus employees who access information assets on a schedule established by the campus and not to exceed three years.

e) Annual information security training for privileged users (e.g., system and security administrators) who interact with information systems containing protected data.

f) Information security training for the ISO and other managers responsible for developing and coordinating the campus information security program and controls as needed to address changes in law, policy or present information security threats.

1.2 Ongoing security awareness outreach activities for all persons who use or access campus information assets must be recorded and available for internal audit.

1.3 Security awareness refresher training may take the form of activities such as brownbag sessions, information on special topics delivered via email and other presentations or publications.

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>3/2011</td>
<td>Macklin</td>
<td>Draft Standard</td>
<td>All</td>
</tr>
<tr>
<td>1.1</td>
<td>9/2/2011</td>
<td>Moske</td>
<td>Format draft.</td>
<td>All</td>
</tr>
</tbody>
</table>

Last Revised: 07/16/13
<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/13/12</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Review</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>
POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing third party relationships and guidance for granting access to third parties.

POLICY STATEMENT

100 Managing Third Parties
Third parties who access CSU information assets must be required to adhere to appropriate CSU and campus information security policies and standards. As appropriate, a risk assessment must be conducted to determine the specific implications and control requirements for the service provided.

200 Granting Access to Third Parties
Third party service providers may be granted access to campus information assets containing protected data as defined in the CSU Data Classification Standard only when they have a need for specific access in order to accomplish an authorized task. This access must be authorized by a designated campus official and based on the principles of need-to-know and least privilege.

Third party service providers must not be granted access to campus level 1 or level 2 information assets as defined in the CSU Data Classification Standard until the access has been authorized, appropriate security controls have been implemented, and a contract/agreement has been signed defining the terms for access.
8040.S001  Third Party Security

Implements:  
CSU Policy #8040.00

Policy Reference:  
8040.00  Managing Third Parties

Introduction

Campuses must ensure that when critical or protected information is shared with third parties, it is either specifically permitted or required by law and that a written agreement is executed between the parties that addresses the applicable laws, regulations, and CSU/campus policies, standards, procedures, and security controls that must be implemented and followed to adequately protect the information asset.

The agreement must also require the third-party, and any of its subcontractors with whom it is authorized to share the data, to share only the minimum information necessary, to securely return or destroy the personal information upon expiration of the contract, and to provide immediate notification to the campus, whenever there is a breach of Level 1 data.

1.0  Third Party Contract Language

When developing a contract, each campus must address the following:

a) Include a clear description of the scope of services provided under the contract or purchase order.

b) Clearly state the security requirements for the vendors to ensure that their work is consistent with the CSU security policy and standards.

c) Require compliance with the CSU security policy and standards. Exceptions may only be granted by the campus President (or President-designee) and must be reported to the ISO.

d) Clearly identify any and all types of protected data to be exchanged and managed by the vendor.

e) Identify incident reporting requirements.

f) Require immediate notification of any security breaches associated with Level 1 information.

g) Require notification within a specified period of time of any security breaches associated with all other information.

h) If appropriate, make provisions for CSU to have the ability to inspect and review vendor operations for potential risks to CSU operations or data.

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/17/2011</td>
<td>Cheryl Washington</td>
<td>Release of New Document</td>
<td>All</td>
</tr>
</tbody>
</table>

Last Revised: 06/13/12
### Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/03/12</td>
<td>ISAC</td>
<td>Approved</td>
</tr>
<tr>
<td>06/13/12</td>
<td>William Perry</td>
<td>Approved</td>
</tr>
</tbody>
</table>
POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing information technology security and guidance for: monitoring CSU information assets; protecting information assets from malicious software; and managing network security and mobile devices.

POLICY STATEMENT

100 Information Technology Security
Campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

200 Protections Against Malicious Software Programs
Each campus must have plans in place to detect, prevent, and report malicious software effectively. Electronic data received from untrusted sources must be checked for malicious software prior to being placed on a non-quarantined location on a campus network or information system.

300 Network Security
Campuses must appropriately design their networks—based on risk, data classification, and access—in order to ensure the confidentiality, integrity and availability of their information assets. Each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

400 Mobile Devices
Campuses must develop and implement controls for securing protected data stored on mobile devices. Protected data must not be stored on mobile devices unless effective security controls have been implemented to protect the data. Campuses must use encryption, or equally effective measures, on all mobile devices that store level 1 data as defined in the CSU Data Classification Standard. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by a designated campus official. Other effective measures include physical protection that ensures only authorized access to protected data.

500 Information Asset Monitoring
Campuses must implement appropriate controls on the monitoring of information systems and network resources to ensure that monitoring is limited to approved activities. Monitoring must not be conducted for the purpose of gaining unauthorized access, "snooping", or for other activities that violate the CSU Responsible Use Policy. Records created by monitoring controls (e.g. logging) must be protected from unauthorized access and reviewed regularly. Campuses must ensure that only individuals who have a "need-to-know" are granted access to data generated from monitoring controls.

Data generated by monitoring must be retained for a period of time that is consistent with effective use, CSU records retention schedules, regulatory, and legal requirements such as compliance with litigation holds. At a minimum, server administrators are required to scan regularly, remediate, and report un-remediated vulnerabilities on critical systems or systems that store protected information within a prescribed timeframe. The risk level of a system determines the frequency at which logs must be reviewed. Risk factors to consider are:

- Criticality of business process.
- Information classification associated with the system.
- Past experience or understanding of system vulnerabilities.
- System exposure (e.g., services offered to the Internet).
8045.S200 Malicious Software Protection

Implements: CSU Policy #8045.0

1.0 Malicious Software Protection

1.1 All campus information systems must be secured with current versions of campus approved anti-malware software unless otherwise authorized by the campus.

1.2 Campus approved anti-malware software must
   a) be capable of detecting, removing, and protecting against malicious software, including viruses, spyware, and adware
   b) scan all data in "real time", including data which is both stored and received by the information system, before data files are opened and before software is executed
   c) be capable of tracking and reporting significant actions taken by the software (e.g., deleted or quarantined malware)
   d) check for and install updates and signatures at least daily

1.3 Unless appropriately authorized, users must not bypass or turn-off anti-malware software installed on campus information systems.

1.4 Each campus must develop and implement controls to filter and limit unsolicited e-mail messages (e.g., spam, phishing, malware-infected, etc.).
### Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/15/2011</td>
<td>Macklin</td>
<td>Incorporation of ISAC Comments</td>
<td>All</td>
</tr>
<tr>
<td>1/3/2012</td>
<td>Moske</td>
<td>Formatted</td>
<td>All</td>
</tr>
<tr>
<td>1/11/2012</td>
<td>Macklin</td>
<td>Editing, formatting. Final Review</td>
<td>All</td>
</tr>
<tr>
<td>3/4/2013</td>
<td>Shaffer</td>
<td>Incorporated changes based on ISAC review</td>
<td>All</td>
</tr>
<tr>
<td>3/11/2013</td>
<td>Macklin</td>
<td>Numbering, Musts.</td>
<td>1</td>
</tr>
</tbody>
</table>

### Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/21/2013</td>
<td>ISAC</td>
<td>Reviewed, approved and recommended for CISO review</td>
</tr>
<tr>
<td>3/3/2014</td>
<td>CISO</td>
<td>CISO Reviewed, approved. Posted</td>
</tr>
</tbody>
</table>
8045.S300 Network Controls Management

Implements: CSU Policy #8045.00
Policy Reference: 8045.00 Information Technology Security

Introduction

Campuses must establish a method for documenting the campus network topology, equipment configuration and network address assignments.

1.0 Network Information Requirements

Each CSU campus must develop and maintain documentation of its network structure and configuration. At a minimum, the following information must be included:

1.1 Network topology information containing:
   a) The locations and IP addresses of all segments, subnets, and VLANs.
   b) Identification of any established security zones on the network and devices that control access between them.
   c) The locations of every network drop and the associated switch and port on the switch supplying that connection.
   d) A summary representation (e.g., drawing) of the logical design appropriate for managerial discussions.
   e) A summary security model appropriate for managerial discussion.

1.2 IP address management
   a) Static IP address assignments information sufficient to identify host, contact and device location (for wired ports)
   b) Dynamic address server (i.e., DHCP) settings showing:
      - Range of IP addresses assigned
      - Subnet mask, default gateway, DNS server settings, WINS server settings assigned

1.3 Configuration information network devices such as:
   a) Switches
   b) Routers
   c) Firewalls
   d) Any other device critical to the functioning of the network

1.4 Configuration information for devices must include but not be limited to:
   a) Net masks
   b) Default gateway
   c) DNS server IP addresses for primary and secondary DNS servers
   d) Any relevant WINS server information
   e) Responsible administrator contact information
2.0 Network Documentation Management

2.1 Each campus may determine its specific methods for documentation using any combination of online network tools, databases, or hard copies; however, the resulting information must be in a form and format available for audit and review.

2.2 Each campus must establish a method for self-review of network documentation such that each element is reviewed for accuracy and completeness at least every 36 months, and designated critical system information at least every 12 months.

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/8/11</td>
<td>Macklin</td>
<td>Incorporation of ISAC and NTA comments</td>
<td>All</td>
</tr>
<tr>
<td>11/9/2011</td>
<td>Moske</td>
<td>Formatted</td>
<td>All</td>
</tr>
<tr>
<td>1/11/2012</td>
<td>Macklin</td>
<td>Final review</td>
<td>None</td>
</tr>
<tr>
<td>12/13/12</td>
<td>Macklin</td>
<td>ISAC Review – Approved to publish,</td>
<td>Intro</td>
</tr>
<tr>
<td>9/26/13</td>
<td>Hendricks</td>
<td>Renumbered for consistency</td>
<td></td>
</tr>
</tbody>
</table>

Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/13/12</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/6/13</td>
<td>ITAC</td>
<td>Reviewed</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>
8045.S301 Boundary Protection and Isolation

Implements: CSU Policy #8045.0

Introduction
Campuses must implement controls designed to provide or limit access to networked CSU assets.

1.0 Boundary Protection and Isolation

1.1 Access to campus networks must be controlled by a technical solution which permits only authorized inbound traffic. Campuses must determine, based on risk analysis, the extent to which outbound traffic is blocked or limited.

1.2 The campuses must appropriately separate network access to public information system resources from those which store protected Level 1 and Level 2 information.

1.3 Campuses must establish zoning or separation within internal networks based on established trust relationships, authorized services, and data classification in order to ensure that protected information is not made available to unauthorized persons.

1.4 All unnecessary services (e.g., Web service, SNMP) on any system which is directly accessible from the internet must be disabled.

1.5 All privileged administrator network access to systems which are directly accessible from the internet must be encrypted and authenticated.

1.6 Each campus must maintain documentation as follows:
   a) A formal, documented process for approving and testing configuration changes to its network and network control devices.
   b) Formal network configuration document that defines all open ports and services on systems directly accessible from the internet.
   c) Justification and risk analysis as appropriate for any allowed service or protocol.
   d) Annual review for all configurations and firewall rules associated with border devices and/or systems directly accessible from the Internet to determine if the rule is still valid, still necessary and performing the function for which it was requested.
## Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/15/2011</td>
<td>Macklin</td>
<td>Incorporation of ISAC Comments</td>
<td>All</td>
</tr>
<tr>
<td>1/3/2012</td>
<td>Moske</td>
<td>Formatted</td>
<td>All</td>
</tr>
<tr>
<td>1/11/2012</td>
<td>Macklin</td>
<td>Final Review – format</td>
<td>All</td>
</tr>
<tr>
<td>6/7/2012</td>
<td>Macklin</td>
<td>Corrected transfer problems – no content change</td>
<td>All</td>
</tr>
<tr>
<td>2/19/2013</td>
<td>Macklin</td>
<td>ISAC Comments</td>
<td>All</td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/19/13</td>
<td>ISAC</td>
<td>Reviewed, approved and recommended for CISO review</td>
</tr>
<tr>
<td>3/03/14</td>
<td>CISO</td>
<td>CISO Reviewed, approved. Posted</td>
</tr>
</tbody>
</table>
8045.S302 Remote Access to CSU Resources

Implements: CSU Policy #8045.00
Policy Reference: 8045.00 Information Technology Security

Introduction

Campuses must implement controls designed to protect CSU resources from unauthorized access from external hosts while making these resources available to legitimate CSU users who are not on campus.

1.0 Public Access Systems

Public access systems are those made available to the public via the Internet, requiring no special access or authentication process. Examples include, but are not limited to: campus informational web pages and class schedule information.

2.0 Non-Public Access Systems

Non-public access systems, regardless of where they are hosted, are those that are available only after authentication or other special access process. Examples include, but are not limited to: online courses, class registration web pages, and internal campus email systems.

2.1 All remote access (wired or wireless) to non-public campus information assets must:
   a) Be authorized and authenticated by use of a unique user identifier.
   b) Pass through a campus-approved access control device (e.g., a firewall or access server).
   c) Be made using an approved method (e.g. campus-authorized remote desktop service).
   d) Use a secure encrypted protocol for the entire session
   e) Be logged and tracked consistent with campus logging procedures.

2.2 Non-public access systems must be configured to automatically terminate inactive connections after an appropriate period of time.

3.0 Non-Public CSU-shared Resources

Remote access to non-public CSU-shared resources (e.g., CMS, CSU SharePoint, etc) must meet or exceed the same access criteria described above for campus information systems and data.

3.1 Campuses must identify and communicate:
   a) Approved user practices for remote connections.
## Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/8/11</td>
<td>Macklin</td>
<td>Incorporation of ISAC and NTA comments</td>
<td>All</td>
</tr>
<tr>
<td>11/9/2011</td>
<td>Moske</td>
<td>Formatted</td>
<td>All</td>
</tr>
<tr>
<td>1/12/2012</td>
<td>Macklin</td>
<td>Format/Bulleted adjustment</td>
<td>All</td>
</tr>
<tr>
<td>7/27/2012</td>
<td>Macklin</td>
<td>Clarified definition remote access compromise</td>
<td></td>
</tr>
<tr>
<td>12/13/2012</td>
<td>Macklin</td>
<td>ISAC: non-public systems may be hosted, CSU shared resources minimum and defn language updated. Reporting of device loss removed as it is covered elsewhere. Approved to publish.</td>
<td></td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/13/12</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Review</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for posting</td>
</tr>
</tbody>
</table>
8045.S400 Mobile Device Management

Implements: CSU Policy #8045.00
Policy Reference: 8045.00 Information Technology Security

Introduction

Campuses must implement controls designed to protect CSU resources that are accessed from or stored on mobile devices.

1.0 Mobile Device Management

As determined necessary by risk assessment, mobile devices must be protected with appropriate security controls. Appropriate security controls can include, but are not limited to:

a) Access control
b) Encryption
c) Strong passwords
d) Anti-virus software
e) Personal firewall

2.0 Storage of Protected Data

2.1 Protected Level 1 data may not be stored on a mobile device unless authorized by appropriate campus administration and encrypted via campus-approved method.

2.2 Each campus must maintain a current inventory of mobile devices that contain protected Level 1 data. This inventory must be reviewed at least annually.

3.0 User Practices for Mobile Devices

3.1 Campuses must identify and communicate approved user practices for mobile device security. Campuses must provide these practices to any individual issued a campus-provided mobile device and include information about mobile device security in security and awareness training material for all campus users.

3.2 Campuses must maintain and publish and a process for users to report if they determine or suspect that any mobile device (including those not provided by campus) which enables access to non-public campus information assets has been lost, stolen, or compromised.
## Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/8/11</td>
<td>Macklin</td>
<td>Incorporation of ISAC and NTA comments</td>
<td>All</td>
</tr>
<tr>
<td>11/9/2011</td>
<td>Moske</td>
<td>Formatted</td>
<td>All</td>
</tr>
<tr>
<td>1/12/2012</td>
<td>Macklin</td>
<td>Final Review</td>
<td>None</td>
</tr>
<tr>
<td>2/19/2013</td>
<td>Macklin</td>
<td>ISAC Review/Approved</td>
<td>3.0, 4.0</td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/19/13</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Review</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for posting</td>
</tr>
</tbody>
</table>
8045.S600 Logging Elements

Implements: CSU Policy #8045.0

Introduction

Each campus must identify and implement appropriate logging and monitoring controls for information assets. These controls must take into consideration the technical capabilities of each resource.

1.0 Logging Elements

1.1 At a minimum and as appropriate, taking into account the capabilities of the device or application creating the log entries, such controls must track and log the following events:
   a) Actions taken by any individual with root or administrative privileges
   b) Changes to system configuration
   c) Access to audit trails
   d) Invalid access attempts (failed login)
   e) Use of identification and authentication mechanisms (logins)
   f) Notifications and alerts
   g) Activation and de-activation of controls, such as anti-virus software or intrusion detection system
   h) Changes to, or attempts to change system security settings or control.

1.2 For each of the above events, the following must be recorded, as appropriate:
   a) User identification
   b) Type of event
   c) Date and time
   d) Success or failure indication
   e) Data accessed
   f) Program or utility used
   g) Origination of event (e.g., network address)
   h) Protocol
   i) Identity or name of affected data, information system or network resource.

1.3 Each campus must establish procedures for the retention of logs and monitoring information.

1.4 Critical servers, at a minimum, must store a copy of their log data on another device; this copy must be protected from unauthorized access.

1.5 Each campus must establish methods for time synchronization of logging and monitoring activities.
### REVISION CONTROL

#### Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/15/2011</td>
<td>Macklin</td>
<td>Incorporation of ISAC Comments</td>
<td>All</td>
</tr>
<tr>
<td>11/15/2011</td>
<td>Moske</td>
<td>Formatted</td>
<td>All</td>
</tr>
<tr>
<td>1/11/2012</td>
<td>Macklin</td>
<td>Format, final review</td>
<td>All</td>
</tr>
</tbody>
</table>

#### Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/23/2013</td>
<td>ISAC</td>
<td>Reviewed, approved and recommended for CISO review</td>
</tr>
<tr>
<td>7/16/2013</td>
<td>CISO / Perry</td>
<td>Approved</td>
</tr>
<tr>
<td>3/3/2014</td>
<td>CISO</td>
<td>Request to Post</td>
</tr>
</tbody>
</table>
8050.00 | Configuration Management

Effective Date: 4/19/2010 | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing a configuration management program.

POLICY STATEMENT

Campuses must develop, implement, and document configuration standards to ensure that information technology systems, network resources, and applications are appropriately secured to protect confidentiality, integrity, and availability.
8050.S100 Configuration Management – Common Workstation Standard

Implements: CSU Policy #8050.0

Introduction
Campuses must develop and implement configuration management standards to address information security risks on campus desktop and laptop computers (workstations) along with associated devices which may store data. Other configuration standards include:

- 8050.S200 Configuration Management – High Risk Workstation Standard
- 8050.S300 Configuration Management – Mobile Device Standard
- 8050.S400 Configuration Management – Common Servers Standard
- 8050.S500 Configuration Management – High Risk Server Standard

1.0 Minimum Configuration Features

1.1 Password Management
State owned desktop and laptop computers must comply with the campus password complexity and aging policies.¹

1.2 Inventory
a) Campus methods for managing computer inventory must have capability of maintaining inventory records for any campus computing devices, such as workstations, laptops, etc.

b) All desktop and laptop computers purchased by the University must be tracked via the campus inventory management system.

c) The campus must establish a periodic inventory process sufficient to ensure that inventory records are current and accurate, and contain information sufficient to support data classification and incident response activities.

d) All devices, including workstations, peripherals, external drives and memory sticks, which store Level 1 protected data must:
   i) Be encrypted using campus approved encryption methods.
   ii) Be tracked and managed via the campus inventory process.²

1.3 Anti-Virus

¹ Please note CSU Standard 8020.S001 Exception Standard for information to be used for any non-compliant workstation.
Up to date anti-virus software must be installed and maintained on all systems. Regular updates to virus definitions and software must be activated.

1.4 Software Updates
Workstation computers must be configured to allow automatic application of software updates through a patch management system.

1.5 Supported Operating Systems
The desktop or laptop device must use a supported operating system in order to ensure that security vulnerabilities are addressed. Where the campus determines that an exception to this standard applies, the campus exception documentation must include controls sufficient to address the risk.

1.6 Enterprise Management
The workstation must be managed by an appropriate configuration management system, such as a campus enterprise desktop management system, that ensures:
   a) The workstation is subject to periodic vulnerability reporting.
   b) The success and/or failure of critical patches is reported.

1.7 Inactivity Screen Lock
a) Workstations must be configured with screen locking features to prevent unauthorized access to a machine while not in use.
   b) Campuses must identify screen lock time limits appropriate to the purpose of the workstation and the environment in which it is located.

---

**REVISION CONTROL**

**Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5</td>
<td>6/10/2014</td>
<td>Macklin</td>
<td>First draft – ISAC development team</td>
<td>All</td>
</tr>
<tr>
<td>0.6</td>
<td>6/27/14</td>
<td>Macklin</td>
<td>ISAC dev team review</td>
<td>All</td>
</tr>
<tr>
<td>0.7</td>
<td>7/22/14</td>
<td>Macklin</td>
<td>Added</td>
<td>1.8</td>
</tr>
<tr>
<td>0.9</td>
<td>9/14/14</td>
<td>Macklin</td>
<td>Revised per ISAC review</td>
<td>All</td>
</tr>
<tr>
<td>1.0</td>
<td>10/15/14</td>
<td>Macklin</td>
<td>Incorporated campus feedback</td>
<td>§ 1.2(a)</td>
</tr>
<tr>
<td>1.1</td>
<td>5/15/15</td>
<td>Macklin</td>
<td>Incorporated feedback from FOA</td>
<td>§ 1.2(b)</td>
</tr>
<tr>
<td>1.2</td>
<td>6/9/15</td>
<td>Grayson</td>
<td>Incorporated feedback from Kircher</td>
<td>§ 1.2(b)         § 1.2(c) § 1.2(d) 1.4 1.6</td>
</tr>
</tbody>
</table>

Last Revised: 1/27/2014
<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/03/15</td>
<td>Perry (CISO)</td>
<td>Reviewed: Submitted to ITAC/ISAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review Timeframe: 06/09/15 until 07/09/15</td>
</tr>
<tr>
<td>07/13/15</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>

Incorporated feedback from Kircher. Cosmetic changes only.

| § 1.2(a)    | § 1.2(b)      |
8050.S200 Configuration Management – High-Risk/Critical Workstation Standard

Implements: CSU Policy #8050.0

Introduction

This standard is intended to provide minimum requirements campuses must implement in order to ensure that those workstations which store or are used to access critical data are protected from unauthorized access.

Other configuration standards include:

- 8050.S100 Configuration Management – Common Workstation Standard
- 8050.S300 Configuration Management – Mobile Device Standard
- 8050.S400 Configuration Management – Common Servers Standard
- 8050.S500 Configuration Management – High Risk Server Standard

1.0 Definitions

A “High Risk” workstation is defined as any workstation that stores or accesses “critical” data or systems.

“Critical data” includes protected level 1 information in such quantities as to require notification of a government entity (i.e. over 500 records under HIPAA or CA 1798.29), or information classified as protected level 1 due to severe risk.\(^1\)

“Access to critical systems” means an elevated access privilege\(^2\) to a system which stores protected level 1 information. Examples of this may include access to the Student Health System, access to payment card processing system, access to student financial records, etc.

2.0 High Risk Workstation Governance

2.1 Incorporating Common Workstation Standards

All High Risk Workstations must meet Common Workstation Standards 8050.S100.

---

\(^1\) See 8065.S02 Information Security Data Classification

\(^2\) System support personnel with elevated access required to support campus critical systems or infrastructure may need to utilize the campus Exception process as per the CSU Information Security Risk Management – Exception Standard 8020.S000.
2.2 **High Risk Workstation Designation**
Campuses must implement a process for designating and reviewing the designation of critical or high risk workstations.

2.3 **Change Control**
The configuration of a High Risk Workstation may not be altered except as approved via the campus Change Control Process.³

2.4 **Physical Security**
High Risk workstations must be physically protected as per the as per the CSU Information Security Standard 8080.501⁴.

### 3.0 **High Risk Workstation Configuration**

#### 3.1 **Network Protection**
In order to protect the high risk workstation from malware and/or data exfiltration, network access must be limited. Additional network protection can be achieved by **one or more** of the following methods, to be determined by risk assessment:

- **a)** Network traffic limited to the minimum necessary to perform business functions by use of isolated network segment with traffic restricted to authorized inbound and outbound ports and destinations. (Please note that this may be used in combination with a virtual desktop environment for other work functions (web browsing, etc.) in order to address productivity.)

- **b)** Intrusion detection and prevention technologies which address hostile sites, malware, etc.

- **c)** Software defined networking, user based and/or application-defined routing or similar use of technology to control connectivity.

#### 3.2 **Protection against “zero day” malware**
For high risk workstations with operating systems commonly vulnerable to malware, either restricted outbound network egress (see § 3.2(a)) or application whitelisting must be used in order to protect against “zero-day” malware.

#### 3.3 **Host-based Firewall**
In order to prevent unauthorized access from other “local” hosts, a Host-Based Firewall must be enabled and configured to restrict access to only authorized hosts.

#### 3.4 **Security Event Logging**
- **a)** The High Risk Workstation must be configured to log security events:

---

b) Campus must identify the logging requirements and configuration settings for the high risk workstation and its application environment including:
   i. Remote or local log storage
   ii. Log retention of at minimum 30 days

c) Log activity must comply with 8045.S600 Logging Elements

3.5 Administrative Accounts
Local administration rights must not be granted to the campus account used for activities such as web browsing. As necessary, the user may be issued a separate local administration account.

3.6 Encryption
High Risk Workstations must use University approved encryption on both the hard drive and removable device peripherals and/or media.

3.7 Remote Support
Remote support applications must be configured to require the user to acknowledge and consent to the remote session.

3.8 High Security Workstation Configuration Checklists
High Risk Workstations must use a current standard secure configuration checklist. Useful resources for developing a checklist include but are not limited to those offered by CIS benchmarks, National Institute of Standards and Technology (NIST USCGB) and/or the Department of Homeland Security. 

3.9 Vulnerability Scanning
Periodic vulnerability scans must be completed and assessed in order to verify that operating systems and application are adequately updated (see 8050.S100 Configuration Management § 1.4).

3.10 Peripheral Communications
Peripherals and association communication protocols (e.g. Bluetooth) must either be adequately secured via encryption or disabled in order to avoid unauthorized access and denial of service issues.

---

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>6/23/2014</td>
<td>Macklin</td>
<td>First draft – ISAC development team</td>
<td>All</td>
</tr>
<tr>
<td>0.4</td>
<td>7/22/14</td>
<td>Macklin</td>
<td>After 7/8 ISAC</td>
<td></td>
</tr>
</tbody>
</table>

6 http://web.nvd.nist.gov/view/neg/repository (link to it) - add to sound business practices.
<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/9/14</td>
<td>Macklin</td>
<td>After 8/26 ISAC Standard Team review</td>
</tr>
<tr>
<td>9/9/14</td>
<td>Macklin</td>
<td>Working on... 9.9 meeting</td>
</tr>
<tr>
<td>9/14/14</td>
<td>Macklin</td>
<td>Changes accepted – publish for ISAC</td>
</tr>
<tr>
<td>9/23/14</td>
<td>Macklin</td>
<td>Incorporated ISAC comments</td>
</tr>
<tr>
<td>10/14/14</td>
<td>Macklin</td>
<td>Incorporated campus feedback</td>
</tr>
<tr>
<td>2/24/15</td>
<td>Macklin</td>
<td>Incorporate CISO comment</td>
</tr>
</tbody>
</table>

**Review / Approval History**

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/7/14</td>
<td>ISAC</td>
<td>ISAC approved, moved to CISO review</td>
</tr>
<tr>
<td>3/2/15</td>
<td>CISO</td>
<td>CISO Reviewed. Next step is collaborative review.</td>
</tr>
<tr>
<td>6/4/15</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>
POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing changes to CSU information assets and provides guidance for implementing emergency changes to CSU information assets.

POLICY STATEMENT

100 Change Control
Changes to information technology systems, network resources, and applications need to be appropriately managed to minimize the risk of introducing unexpected vulnerabilities and ensure that existing security protections are not adversely impacted. Campuses must establish and document a process to manage changes to campus information assets containing level 1 or level 2 data, as defined in the CSU Data Classification Standard.

Campuses must evaluate the information security impact of changes by taking a risk-based approach to change control.

Changes to information assets which store protected data will likely require a more rigorous review than changes to non-critical assets and must be made in accordance with a formal, documented change control process. Changes that may impact the security of these information assets must be identified along with the level of control necessary to manage the change.

Campuses must define and communicate the scope of significant changes to level 1 and level 2 information assets in order to be sure that all affected parties have adequate information to determine if a proposed change is subject to the change management approval process.

200 Emergency Changes
Only authorized persons may make an emergency change to campus information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. Emergency changes are defined as changes which, due to urgency or criticality, need to occur outside of the campus' formal change management process. Such emergency changes must be appropriately documented and promptly submitted, after the change, to the campus normal change management process.
8055.S01 Change Control

Implements: CSU Policy #8055.00
Policy Reference: 8055.00 Change Control

1.0 Introduction

Campuses must establish and document a risk-based process for managing changes to common and shared information assets. Campuses must identify those assets subject to the change control process. However, at a minimum, the campus change management process must include critical and protected information assets.

2.0 Change Management Methodology

The change control review process must include:

   a. Identification and documentation of changes.

   b. Assessment of the potential impact of changes, including security implications.

   c. Identification of a change control authority, which may be vested in either individuals or groups as appropriate.

   d. Documented review and approval by the designated change control authority.

   e. Methods for scheduling and appropriate notification of significant changes.

   f. Methods and standard template for notification to end users of scheduled changes and expected impact.

   g. Ability to terminate and recover from unsuccessful changes.

   h. Testing procedures to ensure the change is functioning as intended.

   i. Communication of completed change details to all appropriate persons.

   j. Updating of all appropriate system documentation upon the completion of a significant change.

   k. Significant changes made to a common or shared CSU information asset (e.g., CMS) must be appropriately reviewed and approved by a centralized CSU change control oversight group.

   l. Significant changes made to a campus-specific information asset must be appropriately reviewed and approved by the designated change control authority.
### 3.0 Sample Change Management Methodology

While each campus may identify its own change control methods, an example follows:

<table>
<thead>
<tr>
<th>Description of Change</th>
<th>Low Impact Changes</th>
<th>Medium Impact Changes</th>
<th>High Impact Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A change intended to repair a fault in an information system or network resource.</td>
<td>A change intended to update or upgrade an information system or network resource.</td>
<td>A change, which will result in major changes to an information system or network resource.</td>
</tr>
<tr>
<td></td>
<td>Such changes can include either the hardware or software components of information systems and network resources.</td>
<td>Such changes can include major patches or significant changes to system configuration to meet a new policy, security guideline, or campus requirement.</td>
<td>Such changes can include implementing new functions or replacing entire systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Such changes can include either the hardware or software components of information systems and network resources.</td>
<td>Such changes can include either the hardware or software components of information systems and network resources.</td>
</tr>
<tr>
<td>Pre-change Requirements</td>
<td>A change plan, including back-out procedures, must be developed and approved.</td>
<td>A formal risk assessment must be conducted on the change.</td>
<td>A formal risk assessment must be conducted on the change.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A change plan, including back-out procedures, must be developed and approved.</td>
<td>A change plan, including back-out procedures, must be developed and approved.</td>
</tr>
<tr>
<td>Approval Required</td>
<td>• System owner&lt;br&gt;• IT manager</td>
<td>• System owner&lt;br&gt;• IT manager (may include ISO and TSO)&lt;br&gt;• Change control group</td>
<td>• System owner&lt;br&gt;• IT manager (may include ISO and TSO)&lt;br&gt;• Change control group</td>
</tr>
<tr>
<td>Post-change Requirements</td>
<td>After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated.</td>
<td>After the change is made, appropriate information system or network resource documentation, operations processes and configuration documentation must be updated.</td>
<td>After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated.</td>
</tr>
<tr>
<td></td>
<td>Change results must be logged and reported to change control group.</td>
<td>Change results must be logged and reported to change control group.</td>
<td>Change results must be logged and reported to change control group.</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/11/2011</td>
<td>Moske</td>
<td>Document Revision: Draft Standards Template</td>
<td>Click here to enter Revision Date</td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/28/11</td>
<td>Washington</td>
<td>Approved</td>
</tr>
</tbody>
</table>
8060.00 | Access Control

Effective Date: 4/19/2010 | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing access to CSU information assets and guidance for: granting access to CSU information assets; separating duties of individuals who have access to CSU information asset; conducting reviews of access rights to CSU information assets; and modifying user access rights to CSU information assets.

POLICY STATEMENT

100 Access Control
On-campus or remote access to information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard must be based on operational and security requirements. Appropriate controls must be in place to prevent unauthorized access to protected information assets. This includes not only the primary operational copy of the protected information assets, but also data extracts and backup copies. Campuses must have a documented process for provisioning approved additions, changes, and terminations of access rights and reviewing access of existing account holders. Access to campus protected information assets must be denied until specifically authorized.

Access to public and shared resources may be excluded from this requirement. Campuses are required to identify and document public or shared resources that are excluded from this requirement. Authorized users and their access privileges must be specified by the data owner, unless otherwise defined by CSU/campus policy.

200 Access Control
Access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of need-to-know and least privilege.

Authentication controls must be implemented for access to campus information assets that access or store protected data, must be unique to each individual and may not be shared unless authorized by appropriate campus management. Where approval is granted for shared authentication, the requesting organization must be informed of the risks of such access and the shared account must be assigned a designated owner. Shared authentication privileges must be regularly reviewed and re-approved at least annually.

300 Separation of Duties
Separation of duties principles must be followed when assigning job responsibilities relating to restricted or essential resources. Campuses must maintain an appropriate level of separation of duties when issuing credentials to individuals who have access to information assets containing protected data. Campuses must avoid issuing credentials that allow a user greater access or more authority over information assets than is required by the employee’s job duties.

400 Access Review
Campuses must develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate campus managers and data owners must review, at least annually, user access rights to information assets containing protected data. The results of the review must be documented.

500 Modifying Access
Modifications to user access privileges must be tracked and logged. Users experiencing a change in employment status (e.g., termination or position change) must have their logical access rights reviewed, and if necessary, modified or revoked.
8060.S000 Access Control

Implements: CSU Policy #8060.00
Policy Reference: 8060.00 Access Control

Introduction
Access to campus information assets containing protected data must include a process for documenting appropriate approvals before access or privileges are granted. All changes to user accounts (i.e., account termination, creation, and changes to account privileges) on campus information systems or network resources (except for password resets) must be approved by appropriate campus personnel. Such approval must be adequately documented in order to facilitate auditing of access control practices.

1.0 Access Authorization
Campuses must identify and document individuals who are authorized to define and approve user access to campus information assets. Campuses must document their authorization procedures. Authorizations must be tracked and logged following campus defined processes and must include information appropriate to the nature of the data stored on the information asset. Information should include:

a) Date of authorization
b) Identification of individual approving access
c) Description of access privileges granted
d) Description of business reason for which access privileges were granted

1.1 Granting Access
Authentication controls must be implemented for campus information assets which store or access protected information, and for systems the campus considers critical to operations. Campus-defined controls must take into consideration:

a) The need to validate user identity prior to granting access to protected data.
b) The requirement for unique user accounts and corresponding access privileges.
c) The requirement to deny all access rights until rights are formally approved and assigned.
d) The ability to report repeated failed access attempts.
e) The ability for access rights to be promptly modified or revoked.
f) The need for authentication credentials to be regularly changed.

1.2 User Account Management

a) Unless otherwise authorized, all users of campus information assets must be identified with a unique credential that establishes identity. This unique credential must not be shared with others except where authorized as an exception to this standard. User credentials must require at least one factor of authentication (e.g., token, password or biometric devices).
b) Campuses must establish criteria for expiring, disabling, and removing user accounts on critical systems and campus information systems or network resources that store or access protected information. The period of acceptable inactivity must be based upon the nature of the data and/or the criticality of the system.

c) "Guest" or generic accounts on campus information systems or network resources may be activated only when authorized by appropriate personnel. Any such account created on a critical system must be reported to the campus information security officer.

d) Campuses must establish processes for re-enabling or resetting user accounts once they have been disabled. User identity must be appropriately verified prior to re-enabling or resetting user accounts.

e) System administrators of campus information systems and network resources must have individual user accountability on the information systems and network resources they administer or use protected utilities to perform system administration tasks. System administrator accounts must not be used for non-administrative uses (e.g., browsing the Web while logged in as administrator).

f) Campuses must establish criteria for creating application or system-level access accounts. These accounts must be assigned appropriate stewards and reviewed at least annually.

1.3 Password Management

a) Campuses must identify and implement password criteria which meets NIST Level 1 “Resistance to Guessing Authentication Secret”\(^1\) at a minimum. To prepare for InCommon Bronze/Silver implementation, campus should consider meeting NIST Level 2 for “Resistance to Guessing Authentication Secret”. Password criteria involves a combination of minimum password length and complexity, password aging, exclusion of dictionary words, and account locking based on failed authentication attempts. Refer to NIST Special Publication 800-63-2 [SP 800-63-2], for a discussion of Authentication Secret complexity and resistance to online guessing. See Appendix A for examples of compliant password criteria and a link to a complexity calculator.

- Complexity: Campuses must implement password complexity standards sufficient to protect against password guessing.
- Failed Attempts: Campuses must identify criteria for disabling (locking) user accounts on critical campus information assets after a number of failed logon attempts, and acceptable timeframes to maintain a disabled state.
- Aging: Campuses must identify and enforce a password change (aging) schedule. The schedule may vary by system or application at the campus’ discretion as determined by risk.

b) Critical information systems and those with protected data should use a secure external authentication method, such as a campus directory server.

c) Passwords and credentials that grant access to Level 1 and Level 2 data must not be used as credentials for personal (non CSU) accounts.

d) Password Issuance – When passwords are issued they must be One-Time Passwords/Keys. One-Time passwords (e.g., passwords assigned during account creation, password resets, or as a second factor for authentication) must be set to a unique value per user and changed immediately after first use.

\(^1\) At present, this publication can be located on line at http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-2.pdf
1.4 Password Storage and Transmission
   a) Passwords or credentials that grant access to level 1 and level 2 data are classified as level 1 data by the
      CSU data classification standard. When transmitted electronically, they must be sent via a
      method that uses strong encryption as per the CSU Information Security Asset Management
      Standard.
   b) All other user account passwords should be protected with strong encryption during storage and
      transmission.
   c) Strong encryption or hash methods must be used to protect any passwords stored in a collection of
      passwords (database).
   d) Campuses may identify service accounts or other low risk applications where password storage or
      transmission in clear text is appropriate.

2.0 Access Modification
At least annually, appropriate campus managers, data stewards, and/or their designated delegates must review,
verify, and revise as necessary user access rights to campus information assets which store or access protected
data. All such revisions must be tracked and logged following campus defined processes and must at least
include:
   a) Date of revision
   b) Identification of person performing the revision
   c) Description of revision
   d) Description of why revision was made

REVISION CONTROL

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>9/1/2011</td>
<td>Macklin</td>
<td>Incorporate ISAC comments</td>
<td>all</td>
</tr>
<tr>
<td>1.2</td>
<td>10/11/2011</td>
<td>Macklin</td>
<td>Incorporate ISAC comments</td>
<td>1.1 – 1.3</td>
</tr>
<tr>
<td>1.3</td>
<td>6/1/2012</td>
<td>Arboleda/Harwood</td>
<td>Incorporated CalPoly Pomona comments and Auditor Concerns</td>
<td>1.0, 2.2, 2.3</td>
</tr>
<tr>
<td>1.4</td>
<td>6/4/2012</td>
<td>Macklin</td>
<td>Comments to v1.3</td>
<td>All</td>
</tr>
<tr>
<td>1.5</td>
<td>6/5/2012</td>
<td>Harwood/Macklin</td>
<td>Final Draft</td>
<td>All</td>
</tr>
<tr>
<td>1.6</td>
<td>3/11/2013</td>
<td>Hendricks</td>
<td>Draft Revision Password Mgmt</td>
<td>1.3</td>
</tr>
<tr>
<td>1.7</td>
<td>5/2/2013</td>
<td>Macklin</td>
<td>Incorporated comments, Created Appendix A</td>
<td>Primarily 1.3</td>
</tr>
<tr>
<td>1.8</td>
<td>5/7/2013</td>
<td>Macklin/Hendricks</td>
<td>Incorporated comments</td>
<td>1.3, 1.4</td>
</tr>
<tr>
<td>1.9</td>
<td>5/15/2013</td>
<td>Macklin</td>
<td>Incorporated comments</td>
<td>1.3(a)(1), 1.3(b)</td>
</tr>
</tbody>
</table>

Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/5/2012</td>
<td>Macklin</td>
<td>Reviewed/Approved</td>
</tr>
<tr>
<td>6/5/2012</td>
<td>Perry (CISO)</td>
<td>Approved</td>
</tr>
<tr>
<td>5/21/13</td>
<td>ISAC</td>
<td>Recommended Updated Draft</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Review</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>

Last Revised: 07/16/13
1.0 Examples of password management settings

1.1 Compliant examples of password criteria that Meet NIST Level 1 include but are not limited to:
   a) 8 characters, with composition rules, no dictionary check, 90 day lifetime, 3 failed logins lock account for 25 minutes
   b) 8 characters, with composition rules, no dictionary check, 180 day lifetime, 3 failed logins lock account for 50 minutes
   c) 15 characters, no composition rules, no dictionary check, 180 day lifetime, 3 failed logins lock account for 30 minutes

1.2 Compliant examples of password complexity that meet NIST Level 1 include but are not limited to:
   a) Minimum password length of eight (8) characters, password must contain at least three (3) out of the four (4) following character types:
      • At least one uppercase alphabetic character (A-Z)
      • At least one lowercase alphabetic character (a-z)
      • At least one special character
      • At least one number (0-9)

   b) Minimum password length of fifteen (15) characters, password must use "pass phrase" composed of four (4) words and punctuation

1.3 Compliant examples of failed login attempt lockout settings include but are not limited to:
   a) After 8 sequential failed authentication attempts, account is locked for 50 minutes

1.4 Compliant examples of password ageing re-use settings include but are not limited to:
   a) Passwords protecting administrative access to Level 1 or Level 2 data must be changed every 90 days
   b) Passwords protecting the ability to create application transactions (e.g. create and/or approve purchase requisitions, create general ledger transactions) must be changed every 180 days
   c) Password reuse must be restricted to no more than one in every four (4) password used.
POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing CSU information assets.

POLICY STATEMENT

Each campus must develop and maintain a data classification standard that meets or exceeds the requirements of the CSU Data Classification Standard.

Campuses must maintain an inventory of information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction.

The designated owner of information assets that store protected data is responsible for:

- Classifying the information asset according to the campus Data Classification Standard.
- Defining security requirements that are proportionate to the value of the information asset.
- Managing the information asset according to the requirements described in the campus Information Asset Management Standard.

Critical or protected data must not be transferred to another individual or system without approval of the data owner. Before critical or protected data is transferred to a destination system, the data owner should establish agreements to ensure that authorized users implement appropriate security measures.
12.0 Asset Management

Each campus must provide for the integrity and security of its information assets by identifying ownership responsibility, as defined with respect to the following:

a) Owners of the information within the campus.
b) Custodians of the information.
c) Users of the information.
d) Classification of information to ensure that each information asset is identified as to its information class in accordance with law and administrative policy.

12.1 Data Ownership

Campuses must complete an inventory identifying Level 1 protected data. Campuses must assign ownership of each information asset containing Level 1 protected data. Normally, responsibility for Level 1 protected data resides with the manager of the campus program that employs the information. When the information is used by more than one program, considerations for determining ownership responsibilities include the following:

a) Which program collected the information.
b) Which program is responsible for the accuracy and integrity of the information.
c) Which program budgets the costs incurred in gathering, processing, storing, and distributing the information.
d) Which program has the most knowledge of the useful value of the information.
e) Which program would be most affected, and to what degree, if the information were lost, inaccurate, compromised, delayed, or disclosed to unauthorized parties.

12.2 Data Classification

The designated owner of an information asset is responsible for making the determination as to how an asset must be classified (e.g., Level 1, Level 2, or Level 3). Data stored on campus hardware or media (both paper and electronic) must be classified per the campus's Data Classification Standard, which must meet or exceed the CSU Data Classification Standard listed in Appendix A of this document.

12.2.1 Use of the CSU Data Classification Standard

a) Campuses may elect to move or add data elements from one classification level to another classification level with higher protection requirements, but never to a classification level with lower protection requirements than the CSU Data Classification Standard. For example, a data element classified as Level 2 can be moved to a Level 1 classification but it cannot be moved to a Level 3 classification.
b) Aggregates of data must be classified based upon the most secure classification level. That is, when data of mixed classification exist in the same file, document, report or memorandum, the classification of that file, document, report or memorandum must be of the highest applicable level of classification. If additional guidance is needed, then the campus ISO must be consulted.

12.2.2 **Maintaining the CSU Data Classification Standard**

a) The CSU's Senior Director for Information Security Management (CISO) must determine what data will be designated Level 1 data and must identify appropriate minimum controls.

b) The CISO must establish a process for the review and maintenance of the data classification standard. The CISO must review the classification standard on an annual basis.

12.3 **Data Handling**

a) Data owners are responsible for identifying procedures that must be followed to ensure the integrity, security, and appropriate level of confidentiality of their information, subject to ISO review. These procedures may include but are not limited to methods for or restrictions on storage of hardcopy, verbal communication of data, etc. Data stored on campus hardware or media must be appropriately labeled and protected according to its classification.

b) When Protected Level 1 data is transmitted electronically, it must be sent via a method that uses strong encryption.

c) When Protected Level 2 data is transmitted electronically, it must be protected using approved campus processes.

12.4 **Data Storage**

a) Each campus must develop and implement appropriate controls for securing protected data. These controls must ensure the confidentiality, integrity, and availability of the asset.

b) Campus electronic media and hardware on which protected data is stored, distributed or accessed must be located and stored in secure locations that are protected by appropriate physical and environmental controls. Hardcopy material containing protected data must be stored in a locked enclosure.

12.5 **Data Retention and Disposition**

All data on campus hardware and electronic and non-electronic media must be retained and disposed of in accordance with CSU Executive Order 1031.

Information that has been identified as or is reasonably believed to be relevant to an existing or potential legal proceeding must be retained while the matter is ongoing in accordance with established campus procedures.

12.6 **Data Backup**

Information systems or files must be backed up using a schedule which is based on the value of the information asset and the requirements of the campus business continuity plan.

Transportation procedures for backup media containing protected data must be documented and reviewed annually.
Backup media containing protected level 1 data must be encrypted using strong encryption methods.

Backups of campus electronic media, records of the backup copies, and documented restoration procedures must be stored in secure locations with an appropriate level of physical and environmental protection.

13.0 REVISION CONTROL

Last Revised:

FINAL:

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>6/20/2011</td>
<td>Macklin</td>
<td>Draft Standard</td>
<td>All</td>
</tr>
<tr>
<td>1.1</td>
<td>6/20/2011</td>
<td>Moske</td>
<td>Format draft</td>
<td>All</td>
</tr>
<tr>
<td>1.2</td>
<td>6/22/2011</td>
<td>Macklin</td>
<td>Incorporating ISAC comments</td>
<td>§ 12.3 – 12.5</td>
</tr>
<tr>
<td>1.3</td>
<td>9/1/2011</td>
<td>Macklin</td>
<td>Added hardcopy restriction to</td>
<td>§ 12.4</td>
</tr>
<tr>
<td>1.4</td>
<td>9/14/2011</td>
<td>Macklin</td>
<td>Modified to scope &quot;Protected Level 1&quot;</td>
<td>§ 12.1</td>
</tr>
<tr>
<td>1.5</td>
<td>10/11/2011</td>
<td>Macklin</td>
<td>Updated with comments from ISAC</td>
<td>§ 12.3, § 12.6</td>
</tr>
<tr>
<td>1.6</td>
<td>1/17/2012</td>
<td>Macklin</td>
<td>Updated with comments from ISAC</td>
<td>§ 12.3, § 12.6</td>
</tr>
</tbody>
</table>

Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/26/12</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Reviewed</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for Posting</td>
</tr>
</tbody>
</table>
The California State University
INFORMATION SECURITY MANAGEMENT

8065.S02 Information Security Data Classification

Implements: CSU Policy #8065.00
Policy Reference: 8065.00 Information Asset Management

1.0 Introduction

This document describes the three levels of data classification that the University has adopted regarding the level of security placed on the particular types of information assets. The three levels described below are meant to be illustrative, and the list of examples of the types of data contained below is not exhaustive. Please note that this classification standard is not intended to be used to determine eligibility of requests for information under the California Public Records Act or HEERA. These requests should be analyzed by the appropriate legal counsel or administrator.

Classification Description: Level 1 - Confidential

Access, storage and transmissions of Level 1 Confidential information are subject to restrictions as described in CSU Asset Management Standards.

Information may be classified as confidential based on criteria including but not limited to:

a) Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.

b) Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU’s reputation, and legal action could occur.

c) Limited use - Information intended solely for use within the CSU and limited to those with a “business need to know.”

d) Legal Obligations - Information for which disclosure to persons outside of the University is governed by specific standards and controls designed to protect the information.

Examples of Level 1 – Confidential information include but are not limited to:

- Passwords or credentials that grant access to level 1 and level 2 data
- PINs (Personal Identification Numbers)
- Birth date combined with last four digits of SSN and name
- Credit card numbers with cardholder name
- Tax ID with name
- Driver’s license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name
- Social Security number and name
- Health insurance information
- Medical records related to an individual
- Psychological Counseling records related to an individual
- Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual’s financial account
- Biometric information
- Electronic or digitized signatures
- Private key (digital certificate)
- Law enforcement personnel records
- Criminal background check results
Classification Description: Level 2 – Internal Use

Access, storage and transmissions of Level 2 - Internal Use information are subject to restrictions as described in CSU Asset Management Standard.

Information may be classified as “internal use” based on criteria including but not limited to:

a) Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.

b) Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the CSU’s reputation, violate an individual’s privacy rights, or make legal action necessary.

Examples of Level 2 – Internal Use information include but are not limited to:

- Identity Validation Keys (name with)
  - Birth date (full: mm-dd-yy)
  - Birth date (partial: mm-dd only)

- Photo (taken for identification purposes)

- Student Information-Educational Records not defined as “directory” information, typically:
  - Grades
  - Courses taken
  - Schedule
  - Test Scores
  - Advising records
  - Educational services received
  - Disciplinary actions
  - Student photo

- Library circulation information.

- Trade secrets or intellectual property such as research activities

- Location of critical or protected assets

- Licensed software

- Vulnerability/security information related to a campus or system

- Campus attorney-client communications

- Employee Information
  - Employee net salary
  - Home address
  - Personal telephone numbers
  - Personal email address
  - Payment History
  - Employee evaluations
  - Pre-employment background investigations
  - Mother’s maiden name
  - Race and ethnicity
  - Parents’ and other family members’ names
  - Birthplace (City, State, Country)
  - Gender
  - Marital Status
  - Physical description
  - Other

Classification Description: Level 3 - General

Information which may be designated by your campus as publically available and/or intended to be provided to the public.

Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the campus in order to mitigate potential risks.

Disclosure of this information does not expose the CSU to financial loss or jeopardize the security of the CSU’s information assets.
# REVISION CONTROL

**Last Revised:**

**FINAL: 09/28/11**

## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>6/16/2011</td>
<td>Macklin</td>
<td>Draft Standard</td>
<td>All</td>
</tr>
<tr>
<td>1.1</td>
<td>6/17/2011</td>
<td>Moske</td>
<td>Format draft.</td>
<td>All</td>
</tr>
<tr>
<td>1.2</td>
<td>9/23/2011</td>
<td>Macklin</td>
<td>Reformat, updates to definitions</td>
<td>All</td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/28/11</td>
<td>Washington</td>
<td>Approved</td>
</tr>
</tbody>
</table>
8065.S003 Information Security Asset Management – Cloud Storage & Services

Implements: CSU Policy #8065.0
Policy Reference: http://www.calstate.edu/csiam/sections/8000/8065_0.shtml

Introduction

The purpose of this standard is to ensure that CSU data is appropriately stored or shared using public cloud computing and/or file sharing services.

Cloud computing services are application and infrastructure resources that users access via the Internet. These services enable customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide services, platforms, and infrastructure to support a wide range of business activities.

Employees must not store or transmit protected University data using services hosted by third parties which do not have a contract in place with the campus or its Auxiliaries, such as personal cloud accounts.

There are a number of information security and data privacy concerns about use of cloud computing services by University Personnel, departments, auxiliaries and centers. They include but are not limited to:

- University no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers
- University dependency on a third party for critical infrastructure and data handling processes
- Potential security and technological defects in the infrastructure provided by a cloud vendor
- University has limited service level agreements for a vendor’s services and the third parties that a cloud vendor might contract with
- University is reliant on vendor’s services for the security of some academic and administrative computing infrastructure

Note that all requirements from all other relevant CSU policies and standards remain in full effect when cloud services are used.

1.0 Definitions

Cloud computing and file sharing, for this purpose, is defined as the utilization of information technology services of any type that is not provided by servers which are owned/leased by the CSU or auxiliaries including, but not limited to, social networking applications, file storage, and content hosting.

The following definitions are taken from NIST Special Publication 800-145, The NIST Definition of Cloud Computing (http://dx.doi.org/10.6028/NIST.SP.800-145).

1.1 Software as a Service (SaaS)

The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not
manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

1.2 Platform as a Service (PaaS)  
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

1.3 Infrastructure as a Service (IaaS)  
The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

2.0 Scope  
This standard applies to all uses of Cloud Computing Services by the CSU or auxiliaries.

3.0 Asset Management  
3.1 Access to Data Stored in the Cloud  
Campus information assets stored in the cloud shall be protected with no less control than that used for on-premise systems, as per ICSUAM 8065 Asset Management and associated standards.

3.2 Protected Level One Data Stored in the Cloud  
Campuses shall not use cloud services to store protected level one data (i.e. storage hosting solutions such as box.com, dropbox.com, google docs, etc) unless such access can be limited by technical or procedural controls in order to reduce inadvertent exposure. Examples of adequate controls include but are not limited to:

- Configuration options which limit user ability to share documents or folders outside the organization
- Training and awareness for users who store protected level one data
- Periodic reports showing user permissions/access, including:
  - Reports of all access
  - Reports of all access granted to off campus entities
- Periodic assessment of protected level one data stored off campus
- Procedures for the management of encryption keys must protect the keys from unauthorized disclosure.

3.3 Synchronization of Stored Content  
Level 1 data stored in a cloud provider may only be automatically synchronized with compliant assets, computers, and devices that are university owned and managed.
4.0 Access Control

4.1 Authentication to Cloud Services

Authentication to campus information assets hosted in the cloud shall be subject to no less control than those hosted on campus and must comply with ICSUAM 8060 Access Control and associated standards.

Central Authentication

Web-based SAAS cloud services must use a campus central authentication method in order to ensure that campuses may appropriately provision and deprovision identities and authorization for campus personnel. Examples of this include but are not limited to Shibboleth, SAML, ADFS, and CAS.

Campus authentication services must be configured in such a manner that the cloud provider does not have access to passwords in either text or encrypted format. Examples of protocols that expose user passwords to the service providers include but are not limited to: LDAP and Radius.

When Central Authentication is Unavailable

The campus must establish a procedure for approving web-based SAAS cloud services that do not use central authentication. This procedure must include a documented risk assessment and periodic review of the service. Where campus authentication is not used, the campus must have a way to recover any account when the community member separates, such as using a campus email address as the contact for password resets, maintaining an appropriately protected list of passwords, or having the campus administer the accounts. Additionally, the cloud host may not store passwords in text, or clear text.

4.2 Multi-Factor Authentication

To mitigate the risk of a data breach occurring as a result of compromised credentials (such as through a successful phishing attack), multi-factor authentication is required for access to level one data belonging to someone else from off campus.

5.0 Acquisition

5.1 Campuses must establish a process and assign responsibility for ensuring that contracts and renewals for cloud services are reviewed in order to identify appropriate supplemental contract language.

5.2 A risk assessment may be necessary where 3rd party contract terms substantially deviate from CSU supplemental or general IT terms in such manner as to pose a risk to the confidentiality, integrity, or availability of CSU protected data.

5.3 To assist campuses in responsibly assessing the risk of contemplated cloud purchases, cloud vendors who will be storing or accessing Protected Level 1, 2, or 3 data, or using central authentication must provide the campus with a security plan and/or policy and at least one of the following before the acquisition of any cloud services:

1. **A current SSAE-16 SOC 2 Type II (or equivalent third party audited security standard)**
   This is a questionnaire that demonstrates the SOC compliance status in the following areas: Security, Availability, Processing Integrity, Confidentiality and Privacy. Each provider must demonstrate adherence to these principles to produce a qualified opinion.

2. **A current Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CSA CAIQ)**
   This is a questionnaire of about 300 questions used to assist both cloud providers, by providing principles of cloud security standards, and clients looking for appropriate cloud providers to suit their business needs and meet their security standards.
3. The *SurveyAnalytics's Standardized Information Gathering Questionnaire*
   This questionnaire is used by outsourcers to obtain required documentation on a service provider and establish a profile on operations and controls for each control area.

4. The *Higher Education Cloud Vendor Assessment Tool*
   This questionnaire is designed specifically to help higher education institutions evaluate the security of cloud vendors.
   
   The vendor provided information must be referenced in the contract. Campuses can tailor the CSA CAIQ or questionnaire, and the risk assigned to each portion of the CSA CAIQ or questionnaire, as appropriate for each purchase. Examples are provided in Appendix A.

5.4 The requestor must provide a complete description of how they will deploy the product, including the type of data that will be involved and the type of authentication that will be used. A sample format is included in Appendix B.

5.5 Acquisition of cloud services which store, or access, or provided access to protected data must comply with ICSUAM 8040 Managing Third Parties. Informing users: Campus must publish a guideline indicating what types of data may be stored on each cloud storage solution and how each cloud storage solution may be used, and must inform all users of cloud storage of this guideline.

6.0 Appendix A

   *CAIQ Protected Level 1 Cloud Assessment*
   *CAIQ Protected Level 2 Cloud Assessment*
   *CAIQ Protected Level 3 Cloud Assessment*

7.0 Appendix B

   *Security Data Requirements Checklist*
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>8/3/2015</td>
<td>CSU Chico</td>
<td>Initial version provided by CSU Chico.</td>
<td>All Sections</td>
</tr>
<tr>
<td>1.0</td>
<td>12/13/2016</td>
<td>Andru Luvisi</td>
<td>Revised all sections.</td>
<td>All Sections</td>
</tr>
<tr>
<td>1.1</td>
<td>2/17/2017</td>
<td>Andru Luvisi</td>
<td>Added details on each type of questionnaire</td>
<td>Section 5.3</td>
</tr>
<tr>
<td>1.2</td>
<td>9/5/2017</td>
<td>Andru Luvisi</td>
<td>Minor Edits</td>
<td>Sections 3.0-5.0</td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/06/2017</td>
<td>W. Perry</td>
<td>Reviewed and Approved</td>
</tr>
<tr>
<td>2/22/2017</td>
<td>W. Perry</td>
<td>Reviewed: Submitted to ITAC/ISAC Review Timeframe: 02/24/17 until 03/24/17.</td>
</tr>
<tr>
<td>9/5/2017</td>
<td>E. Hudson</td>
<td>Reviewed: Minor edits. Submitted to ITAC/ISAC Review Timeframe 9/7/17 to 10/2/17</td>
</tr>
<tr>
<td>10/2/2017</td>
<td>E. Hudson</td>
<td>Reviewed and Approved</td>
</tr>
</tbody>
</table>
POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing the acquisition, development and maintenance of CSU information systems.

POLICY STATEMENT

Campuses must integrate information security requirements into the software life cycle of information systems that contain protected data. The security requirements must identify controls that are needed to ensure confidentiality, integrity, and availability. These controls must be appropriate, cost-effective, and mitigate risks that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of the protected data.
**REVISION CONTROL**

**Document Title:** Application Security  
**Author:** Information Security  
**File Reference:** 8070.S000_Application_Security.docx

**Revision History**

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/8/12</td>
<td>Alex Harwood</td>
<td>Copied text from the Sac State Application Standard and made adjustments to make it CSU generic versus Sac State specific.</td>
<td></td>
</tr>
<tr>
<td>2/15/13</td>
<td>Alex Harwood</td>
<td>Major changes done with the team</td>
<td>All</td>
</tr>
<tr>
<td>3/1/13</td>
<td>Alex Harwood</td>
<td>Minor changes to the document for final draft</td>
<td>All</td>
</tr>
<tr>
<td>6/11/13</td>
<td>Macklin</td>
<td>Updates based on team comments</td>
<td>All</td>
</tr>
<tr>
<td>7/2/13</td>
<td>Macklin</td>
<td>Updates based on team comments</td>
<td>All</td>
</tr>
<tr>
<td>2/26/15</td>
<td>Leslie DeCato</td>
<td>Corrected references to other standards in document</td>
<td>1.5.2, 1.3</td>
</tr>
</tbody>
</table>

**Review / Approval History**

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/15/13</td>
<td>Dustin DeBrum</td>
<td>Reviewed</td>
</tr>
<tr>
<td>3/1/13</td>
<td>Felecia Vlahos</td>
<td>Approved for submission to Policy/Standard/Guideline</td>
</tr>
<tr>
<td>3/1/13</td>
<td>Alex Harwood</td>
<td>Approved for submission to Policy/Standard/Guideline</td>
</tr>
<tr>
<td>7/18/2013</td>
<td>ISAC</td>
<td>Reviewed, approved and recommended for CISO review</td>
</tr>
<tr>
<td>02/26/15</td>
<td>CISO</td>
<td>CISO Approved. Posted</td>
</tr>
</tbody>
</table>
8070.S000 Application Security

Implements: CSU Policy 8070.0
Policy Reference: https://csyou.calstate.edu/Policies/icsuam/Pages/8070-00.aspx

1.1 Application Security Standards

This standard applies to all CSU applications and web environments which:

- Are considered mission critical systems,
- Access protected level 1 information,
- Access protected level 2 information and are accessible from the Internet, or
- Provide an official public campus service or presence.

Application and web development environments must comply with CSU and campus standards and procedures. Contracts for services involving application, web development or hosting must incorporate appropriate language (see 8040S000 Third Party Contract Language).

Campuses must develop and maintain information security criteria for application development. These criteria must apply both to internally developed applications and those developed by contractors or vendors. Criteria must include a process for ensuring that the campus Information Security Office is made aware of applications which access or provide protected level 1 data.

1.2 Application and Web Development Environment Assessment

Campus procedures for local development must ensure that before development begins:

- The planned application and supporting environment have been documented. Documentation must:
  - Adequately describe the purpose and behavior of the application
  - Identify the type and configuration of the supporting systems and networks.
- Risk analysis verifies that:
  - The application and supporting environment will comply with all applicable policies, standards, and procedures
  - Deploying the application will not introduce any unacceptable risks.

1.3 Application Development and Production Architecture

Development and testing must be performed in a non-production environment:

- Production environments for applications with high risk should run on stand-alone dedicated servers or VM server containers.
- Production servers and development servers which store, process or transmit protected data must be housed in a data center that meets physical and logical security control requirements as per CSU Information Security Policy 8080 Physical Security.
- Servers must be placed in the appropriate network zone based on the campus approved network architecture plan as per 8045S4301 Boundary Protection and Isolation Standard § 2.2.
- Servers should be "hardened" according to the campus configuration procedures in order to ensure that they are secure.
1.4 Application Coding
Applications must be reviewed, tested, and documented as determined by a risk assessment, before being placed into a production environment to ensure vulnerabilities are addressed, including but not limited to:

- Un-validated input
- Inadequate access control
- Inadequate authentication and session management
- Cross-site scripting (XSS) attacks
- Buffer overflows
- Injection flaws
- Improper error handling
- Insecure storage
- Denial of service Standards
- Insecure configuration management

The integrity and availability of source code and/or critical files/folders must be ensured by use of a source code control system and scheduled backups.

1.5 Application Development

1.5.1 Data Security
Within the development environment:

- Application developers must remove all test data and test accounts before deploying an application into a production environment.
- Protected data should be redacted where possible in the development environment.

Within the production environment:

- Sample or example scripts must be removed from production servers.
- Protected data may not be displayed in any documentation.
- Developers must check system, test and development tools and processes to be sure that protected data is not copied or created accidentally. Refer to CSU Policy 8065 Information Asset Management along with associate standards.

1.5.2 Logging
Applications should log information as per 8045S600.

All log data should be written to an external log server or solution as determined by risk.

Logging should be enabled for operating system, database, network, application server, web server and other components of the application system in order to provide sufficient information for incident or problem analysis. See 8045S600 Logging Elements for more information about logging requirements.

1.5.3 Applications Collecting Personally-Identifiable Data
CSU Policy 8025.0, Privacy of Personal Information, governs the collection and storage of personal information. Respondents should be informed in advance of the use of "web bugs," URL keywords, or other methods to track respondents' identities. Applications collecting personally identifiable information should, and ecommerce sites must post a web privacy statement describing the type of information collected, how it is to be used, and how it may be disclosed.
1.5.4 Encrypt Protected Information
Applications must encrypt Protected Level 1 information as it is transmitted over the network, including login credentials and session identifiers as per 8065S000 § 12.3 The SSL/TLS (Secure Sockets Layer) protocol is the CSU standard for protecting web-based network traffic. Certificates must be used to provide positive identification of applications to users. Servers must have valid certificates, signed by a recognized Certificate Authority.

1.5.5 Application Authentication
Applications that authenticate users must establish sessions using a randomized session identifier that expires after a specified total time or user inactivity.

1.5.6 Access Control
Applications shall implement the philosophy of “default deny”. Access application content and environments should be denied except for those users and conditions under which access is specifically permitted.

- Developer access privilege should be limited to the least privilege necessary for development.
- If an application needs a system account, an approved and secure service level account must be created and incorporated into the development of the application.
- Users of applications should be prevented from accessing data to which they have not been granted authorization.

Refer to 8060 – Access Control and related standards for more information.

1.5.7 Application Management
Each application process should execute with the least set of privileges necessary to complete the job.

Any elevated permission (system admin account, dba, etc.) should be protected (on a need to know basis), documented and approved through Access Control Processes. Refer to 8060 – Access Control and related standards for more information on granting permissions.

1.6 Web and Application Testing and Change Management
The security of applications and information systems must be appropriately documented prior to production deployment.

Developers must test the information system’s security controls. These tests must verify that controls are working properly.

Tests should be done from a hacker’s point of view, and must be conducted prior to production deployment.

The rigor of the test plan must reflect the risk associated with the application along with the classification of the data being stored or accessed. **NOTE:** The CSU Data Classification Schedule is located at [http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf](http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf).

Developers must document the test plan(s) and test results.

Previously deployed systems must be tested as part of any significant upgrade or as determined by a risk assessment.
1.6.1 Code Reviews
A code review of application code to locate potential security flaws and functionality problems should be performed before production deployment. Any security flaws found should be documented and tracked to resolution.

1.6.2 Web Application Vulnerability Scanning
Web applications should be scanned with an approved web application scanner prior to production deployment and periodically at a frequency determined by risk.

Security vulnerabilities must be remediated or mitigated based on a risk assessment.

1.6.3 Web and Application Change Management
Change management procedures should be in place for all production application implementations.

1.7 Web and Application Periodic Review
Periodic risk assessment reviews should be performed on the application and supporting infrastructure to ensure no new security risks have been introduced.
8075.00 | Information Security Incident Management

Effective Date: 4/19/2010 | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing an information security incident management program.

POLICY STATEMENT

Campuses must develop and maintain an information security incident response program that includes processes for investigating, responding to, reporting, and recovering from incidents involving loss, damage, misuse of information assets containing protected data, or improper dissemination of critical or protected data, regardless of the medium in which the breached information is held or transmitted (e.g., physical or electronic). The campus program must:

- Define and/or categorize incidents.
- Designate specific personnel to respond and investigate information security incidents in a timely manner.
- Include procedures for documenting the information security incident, determining notification requirements, implementing remediation strategies, and reporting to management.
- Include processes to facilitate the application of lessons learned from incidents.
- Support the development and implementation of appropriate corrective actions directed at preventing or mitigating the risk of similar occurrences.

The campus information security incident response plans must be reviewed and documented annually and comply with the CSU Information Security Incident Management Standards.

Campus procedures must include the following notification protocol:

- If a breach of level 1 data has occurred, the campus President must notify the Chancellor, the CIO must notify the Assistant Vice Chancellor for Information Technology Services, and the campus ISO must notify the Senior Director of Systemwide Information Security Management.
- If a breach of level 2 data has occurred, the campus ISO must notify the Senior Director of Systemwide Information Security Management. The Senior Director will provide the Chancellor with quarterly status reports on level 2 data breaches that have occurred in the CSU.
8075.S000 Information Security Incident Management

 Implements: CSU Policy #8075.0
 Policy Reference: 8075.00 Information Security Incident Management

Introduction
Incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff who are capable of investigating and developing a response to, appropriate reporting about, and successful recovery from a variety of incidents. In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences.

1.0 Campus Incident Management Plans
Each campus must develop incident management plans and procedures that include, at a minimum, the following:

1.1 Identification of a Computer Security Incident Response Team (CSIRT). Each campus shall identify the positions responsible for responding to an incident.

1.2 Protocol for escalation and internal reporting. Campus procedures shall outline the method, manner, and progression of internal reporting, so as to ensure that:
   a) Appropriate campus officials are informed about appropriate security incidents.
   b) The CSIRT is assembled.
   c) The incident is addressed in the most expeditious and efficient manner.
   d) Any actual or suspected breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is reported immediately to the CSU Chief Information Security Officer.

1.3 Procedures for investigating an incident. Each campus must document and develop appropriate procedures and processes for investigating information security events and incidents. These procedures must include minimal investigative requirements required to determine if protected information was stored on or accessible by a potentially compromised system. Campuses must document the mitigation process after identifying vulnerabilities on previously deployed systems.

1.4 Post incident analysis. Campuses shall review each incident to identify and apply lessons learned.

2.0 Investigating
Each campus must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. For the purposes of this standard, incidents include, but are not limited to, the following:

2.1 Data (includes electronic, paper, or any other medium):
a) Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any Level 1 or Level 2 data.
b) Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29, HIPAA regulations or other legal or contractual obligation.
c) Deliberate or accidental distribution or release of personal information by a campus, its employee(s), or its contractor(s) in a manner not in accordance with law or CSU/campus policy.
d) Data handling compliance failures that constitute information security risk potential.

2.2 Inappropriate Use and Unauthorized Access – This includes tampering, interference, damage, or unauthorized access to campus information assets. This also includes, but is not limited to: successful virus attacks, web site defacements, server compromises, and denial of service attacks.

2.3 Equipment – Theft, damage, destruction, or loss of campus IT equipment, including laptops, tablets, integrated phones, personal digital assistants (PDAs), or any electronic devices containing or storing confidential, sensitive, or personal data.


2.5 Any other incidents that violate campus information security policy or conditions that provide substantial information security risk.

3.0 Evidence Collection and Handling

3.1 Each campus must develop and maintain procedures and processes for evidence handling. At a minimum, the campus plan must describe the campus' access to forensic resources (either internal or through external arrangements) and its criteria for contacting law enforcement.

3.2 If a campus chooses to maintain its own forensic capability, the campus must maintain procedures and processes for ensuring that evidence and/or information collected under circumstances such as a litigation hold, or Public Information Act request is collected, documented and stored in a manner consistent with legal requirements as appropriate.

4.0 Incident Reporting

4.1 Each campus must identify a point of contact (POC) for information security incident reporting. A campus POC can be an individual (e.g., ISO) or an organization (e.g., IT Help Desk or Computer Security Incident Response Team (CSIRT)).

4.2 A formal, centralized method (i.e., email or phone number) for reporting information security incidents to campus POCs must be provided to users. Each campus must identify and communicate means for users and third parties to report suspected incidents. This information must be part of routine security awareness activities. Any user who observes or suspects that an information security incident is occurring with a campus' information assets must promptly report the incident to the campus' POC. Third parties who observe or suspect that an information security incident is occurring with a campus's information asset must promptly report the incident to their campus business contact. A user must not prevent or obstruct another user from reporting an information security incident in the above manner.

4.3 Each campus' POC must implement feedback processes to ensure that those reporting information security incidents are appropriately acknowledged.
5.0 Internal Notifications

5.1 Each campus must inform the CSU CISO of any security incident resulting in exposure of protected information. The notification process must include the following steps:

a) Initial notification informing the CSU CISO that the campus is investigating a potential breach. This notification must be made immediately. If notice is made via voice, the campus must provide an email message confirming that the notice has been made and providing the required elements of § 5.1(b).

b) The initial notification must include the nature of the potential breach, an estimate of the severity — i.e. number of records and types of information at risk of exposure.

c) On completion of the incident risk assessment, the campus ISO must immediately notify the CSU CISO and the campus whether or not the campus has determined that there is a low probability that protected information has exposed.

d) If protected data has been exposed:
   a. The CSU CISO will then:
      i. Notify CSU Risk Management
      ii. Notify the CSU HIPAA Privacy Officer if appropriate (HIPAA related incidents
      iii. Notify the CSU OGC
      iv. Notify the CSU CIO
      v. Notify the CSU CFO if appropriate (PII or HIPAA related incidents)

b. The ISO shall
   i. Notify the campus President and CIO as appropriate.
   ii. Notify the campus OGC liaison.

c. The campus President shall contact the Chancellor.

6.0 External Notifications

6.1 In the case that external notifications are to be made to impacted party(ies), the notification process must include the following steps:

a) A DRAFT copy of the notification must be sent to the CSU CISO for review.
   a. The CSU CISO will then:
      i. Review DRAFT and provide input
      ii. Send the DRAFT to CSU OGC for review and input
      iii. Send updated DRAFT to campus ISO / POC

6.2 In the case that the exposed data contains HIPAA or PII and the impacted group is 500 records or greater, the following steps must occur:

a) The ISO will send a DRAFT copy of the notice intended for the appropriate organization (AG, HHS, DOE, Media, etc.) to the CSU CISO.
   a. The CSU CISO will then:
      i. Review DRAFT and provide input
      ii. Send the DRAFT to CSU OGC for review and input
      iii. Send the updated DRAFT to campus ISO / POC for external organization
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>3/7/2011</td>
<td>Macklin</td>
<td>Incorporates campus and ISAC comments. TBD Clarification on evidence/forensics</td>
<td>14.X</td>
</tr>
<tr>
<td>1.0</td>
<td>3/22/2011</td>
<td>Washington</td>
<td>Formerly known as standard &quot;14&quot;. Reformatted and re-arranged text. Add a statement regarding post-event reviews.</td>
<td>All</td>
</tr>
<tr>
<td>1.1</td>
<td>1/23/14</td>
<td>Macklin</td>
<td>Updated notification, HIPAA updates</td>
<td>§1, 2, 5</td>
</tr>
<tr>
<td>1.2</td>
<td>2/20/14</td>
<td>Perry</td>
<td>Updated notifications</td>
<td>5.1.d, 6</td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/21/12</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Review</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for posting</td>
</tr>
<tr>
<td>2/20/14</td>
<td>CISO</td>
<td>Reviewed Approved for posting</td>
</tr>
</tbody>
</table>
## Revision Control

### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>3/7/2011</td>
<td>Macklin</td>
<td>Incorporates campus and ISAC comments, TBD Clarification on evidence/forensics</td>
<td>14.X</td>
</tr>
<tr>
<td>1.0</td>
<td>3/22/2011</td>
<td>Washington</td>
<td>Formerly known as standard &quot;14&quot;. Reformatted and re-arranged text. Add a statement regarding post-event reviews.</td>
<td>All</td>
</tr>
<tr>
<td>1.1</td>
<td>1/23/14</td>
<td>Macklin</td>
<td>Updated notification, HIPAA updates</td>
<td>§1, 2, 5</td>
</tr>
<tr>
<td>1.2</td>
<td>2/20/14</td>
<td>Perry</td>
<td>Updated notifications</td>
<td>5.1.d, 6</td>
</tr>
</tbody>
</table>

### Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/21/12</td>
<td>ISAC</td>
<td>Recommended</td>
</tr>
<tr>
<td>6/5/13</td>
<td>ITAC</td>
<td>Review</td>
</tr>
<tr>
<td>7/16/13</td>
<td>Perry (CISO)</td>
<td>Approved for posting</td>
</tr>
<tr>
<td>2/20/14</td>
<td>CISO</td>
<td>Reviewed Approved for posting</td>
</tr>
</tbody>
</table>
8080.00 | Physical Security

Effective Date: 4/19/2010 | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for protecting limited access areas from unauthorized physical access.

POLICY STATEMENT

Each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where information assets containing protected data are stored. Campuses must protect these limited-access areas from unauthorized physical access while ensuring that authorized users have appropriate access. Campus information assets which access protected data that are located in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. The level of protection provided must be commensurate with that of identifiable risks. Campuses must review and document physical access rights to campus limited-access areas annually.
1.0 Introduction

Physical and environmental security controls prevent unauthorized physical access, damage, and interruption to campus’ information assets. Campus controls must be adequate to protect critical or protected data. Such controls must:

a. Manage control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by campus staff and outsiders.

b. Prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

2.0 Security Zones

Campuses must assign an appropriate security zone designation to their physical areas. Appropriate physical controls must be implemented in shared and limited access security zones to manage access. Campuses must review these controls regularly.

<table>
<thead>
<tr>
<th>Zone</th>
<th>Brief Description</th>
<th>Necessary Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>No information assets containing protected data or critical systems are located in the area.</td>
<td>None. Access to this area can be unrestricted.</td>
</tr>
<tr>
<td></td>
<td>(Example: Student Union, Library open areas)</td>
<td></td>
</tr>
<tr>
<td>Shared Access</td>
<td>An area containing one or more protected information assets or critical systems.</td>
<td>Appropriate physical access controls and construction must be implemented to restrict access to protected information assets or critical systems that reside in the area.</td>
</tr>
<tr>
<td></td>
<td>Persons in the area include those who do not have authorization to protected information assets or critical systems stored in the area.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Example: Administrative Offices)</td>
<td></td>
</tr>
<tr>
<td>Campus Limited Access Area</td>
<td>An area containing one or more protected information assets or critical systems. Persons in the area are authorized to access the</td>
<td>Appropriate physical access controls and construction must be implemented that limit access to the area to only persons having a need for specific access in order to accomplish a legitimate task. The controls must enforce the principles of need to know and least possible privilege.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td>Brief Description</td>
<td>Necessary Controls</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>protected information assets or critical systems.</td>
<td>All physical access to such areas must be controlled by mechanisms such as tracking and logging. Access records must retain information such as:</td>
</tr>
<tr>
<td></td>
<td>(Example: Data Center)</td>
<td>• Records identifying persons with keys (credentials, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Where possible, systems must provide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Date and time of access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o User ID performing access</td>
</tr>
</tbody>
</table>

### 3.0 Work Area Security

Campuses must establish and communicate user guidelines for securing protected data in work areas. This includes data in electronic and non-electronic form. The guidelines must address:

a. Ensuring that protected data is not left unattended.

b. Limiting the viewing of protected data from unauthorized users.

### 4.0 Viewing Controls

Information systems accessing protected data must not be left unattended or unsecured. Activation of automatic locking software or log off from the systems must occur when information systems are unattended.

The display screens for all campus information systems that have access to protected data must be positioned such that data cannot be readily viewed by unauthorized persons (e.g., through a window, by persons walking in a hallway, or by persons waiting in reception or public areas). If it is not possible to move a display screen to meet the above requirement, a screen filter must be used.

---

**REVISION CONTROL**

**Revision History**

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/11/2011</td>
<td>Lisa Moske</td>
<td>Document Revision: Draft Standards Template</td>
<td>Click here to enter Revision Date</td>
</tr>
</tbody>
</table>

**Review / Approval History**

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/28/11</td>
<td>Washington</td>
<td>Approved</td>
</tr>
</tbody>
</table>
POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing a business continuity and disaster recovery program.

POLICY STATEMENT

An information security program needs to support the maintenance and potential restoration of operations through and after both minor and catastrophic disruptions. Campuses must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users.

Each campus must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event. The campus program must be in compliance with the CSU Business Continuity Program.
8090.00 | Compliance

Effective Date: 4/19/2010 | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing a system-wide information security compliance program.

POLICY STATEMENT

The CSU Information Security Management Office shall, in consultation with the CSU Office of General Counsel and other subject matter experts, regularly identify and define laws and regulations that apply to CSU information assets. The CSU Information Security Management Office shall provide this information to campuses as it develops. Campuses must develop and maintain information security policies and standards that comply with applicable laws and regulations and the CSU policies that apply to campus information assets. The campus policies and standards must include monitoring controls that ensure ongoing compliance with applicable laws, regulations, and CSU policies.
8095.00 | Policy Enforcement

Effective Date: 4/19/2010 | Revised Date: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for enforcing the CSU Information Security Policy.

POLICY STATEMENT

The CSU respects the rights of its employees and students. In support of the CSU Information Security policy, campuses must establish procedures that ensure investigations involving employees and students suspected of violating the CSU Information Security policy are conducted in compliance with appropriate laws, regulations, collective bargaining agreements, and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

The CSU reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of CSU resources or to protect the CSU from liability.

 Allegations against employees that are sustained may result in disciplinary action. Such actions must be administered in a manner consistent with the terms of the applicable collective bargaining agreement and the California Education code. Student infractions of the CSU Information Security policy must be handled in accordance with the established student conduct process. Auxiliary employees who violate the requirements of the policy may be subject to appropriate disciplinary actions as defined by their organization’s policies. Third party service providers who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the CSU.

The CSU may also refer suspected violations to appropriate law enforcement agencies.
POLICY OBJECTIVE

It is the policy of the CSU to permit the use of electronic or digital signatures in lieu of handwritten signatures. Usage of electronic or digital signatures is at the option of an individual campus or the Chancellor’s Office provided they conform to the terms set forth in this policy.

This policy does not pertain to facsimile signatures printed on checks issued by the CSU.

POLICY STATEMENT

100 Electronic Signatures
An electronic signature is an electronic sound (e.g., audio files of a person’s voice), symbol (e.g., a graphic representation of a person in JPEG file), or process (e.g., a procedure that conveys assent), attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record.

200 Digital Signatures
A digital signature is a specific type of electronic signature that uses cryptographic transformation of data to provide authenticity, message integrity, and non-repudiation.

For a digital signature to be valid, it must be created by a technology accepted for use by the State of California and conform to technologies capable of creating digital signatures as set forth in California Government Code Section 16.5:

(1) It is unique to the person using it;
(2) It is capable of verification;
(3) It is under the sole control of the person using it;
(4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated;
(5) It conforms to Title 2, Division 7, Chapter 10, of the California Code of Regulations.

300 Electronic and Digital Signature Implementation
Campuses must develop procedures to identify, evaluate, and document where electronic signatures are permitted and digital signatures are required. Procedures should follow a risk assessment methodology defined in the Electronic and Digital Signature Standard and must be approved by the Vice President for Administration/CFO.

Campus and Chancellor’s Office standards and procedures for electronic signatures must meet CSU electronic and digital signature standards and may be used for transactions between the CSU and outside parties only when approved by the campus Vice President for Administration/CFO and when both parties have agreed to conduct transactions by digital means.

400 Acceptable Use
Simple Electronic Signatures may convey intent of an individual to sign a record and are often easier to implement. Simple electronic signatures may be acceptable and authorized for internal campus or Chancellor’s Office uses involving low risk.

Digital Signatures may be used where simple electronic signatures are acceptable and authorized for use. They may be permitted or required for any record or document where a signature is required by Federal law, California law, or by CSU policy unless a handwritten signature is explicitly required. Digital signatures must be used instead of a simple electronic signature when legally required or when greater risk exists.

The presence of an electronic signature does not mean that a record was properly signed or that the signatory was authorized. Campus and Chancellor’s Office procedures must identify the person by position who is authorized to sign, approve, and/or prevent unauthorized actions from being taken as a result of an electronic signature.
# REVISION CONTROL

**Document Title:** CSU Digital Signature Standards and Procedures  
**Author:** Information Security and Identity Access Management  
**File Reference:** CSU Electronic and Digital Signature Standards.docx

## Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Revised By</th>
<th>Summary of Revisions</th>
<th>Section(s) Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>08/16/2011</td>
<td>Michael Trullinger</td>
<td>Original Document - LA</td>
<td>Multiple</td>
</tr>
<tr>
<td>09/26/2011</td>
<td>Javier Torner</td>
<td>Release of New Document</td>
<td>Multiple</td>
</tr>
<tr>
<td>09/27/2011</td>
<td>Mark Hendricks</td>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td>09/29/2011</td>
<td>Michael Trullinger</td>
<td>Review – No Significant Additions</td>
<td>Multiple</td>
</tr>
<tr>
<td>11/04/2011</td>
<td>Mark Hendricks</td>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td>11/09/2011</td>
<td>Working Group</td>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td>11/09/2011</td>
<td>Michael Trullinger</td>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td>11/10/2011</td>
<td>Michael Trullinger &amp;</td>
<td>Corrections and Revision</td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Mark Hendricks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12/14/2011</td>
<td>Michael Trullinger</td>
<td>Included feedback from ISAC</td>
<td>Multiple</td>
</tr>
<tr>
<td>04/27/2012</td>
<td>Michael Trullinger</td>
<td>Feedback from OGC, Risk Management, HRM, Audit</td>
<td>Multiple</td>
</tr>
<tr>
<td>05/21/2012</td>
<td>Michael Trullinger</td>
<td>Minor Corrections – 1.0 Release</td>
<td>Multiple</td>
</tr>
<tr>
<td>07/14/2015</td>
<td>Teresa Macklin</td>
<td>6.0 updated with additional risk assessment criteria</td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.0 updated with additional granularity for Electronic Signatures (Electronic Acknowledgement and Electronic Approval)</td>
<td></td>
</tr>
<tr>
<td>04/25/16</td>
<td>Andru Luvisi</td>
<td>Minor corrections to section 14.4, 14.5 and Appendix B</td>
<td></td>
</tr>
<tr>
<td>5/10/16</td>
<td>William Perry, CISO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8/8/16</td>
<td>Andru Luvisi</td>
<td>Reviewed ITAC comments</td>
<td>13.4</td>
</tr>
</tbody>
</table>

## Review / Approval History

<table>
<thead>
<tr>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Action (Reviewed, Recommended or Approved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/25/16</td>
<td>William Perry, CISO</td>
<td>Reviewed</td>
</tr>
<tr>
<td>6/15/16</td>
<td>William Perry, CISO</td>
<td>Reviewed: Submitted to ITAC/ISAC Review Timeframe: 06/15/16 until 07/15/16.</td>
</tr>
<tr>
<td>8/15/16</td>
<td>William Perry, CISO</td>
<td>Reviewed and Approved for Posting</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>1.0 Electronic and Digital Signature Definition</td>
<td>5</td>
</tr>
<tr>
<td>2.0 Electronic and Digital Signature Legality</td>
<td>6</td>
</tr>
<tr>
<td>3.0 Reasons for Applying a Digital Signature</td>
<td>6</td>
</tr>
<tr>
<td>4.0 General Standards and Requirements</td>
<td>7</td>
</tr>
<tr>
<td>5.0 Acceptable Use</td>
<td>7</td>
</tr>
<tr>
<td>5.1 Agreement to Conduct Electronic Transactions</td>
<td>7</td>
</tr>
<tr>
<td>5.2 Signature Required by University Policy</td>
<td>7</td>
</tr>
<tr>
<td>5.3 Signature Required by Law</td>
<td>8</td>
</tr>
<tr>
<td>6.0 Risk-based Approach for Determining Appropriate Digital or Electronic Signature Type</td>
<td>8</td>
</tr>
<tr>
<td>6.1 Level of Assurance for Authentication Definitions</td>
<td>8</td>
</tr>
<tr>
<td>6.2 Determining Risk</td>
<td>8</td>
</tr>
<tr>
<td>7.0 Evaluation Process for Use of Electronic Signature</td>
<td>9</td>
</tr>
<tr>
<td>7.1 Evaluation of Risk</td>
<td>9</td>
</tr>
<tr>
<td>7.2 Determination of Electronic Signature Methodology</td>
<td>9</td>
</tr>
<tr>
<td>7.3 Use of “Lower Assurance” Electronic Signature Methods</td>
<td>10</td>
</tr>
<tr>
<td>8.0 Acceptable Forms of Electronic Signatures</td>
<td>10</td>
</tr>
<tr>
<td>8.1 Electronic Acknowledgement</td>
<td>10</td>
</tr>
<tr>
<td>Click to Accept</td>
<td>10</td>
</tr>
<tr>
<td>Scanned Image of a Handwritten Signature</td>
<td>10</td>
</tr>
<tr>
<td>Authorization by Email</td>
<td>10</td>
</tr>
<tr>
<td>8.2 Electronic Approval</td>
<td>11</td>
</tr>
<tr>
<td>Preserving the integrity of the document being approved</td>
<td>11</td>
</tr>
<tr>
<td>Associating the record of the approval with the approved document</td>
<td>11</td>
</tr>
<tr>
<td>Issuance or level of assurance in identity of signer</td>
<td>11</td>
</tr>
<tr>
<td>9.0 Acceptable Forms of Digital Signatures</td>
<td>11</td>
</tr>
<tr>
<td>9.1 Public Key Cryptography</td>
<td>11</td>
</tr>
<tr>
<td>Public Key Cryptography</td>
<td>11</td>
</tr>
<tr>
<td>9.2 Encryption</td>
<td>11</td>
</tr>
<tr>
<td>10.0 Digital Certificates</td>
<td>12</td>
</tr>
<tr>
<td>10.1 Minimum Requirements</td>
<td>12</td>
</tr>
</tbody>
</table>
10.2 Approved Authorities........................................................................................................... 12
  California State...................................................................................................................... 12
  California State University System....................................................................................... 12
11.0 Issuance and Maintenance................................................................................................ 13
  InCommon Digital Certificate Validation Types ................................................................. 13
12.0 Registration....................................................................................................................... 13
  12.1 Duration and Expiration................................................................................................. 13
  12.2 Revocation ..................................................................................................................... 13
13.0 Storage and Protection...................................................................................................... 14
  13.1 Escrow............................................................................................................................ 14
  13.2 Key Recovery .................................................................................................................. 14
  13.3 User Device Storage ...................................................................................................... 14
  13.4 Retention ......................................................................................................................... 14
    Record Retention ................................................................................................................ 14
  13.5 Recovery, Including Disasters....................................................................................... 14
14.0 Roles and Responsibilities.................................................................................................. 15
  14.1 Digital Signature Subscriber .......................................................................................... 15
  14.2 Certificate Administration .............................................................................................. 15
    Certificate Authority .......................................................................................................... 15
    System ................................................................................................................................. 15
    Issuance and Distribution .................................................................................................. 15
  14.3 Data Steward ................................................................................................................... 15
  14.4 Campus and Chancellor's Office ..................................................................................... 16
  14.5 Office of General Counsel .............................................................................................. 16
  14.6 Information Security Office ............................................................................................ 16
  14.7 Campus Vice President for Administration ................................................................... 16
Appendix A: Contacts .............................................................................................................. 17
Appendix B: Applicable Federal and State Laws and Regulations ........................................ 18
Appendix C: Other Resources and Related Documentation ................................................... 19
Introduction

As organizations move away from paper documents with ink signatures, the ability to sign electronic transactions and documents for business, financial, or other reasons is important, if not essential. There is a considerable amount of confusion surrounding signature technologies, and how they might be used for purposes such as signing an electronic document, signing or encrypting an email, or indicating approval in an electronic workflow process.

These standards and procedures are meant to be referenced by anyone requesting, using, or accepting a CSU approved electronic signature and their intent is to:

- Provide the framework for evaluating the appropriateness of an electronic signature technology for an intended purpose
- Establish a CSU System-wide standard for the management and issuance of "key material" used for digital signatures
- Enable greater adoption of digital signature technology across the CSU to streamline business processes, improve identity proofing processes, and increase information security

The legal definition for electronic signatures has been established in the US Federal Electronic Signatures in Global and National Commerce (ESIGN) Act of 2000 and is very broad. A risk based evaluation using OMB 04-04 "E-Authentication Guidance for Federal Agencies" and NIST SP800-63 must be performed by an organization to determine risks associated with using an electronic signature method and the quality as well as security of the electronic signature method required.

For many day-to-day cases, a simple electronic signature (generated through an authentication or "click to accept" process) is adequate to indicate that an individual has demonstrated intent to sign or approve a transaction. Others cases will require or prefer use of a digital signature.

A digital signature is a very specific form of an electronic signature which uses cryptography to establish the authenticity and validity of the signature with much greater certainty. A digital signature may be utilized where an electronic signature is required. For transactions where there is a greater risk to the CSU, or where a "wet" signature is typically required, digital signatures must be used instead of a simple electronic signature.

Entities Affected

These standards and procedures apply to all members of the CSU community and govern all applications of digital signatures used to conduct official University business. They also apply to transactions between the CSU and other parties.

1.0 Electronic and Digital Signature Definition

An electronic signature is an electronic sound (e.g., audio files of a person's voice), symbol (e.g., a graphic representation of a person in JPEG file), or process (e.g., a procedure that conveys assent), attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record (ESIGN Act of 2000). A digitally reproduced (e.g. scanned) physical signature is a common example.

A digital signature is the cryptographic transformation of data, which when added to a message, allows the recipient to verify the signer and whether the initial message has been altered or the signature forged since the
transformation was made. A digital signature is an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a handwritten signature.

Electronic signatures issued by the CSU are considered property of the CSU and are for University business only. Private keys used for digital signatures are considered 'Level 1' confidential data whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damages to the CSU, its students, its employees, or its customers.

2.0 Electronic and Digital Signature Legality

Under California law, a digital signature has the same force and effect as a manual signature. A digital signature may be affixed to any written communication with the University in which a signature is required so long as it complies with the requirements of California Government Code section 16.5 and these Standards and Procedures.

The legality and enforceability of a signature are typically evaluated based on the answer to the following questions:

- Does a signature represent the intent of the signatory?
- Could the statement have been altered?
- How certain is the signatory's identity?

Simple Electronic Signatures may convey the intent of an individual to sign and are often easier to implement, but usually cannot provide satisfactory assurance if authentication, non-repudiation, and integrity are legally required. Determining appropriateness of an electronic signature type (e.g. digital signatures using PKI or a simpler electronic signature) is based on level of risk. A higher assurance level signature may be required for enforceability.

3.0 Reasons for Applying a Digital Signature

The most common reasons for applying a digital signature are authentication, integrity, and non-repudiation.

**Authentication**

Digital signatures can be used to authenticate the source of messages, documents, and digital content. When ownership of a digital signature secret is known to a specific person only, the digital signature created by that secret can be used to validate authenticity of a person's digital signature.

**Integrity**

A recipient may need confidence that content they have received has not been altered during transmission. Although encryption technology can be used to secure transmissions, it does not guarantee that the content being protected has not been changed without the author's knowledge. The integrity of authorship of digitally signed content is maintained with or without encryption, as long as the process used to create, store, or retrieve the digitally signed content does not permit content to be changed without invalidating (and where appropriate removing) the signature.
Non-repudiation

Digital signatures can provide non-repudiation. Non-repudiation means that signatories cannot successfully claim they did not sign a message while concurrently claiming that the secret part remained solely in their possession. Some non-repudiation practices include a time stamp for the digital signature that can be used to determine signature validity when the date and time of a compromised secret can be determined.

4.0 General Standards and Requirements

A digital signature is based on an asymmetric cryptosystem that uses a mathematical formula to scramble content. With use of appropriate technology, signatories can encrypt (scramble) content, and recipients can decrypt (unscramble) and verify it. To affix a digital signature or scramble electronic content, a signatory must obtain a digital signature from an accepted authority which typically consists of an electronic asymmetric key-pair (includes a private (secret) key and publicly distributable key).

For a digital signature to be considered valid, it must be:

- Capable of verification
- Linked to content in such a manner that if the content is changed, the digital signature is invalidated (and where appropriate and necessary, removed).
- In conformity with Title 2, Division 7, Chapter 10, of the California Code of Regulations
- Issued by an authority

5.0 Acceptable Use

Electronic and digital signatures are permissible for many record types and activities. Digital Certificates, specifically, can be issued for the purposes of authentication, signing and securing e-mail messages or electronic documents, and encrypting content. Procedures used for issuing certificates that will be used to encrypt sensitive documents and data, including S/MIME email messages, should be carefully developed after assessing retention requirements since key backup and/or escrowing may be necessary to decrypt the source content. If a Digital Certificate is issued for authentication and signing only, key backup and escrow may be unnecessary.

5.1 Agreement to Conduct Electronic Transactions

Digital signatures may be used for transactions between the campus, the Chancellor’s Office, and outside parties only when the parties have agreed to conduct transactions by electronic means. The party’s agreement to conduct transactions electronically may be informal or recognized through a contract, including cases where a party’s action indicates agreement.

5.2 Signature Required by University Policy

When a CSU or campus policy requires that a record have the signature of a responsible person, that requirement can be met if the associated digital signature was issued and is maintained using an approved digital signature method and procedure.
5.3 Signature Required by Law
When an authorized representative of a CSU campus uses an approved digital signature method for a signing required by a third party, the CSU will consider the valid digital signature as having met the requirement.

6.0 Risk-based Approach for Determining Appropriate Digital or Electronic Signature Type

Individuals and organizations within the CSU wanting to use electronic signatures must conduct a thorough review of associated risks and must select the appropriate, approved technology. OMB 04-04, FIPS 199, and NIST 800-64 provide mechanisms to establish risk and consequences for business processes.

6.1 Level of Assurance for Authentication Definitions
Electronic authentication is the process of establishing confidence in user identities electronically presented to an information system (NIST SP800-63). "Level of Assurance" is the structure used by the CSU to define the technical and procedural practices to determine authentication certainty.

6.2 Determining Risk
OMB 04-04 "E-Authentication Guidance for Federal Agencies" defines four levels of identity authentication, their associated technical requirements, and risk assessment criteria for determining the impact of authentication errors. In their simplest terms, they are:

- **Level 1**: Little or no confidence in the asserted identity's validity.
- **Level 2**: Some confidence in the asserted identity's validity.
- **Level 3**: High confidence in the asserted identity's validity.
- **Level 4**: Very high confidence in the asserted identity's validity.

OMB 04-04 also identifies six potential impact categories for authentication errors:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Impact values assigned by OMB for these categories of harm are defined in Federal Information Processing Standard 199, "Standard for Security Categorization of Federal Information and Information Systems."

**Impact Values (FIPS 199)**

- **Low**: The loss of confidentiality, integrity and availability could be expected to have a limited adverse effect on organizational operations, organization assets or individuals.
- **Moderate**: The loss of confidentiality, integrity and availability could be expected to have a serious adverse effect on organizational operations, organization assets or individuals.
- **High**: The loss of confidentiality, integrity and availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organization assets or individuals.

**Potential Impact of Financial Loss**

- **Low**: at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- **Moderate**: at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- **High**: severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

**Table 1 – Maximum Potential Impacts for Each Assurance Level**

<table>
<thead>
<tr>
<th>Potential Impact Categories for Authentication Errors</th>
<th>Assurance Level Impact Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Inconvenience, distress, or damage to standing or reputation</td>
<td>L</td>
</tr>
<tr>
<td>Financial loss or agency liability</td>
<td>L</td>
</tr>
<tr>
<td>Harm to agency programs or public interests</td>
<td>L</td>
</tr>
<tr>
<td>Unauthorized release of sensitive information</td>
<td>L</td>
</tr>
<tr>
<td>Personal Safety</td>
<td>L</td>
</tr>
<tr>
<td>Civil or criminal violations</td>
<td>L</td>
</tr>
</tbody>
</table>

NIST 800-63 Electronic Authentication Guideline provides technical requirements for each of the authentication levels of assurance defined in OMB 04-04. Each assurance level has defined controls for identity proofing, token (secret) requirements, and authentication/assertion protection mechanisms as published in NIST 800-63.

**7.0 Evaluation Process for Use of Electronic Signature**

**7.1 Evaluation of Risk**

An evaluation must first be performed by the authoritative Operational Unit to determine risks associated with using an electronic signature, including the quality, security, and method required for a given type of content or document. This evaluation process should use the E-Authentication Guidance for Federal Agencies, OMB 04-04 for reference and guidance. The results of that assessment must be documented and included with the official record of approval and any proposals submitted to the record custodian.

**7.2 Determination of Electonic Signature Methodology**

The electronic signature type selected for a document, content, method, or business process should be commensurate to the assurances needed to mitigate the identified risks. Additionally, specifications for recording, documenting, and/or auditing the electronic signature as required for non-repudiation and other legal requirements shall also be determined by the authoritative operational unit. The lowest cost and least complex method for mitigating risk are generally acceptable. The National Institute of Standards and Technology (NIST) Electronic Authentication Guidelines publication (referenced in this document) should be consulted when making this determination.
The highest impact value as determined by section 6.2 can be used to select a methodology.

- A legal or policy mandate for a written signature or an impact value of high requires a digital signature process.
- If the highest impact value is moderate, than an electronic approval will be sufficient.
- If the highest impact value is low, an electronic acknowledgement will be sufficient.

7.3 Use of “Lower Assurance” Electronic Signature Methods

Operational Units that propose electronic signature methods that are at a lower level of assurance than indicated in the risk assessment process shall:

- Describe the reason for variance
- Identify the potential risk of using a tool from a lower assurance level than the risk assessment identifies
- Justify why a lower assurance level method is appropriate
- Identify the steps that will be taken to mitigate the risk
- Obtain the signed approval of the operational unit director and include it with the official record approving use of an electronic signature method

8.0 Acceptable Forms of Electronic Signatures

Electronic Signatures may be classified into two categories based on level of assurance: electronic approval and electronic acknowledgements.

8.1 Electronic Acknowledgement

Electronic acknowledgement is the lowest level of authenticity. This form of acknowledgement is commonly used in systems with acceptance or “approve” checkboxes. Electronic acknowledgement based mechanisms rely on software configuration safeguards to provide authenticity. For instance, login banners or usage agreements that require an action every time prior to the completion of the task may be considered electronic acknowledgements because the system will not proceed to the next step without user acknowledgement. Given the ease with which images may be manipulated, images without other forms of authenticity should be used for low risk transactions only. Examples include:

Click to Accept

The selection of an option (e.g. tick box or button) on an electronic form to indicate agreement can be used.

Scanned Image of a Handwritten Signature

A scanned image of a handwritten signature can be used as an equivalent to a written signature if signing internal CSU data when the appropriate security requirements have been met. Scanned images of a signature must only be used where express permission has been granted by the author and is considered acceptable for high volume processes such as mass mailings.

Authorization by Email

Given the ease with which email may be manipulated, email receipts without other forms of authenticity such as digital signature, should only be used for low risk transactions. Acceptance or agreement of intent through an
official, controlled Email system (e.g. receipt of an email through the University email system) may be used when the appropriate functional requirements, risk, and security have been carefully considered. "Generic or shared" email accounts may only be used for authorization or acceptance if the appropriate procedures are in place to establish the identity of the actual sender.

8.2 Electronic Approval
Electronic approval is a form of electronic signature that has a higher level of validation than a simple electronic acknowledgement, but remains appropriate only for low-risk conditions.

Preserving the integrity of the document being approved
The document or record being approved must exist in a form which may not be altered. For example, a document in a format not easily altered (e.g. PDF or graphic file) along with authorization and a hash of the content and creation date/time.

Associating the record of the approval with the approved document
The record of approval must be stored with the record or document being approved. The approval record must contain the date and time of approval, and the identity of the approving individual. The identity of the approving individual must be clearly distinguishable (e.g. by recording the login username of the individual who has ‘signed’ the agreement).

Issuance or level of assurance in identity of signer
Services which provide or facilitate electronic approval must be use a campus-provided directory service to authenticate access.

9.0 Acceptable Forms of Digital Signatures
For a digital signature to be valid it must be created by a technology accepted for use by the State of California and that has been adopted by the CSU. Acceptable California State technologies currently include public key cryptography and signature dynamics. The most common technology used is public key cryptography. It has a greater degree of verifiability than signature dynamics, does not require the additional handwriting analysis steps of signature dynamics, and is the only technology accepted by the CSU.

9.1 Public Key Cryptography
Public Key Cryptography
Public Key Cryptography (PKC) signatures allow for third party verification of a signature and are affixed to electronic content using software enhancements to existing applications and web browsers. PKC signatures accepted by the CSU must be issued through a Public Key Infrastructure (PKI) scheme and which results in an asymmetrical digital certificate.

9.2 Encryption
Custodians or users of institutional administrative data who deploy personal digital certificates for encryption must establish procedures ensuring that the CSU has access to all such records and data. Each major operating unit
deploying personal digital certificates for encryption is required to implement procedures to archive, secure, and utilize "master recovery keys".

Any custodian or user of institutional administrative data who deploys software or algorithmic programs to encrypt data is required to inform his or her supervisor prior to deployment and disclose, in a comprehensible form, the keys or other means to access the data.

10.0 Digital Certificates

10.1 Minimum Requirements
For a digital certificate to be considered valid, it must follow California State requirements and:

- Identify the issuing Certificate Authority (CA) that has been authorized by the California Secretary of State.
- Uniquely identify its subscriber
- Include its subscriber's public key
- Identify its operational period
- Be comparable against a well-known Certificate Revocation List (CRL) to confirm its validity
- Be digitally signed by the issuing CA

10.2 Approved Authorities
A Certificate Authority is commonly a well-known, third party entity that is entrusted to issue digital certificates, verify matching of public keys to identify information, and provide a current revocation list. A Certificate Authority, or their delegates, has the responsibility to verify the identity of a subscriber before issuing a certificate.

California State
The list of approved California State authorities is currently available at:

http://www.sos.ca.gov/digsig/

California State University System
The CSU has adopted the InCommon Client Certificate Service as a preferred vendor for PKI digital signature certificates. The California Secretary of State has approved and included this CA in their list under their root name, "COMODO Ltd".
11.0 Issuance and Maintenance

Individuals and organizations within the CSU that want to use electronic signatures must conduct a thorough review of associated risks and must select the appropriate approved technology. OMB 04-04, FIPS 199, and NIST 800-64 provide mechanisms to establish risk and consequences for business processes. If the decision to use digital signature certificates is made, the appropriate validation type must also be selected.

InCommon Digital Certificate Validation Types

A Standard Validation type certificate may be issued to an individual whose campus identity meet both Federal NIST Level 1 requirements and these additional requirements:

- Has a valid I-9 Employment Eligibility Verification form or comparable form on record with the issuing campus.
- Has an electronic credential* provided by the campus that can be uniquely matched to the individual’s valid I-9 record or comparable form.
- Was issued in such a way that ensures and maintains:
  - Single ownership and use of the credential
  - Distribution which ties the unique electronic credential to the individual who submitted the associated I-9 record or comparable form

When met, a digital certificate may be issued through automated processes using that electronic credential*. Standard validation certificates are currently available for employees only.

A High Validation type certificate may be issued to an individual whose campus identity verification processes meet Federal NIST Level 3 requirements as well as requirements for issuance of a Standard Validation type certificate. High Validation certificates may not be issued through an automated process.

12.0 Registration

Registration is the process by which an individual or server identifies and authenticates itself before a digital certificate can be obtained. Applications and servers that require the ability to electronically sign a transaction may be issued a certificate through a designated data steward. Data stewards must submit documentation that includes a description of ongoing system administration and maintenance practices, system access controls procedures, event logging configurations, and security incident response procedures prior to issuance.

12.1 Duration and Expiration

All digital signatures must contain an expiration date. It is recommended that the expiration date not exceed one year from the date of original issue or date of last renewal and may not exceed 3 years.

12.2 Revocation

When a signature is issued, it is expected to be in use for its entire validity period; however, circumstances may require it to be invalidated sooner. Revocation may be requested by the subscriber, a Data Steward, or Information Security under the following conditions:

- The individual who was issued the signature has undergone a name change
- There is a reason to believe that the secret portion of the signature or the storage of it has been compromised
• There is substantive reason to believe that misuse has occurred or is likely to occur
• There is reason to believe the signature is not being used in compliance with these standards
• Related security concerns were identified during an audit
• The subscriber's relationship with the issuing campus has been discontinued
• The minimum requirements for the issued signature are no longer met by the subscriber

13.0 Storage and Protection

13.1 Escrow
The purpose of escrowing electronic signatures or portions of them is to provide access to institutional administrative data by ensuring that access does not become dependent on a single individual or an obscure method of storing and/or protecting them. Signatures or portions of them used for encrypting content require escrowing. Escrowing of private keys for digital signatures must be maintained by the Certificate Authority (CA) issuing the keys.

13.2 Key Recovery
Campuses must develop procedures for retrieval of escrowed materials, such as private keys.
Campus Key recovery procedures should include the following:
• Formal process for logging key recovery and approval
• Key recovery authorization should include at least one campus official. For instance; Key recovery may be approved by the appropriate Data Steward and the campus Information Security Officer.

13.3 User Device Storage
Certificates issued for low to medium risk application may be installed in desktop applications such as email clients and web browsers. High Risk/Level of Assurance certificates must be stored in FIPS 140 approved trusted cryptographic devices such as a smartcard or e-Token device. Private keys are CSU Level 1 data and must be protected via encryption.

13.4 Retention

Record Retention
Digital signatures, digital certificates, and escrowed materials must be retained for a period at least as long as the longest retention period for any documents that are signed or encrypted using those certificates and escrowed materials.

13.5 Recovery, Including Disasters
Campuses and the Chancellor's Office must develop procedures for business continuity and disaster recovery of master recovery keys.
14.0 Roles and Responsibilities

14.1 Digital Signature Subscriber
A subscriber is the individual who has been provided a digital signature certificate for the purpose of signing. The subscriber is responsible for:

- Providing accurate information when applying for a digital certificate
- Taking reasonable precautions to protect and not share the secret portion of the digital certificate (e.g. storing a certificate private key in a password-protected container), ensuring that the digital certificate is under their sole control
- Using the digital certificate only for authorized, legal and University purposes
- Providing written notification to campus Information Security immediately if the secret portion of the signature is believed to have been compromised
- Using their digital certificate for authorized purposes
- Renewal of expired certificates

14.2 Certificate Administration
Certificate administrators are the parties responsible for management of certificate infrastructure, up to and including those responsible for issuance and distribution of digital certificates. The parties are responsible for:

Certificate Authority
- Adequately and safely storing backup copies of all files necessary to re-establish and operate the Certificate Authority
- Timely publication of certificates and revocation information

System
- Protection of escrowed materials, and institutional escrow keys required for certificate retrieval
- Delegation of authority to issue certificates

Issuance and Distribution
- Notification of issuance of a certificate to the subscriber who is the subject of the certificate
- Notification of issuance of a certificate to others than the subject of the certificate

14.3 Data Steward
Data stewards are the individual(s) responsible for a segment of institutional data. Data stewards are responsible for the following as it relates to digital signatures of content germane to their duties:

- Physical and electronic security of any signed data
- Evaluation of transactions enabled by digital signature
- Seeking approval for use of a digital signature from University Legal Counsel or Information Security
- Seeking technical advice from Information Technology Services
- Acknowledgement of applicable liability caps and warranties
- Digital signature verification
14.4 Campus and Chancellor’s Office
CSU Campuses, as well as the CSU Chancellor’s Office, are responsible for maintaining operational and business practices in accordance with these standards and procedures.

14.5 Office of General Counsel
Office of General Counsel may be requested to review and potentially approved the proposed use of a digital signature to determine if it is legally permitted.

14.6 Information Security Office
The Information Security Office is responsible for providing security guidance and for assisting in the auditing process, where assigned. The responsibilities may include and are not limited to:

- Reviewing the digital signature uses and providing recommendations to Data Stewards and the campus Vice President for Administration, including evaluation of associated risks
- Assuring proper issuance and maintenance of campus procedures and subscriber credentials
- Notifying Certificate Administration and Data Stewards within 24 hours of suspected compromises
- Reviewing digital signature implementations and conducting and documenting periodic audits of those implementations at least every three years
- Providing assistance to develop new (or refine existing) campus practices and procedures to ensure protection of digital signatures and their appropriate use
- Notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended
- Notification of revocation or suspension of a certificate to others than the subject whose certificate is being revoked or suspended

14.7 Campus Vice President for Administration
The Vice President for Administration is responsible for delegating campus electronic and digital signature review and audit responsibilities. Final approval or dismissal of campus use of a digital signature is at the Vice President for Administration’s discretion. Determination of approval or dismissal for specific uses may also be made after a review has been conducted by the appropriate data steward.
Appendix A: Contacts

For questions regarding this standard, contact:

CO Manager:
William Perry
Chief Information Security Officer
CSU Office of the Chancellor
wperry@calstate.edu

Subject Matter Experts:
Mr. Michael Trullinger
Associate Director, Identity and Access Management
CSU Office of the Chancellor
mtrullinger@calstate.edu

Javier Torner, Ph.D.
Information Security Officer & Interim Associate Vice President, IRT
CSU San Bernardino
jtorner@csusb.edu
## Appendix B: Applicable Federal and State Laws and Regulations

<table>
<thead>
<tr>
<th>State</th>
<th>Title</th>
</tr>
</thead>
</table>
| California Civil Code, Division 3, Part 2, Title 2.5 | California Uniform Electronic Transactions Act (UETA)  
This Act facilitates electronic transactions consistent with other applicable law and specifies consistent practices concerning electronic transactions. |
| California Code of Regulations, Title 2, Division 7, Chapter 10 | Digital Signatures  
This regulation describes acceptable technology for digital signatures. |
| California Government Code, Section 16.5 | Digital Signatures  
[http://www.sos.ca.gov/digsig/code-section-16-5.htm](http://www.sos.ca.gov/digsig/code-section-16-5.htm) |
## Appendix C: Other Resources and Related Documentation

<table>
<thead>
<tr>
<th>ID / Control #</th>
<th>Title</th>
</tr>
</thead>
</table>
| Integrated CSU Administrative Manual | Digital Signatures  
http://www.calstate.edu/icsuam/sections/3000/3701.01.shtml  
This document specifies the requirements for the use of digital signatures in lieu of handwritten signatures. |
| Section General Accounting 3701.01  |                                                                      |
| CSU Executive Order No. 1031        | Executive Order No. 1031: System-wide Records/Information Retention and Disposition Schedules Implementation  
http://www.calstate.edu/EO/EO-1031.html  
This document ensures compliance with legal and regulatory requirements and best practices of records/information retention and disposition. |
| InCommon                            | InCommon Client Certificate Service Overview  
https://www.incommon.org/cert/clientcerts.html |

Last Revised: 08/12/16
8105.00 | Responsible Use Policy

Effective Date: 11/20/2013 | Revised Date: 11/20/2013

POLICY OBJECTIVE
The CSU Information Security policy provides defines user, including faculty, staff, students, third parties, and CSU responsibilities with respect to the use of CSU information assets.

POLICY STATEMENT

Introduction
The California State University (CSU) provides access to information assets for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students and staff. These resources are vital for the fulfillment of the academic, research and business needs of the CSU community. This policy defines user (e.g., faculty, staff, students, third parties, etc) and CSU responsibilities with respect to the use of CSU information assets in conjunction with the CSU Information Security Policy.

The CSU regards the principle of academic freedom to be a key factor in ensuring the effective application of this policy and related standards. Academic freedom is at the heart of a university's fundamental mission of discovery and advancement of knowledge and its dissemination to students and the public. The CSU is committed to upholding and preserving the principles of academic freedom: the rights of faculty to teach, conduct research or other scholarship, and publish free of external constraints other than those normally denoted by the scholarly standards of a discipline.

This policy is intended to define, promote, and encourage responsible use of CSU information assets among members of the CSU community. This policy is not intended to prevent, prohibit, or inhibit the sanctioned use of CSU information assets as required to meet the CSU's core mission and campus academic and administrative purposes.

The requirements stated within this policy must not be taken to supersede or conflict with applicable laws, regulations, collective bargaining agreements or other CSU and campus policies.

1.0 Scope
1.1 It is the collective responsibility of all users to ensure the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the CSU and to use CSU assets in an effective, efficient, ethical, and legal manner.

1.2 The CSU RESPONSIBLE USE POLICY shall apply to the following:
   a) All campuses.
   b) Central and departmentally managed campus information assets.
   c) All users employed by campuses or any other person with access to campus information assets.
   d) All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
   e) Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

1.3 Auxiliaries, external businesses and organizations that use CSU information assets must comply with the CSU RESPONSIBLE USE POLICY.

1.4 This policy establishes basic responsibilities for all users, the CSU and campuses, and describes expectations for responsible use in the following sections:

<table>
<thead>
<tr>
<th>Section 3.0</th>
<th>General Principles</th>
<th>This section sets forth basic policy principles. Situations or behaviors not specifically mentioned in sections 5.0 - 7.0 may be addressed through application of these basic principles.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 4.0</td>
<td>User - Responsibilities</td>
<td>This section highlights policy specifics related to access, responsible use, network and information system integrity, trademarks and patents, and incidental use.</td>
</tr>
</tbody>
</table>
1.5 The development of this policy was expedited by reference to policies from:

   a) CSU campuses: Bakersfield, East Bay, Fresno, Humboldt, Long Beach, Monterey Bay, Northridge, San Diego, San Luis Obispo, San Marcos, and Sacramento

   b) Other institutions: Concordia College, Montana State University, University of Albany, University of Michigan, and Virginia Tech

2.0 Policy Management

2.1 The CSU RESPONSIBLE USE POLICY shall be updated as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations. The CSU Chief Information Security Officer shall be responsible for overseeing a periodic review of this policy and communicating any changes or additions to appropriate CSU stakeholders.

2.2 The policy may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by each campus.

2.3 Each campus through consultation with campus officials and key stakeholders must develop policies, standards, and implementation procedures referenced in the CSU RESPONSIBLE USE POLICY.

3.0 General Principles

3.1 The purpose of these principles is to provide a frame of reference for user responsibilities and to promote the ethical, legal, and secure use of CSU resources for the protection of all members of the CSU community.

3.2 Use of CSU information assets shall be consistent with the education, research, and public service mission of the CSU, applicable laws, regulations, and CSU/campus policies. Note: The term "information assets", along with many other important terms and concepts, is defined in the CSU ICSUAM Policy Glossary: https://csyou.calstate.edu/ICSUAM/Pages/Policy-Glossary.aspx.

3.3 All users (e.g., faculty, staff, students, third parties) are required to comply with CSU and campus policies and standards related to information security.

3.4 All users (e.g., faculty, staff, students, business partners) are required to help maintain a safe computing environment by notifying appropriate CSU officials of known vulnerabilities, risks, and breaches involving CSU information assets.

3.5 It is the policy of the CSU to make information assets and services accessible in order to meet the needs of CSU students, faculty, staff, and the general public. Information regarding the Accessible Technology Initiative can be found at: https://csyou.calstate.edu/Projects-Initiatives/ATI/Pages/default.aspx.

3.6 All users, including those with expanded privileges (e.g., system administrators and service providers), shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics, and video.

3.7 The CSU respects freedom of expression in electronic communications on its computing and networking systems. Although this electronic speech has broad protections, all University community members are expected to use the information technology facilities considerately with the understanding that the electronic dissemination of information may be available to a broad and diverse audience including those outside the university.

3.8 Other than publicly designated official CSU sites, the CSU does not generally monitor or restrict content residing on CSU systems or transported across its networks; however, the CSU reserves the right to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. These activities are not intended to restrict, monitor, or use the content of legitimate academic and organizational communications.

3.9 In the normal course of system and information security maintenance, both preventive and trouble shooting, system administrators and service providers may be required to view files and monitor content on the CSU and campus networks, equipment, or computing resources. These individuals shall maintain the confidentiality and privacy of information unless otherwise required by law or CSU/campus policy.
3.10 The CSU recognizes and acknowledges employee incidental use of its computing and network resources within the guidelines defined in the "Incidental Use" section of this policy, at paragraph 4.5 below.

3.11 All investigations of CSU or campus policy violations, non-compliance with applicable laws and regulations or contractual agreements will be conducted in accordance with appropriate CSU and campus procedures.

4.0 User Responsibilities
This section describes user responsibilities governing access, responsible use, network and information system integrity, and incidental use. These statements are not designed to prevent, prohibit, or inhibit faculty and staff from fulfilling the mission of the CSU. Rather, these statements are designed to support an environment for teaching and learning by ensuring that CSU resources are used appropriately.

4.1 Responsible Use of Information Assets
4.1.1 Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of CSU equipment, its data and software, and its access.

4.1.2 Users must not use or access CSU information assets in a manner that:
   a) Conflicts with the CSU mission;
   b) Violates applicable laws, regulations, contractual agreements, CSU/campus policies or standards; or
   c) Causes damage to or impairs CSU information assets or the productivity of CSU users through intentional, negligent or reckless action.

4.1.3 Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into CSU computing and networking systems.

4.1.4 Unless appropriately authorized, users must not knowingly disable automated update services configured on CSU computers.

4.1.5 Users must take reasonable precautions to ensure their personal and/or CSU-provided devices (e.g., computers, tablets, smart phones) are secure before connecting to CSU information assets.

4.1.6 Users must close or secure connections to CSU information assets (e.g., remote desktop, virtual private network connections) once they have completed CSU-related activities or when the asset is left unattended.

4.1.7 Users must promptly report the loss or theft of any device, which grants physical access to a CSU facility (e.g., keys, access cards or tokens), or electronic access (passwords or other credentials) to CSU resources.

4.1.8 Users who publish or maintain information on CSU information assets are responsible for ensuring that information they post complies with applicable laws, regulations, and CSU/campus policies concerning copyrighted material and fair use of intellectual property.

4.1.9 Software must be used in a way that is consistent with the relevant license agreement. Unauthorized copies of licensed or copyrighted software may not be created or distributed.

4.1.10 Per Section 8314.5 of the California Government Code, it is unlawful for any state employee, or consultant, to knowingly use a state-owned or state-leased computer to access, view, download, or otherwise obtain obscene matter. "Obscene matter" as used in this section has the meaning specified in Section 311 of the California Penal Code. "State owned or state-leased computer" means a computer owned or leased by a state agency, as defined by Section 11000, including the California State University. This prohibition does not apply to accessing, viewing, downloading, or otherwise obtaining obscene matter for use consistent with legitimate law enforcement purposes, to permit a state agency to conduct an administrative investigation, or for legitimate medical, scientific, or academic purposes.

4.1.11 A user who has knowledge (or reasonable suspicion) of a violation of this policy must follow applicable CSU and campus procedures for reporting the violation. A user must not prevent or obstruct another user from reporting a security incident or policy violation. Refer to CSU Information Security Policy 8075 Information Security Incident Management.

4.2 Protection from Data Loss
4.2.1 Individuals who access, transmit, store, or delete Level 1 or Level 2 data as defined in the CSU Data Classification Standard 1 must use all reasonable efforts to prevent unauthorized access and disclosure of confidential, private, or sensitive information.
4.3 Prohibition Against Unauthorized Browsing and Monitoring

4.3.1 The CSU supports and protects the concepts of privacy and protects the confidentiality and integrity of personal information maintained in educational, administrative, or medical records. Information stored in CSU information systems may be subject to privacy laws.

4.3.2 Users must not browse, monitor, alter, or access email messages or stored files in another user's account unless specifically authorized by the user. However, such activity may be permitted under the following conditions:

a) The activity is permitted under CSU or campus policy.

b) The activity is defined in the user's job description.

c) The activity is conducted under the authority and supervision of an approved CSU official acting within his or her job responsibilities.

d) The activity is part of a classroom exercise conducted under the supervision of a faculty member. In this case, the faculty member must ensure the exercise does not result in a breach of confidentiality, availability, and integrity of CSU information assets.

e) The activity is conducted to comply with an applicable law, regulation, or under the guidance of law enforcement or legal counsel.

4.4 Responsibility of Account Owners

4.4.1 The owner or custodian of credentials, such as a username and password, that permit access to a CSU information system or network resource is responsible for all activity initiated by the user and performed under his/her credentials. The user shall assist in the investigation and resolution of a security incident regardless of whether or not the activity occurred without the user’s knowledge and as a result of circumstances outside his or her control.

4.4.2 Users must take reasonable steps to appropriately protect their credentials from becoming known by, or used by others.

a) Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining, and changing passwords.

Unless specific prior authorization has been granted, users are prohibited from:

b) Using or attempting to use the account to access, modify, or destroy CSU or non-CSU information assets for which a user is not normally authorized.

c) Disclosing passwords to any party or including passwords in documentation.

d) Embedding passwords in software code.

4.4.3 With the exception of publicly accessible CSU information assets, users must not transfer or provide access to CSU information assets to outside individuals or groups without proper authorization.

4.4.4 Users of CSU information assets must not purposefully misrepresent their identity, either directly or by implication, with the intent of using false identities for inappropriate purposes.

4.4.5 In the few instances where special circumstances or system requirements mandate that multiple users access the same account, extreme care must be used to protect the security of the account and its access password. Management of this account must conform to written or published CSU procedures designed to mitigate risk associated with shared access accounts.

4.5 Incidental Use

4.5.1 University-owned/managed information assets are provided to facilitate a person's essential work as an employee, student, or other role within the University. Use of university owned computer systems for University-related professional development or academic activities such as research or publication is permitted within the limits of system capacities.
4.5.2 Personal use of CSU information assets must be no more than "de minimis" (e.g. must have so little value that accounting for it would be unreasonable or impractical). Individuals may use CSU information assets for occasional incidental and minimal personal use provided such use:

a) Does not violate applicable laws
b) Is not in pursuit of the individual's private financial gain or advantage.
c) Does not interfere with the operation or maintenance of University information assets.
d) Does not interfere with the use of University information assets by others.
e) Does not interfere with the performance of the assigned duties of a university employee.
f) Does not result in a loss to the University.

5.0 CSU Responsibilities
5.1 The CSU has broad responsibilities with respect to protecting its information assets. These include but are not limited to controlling access to information, responding to and addressing information security incidents, complying with laws and regulations, and ensuring the logical and physical security of the underlying technology used to store and transmit information. CSU policies related to these activities are found in the Integrated CSU Administrative Manual and can be accessed at ICSUAM Section 8000.

5.2 The CSU retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CSU. The CSU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across network services; monitoring actions on information systems; checking information systems attached to the network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

6.0 Policy Enforcement
6.1 The CSU respects the rights of its employees and students. In support of the CSU Information Security policies, campuses must establish procedures that ensure investigations involving employees and students suspected of violating the CSU Information Security policy are conducted. These procedures must comply with appropriate laws, regulations, collective bargaining agreements, and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

6.2 The CSU reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of CSU resources or to protect the CSU from liability. Suspension, block or restriction to information assets in such a manner as to substantially affect the ability to complete assigned coursework or job duties shall be considered disciplinary actions subject to §6.3.

6.3 Allegations against employees that are sustained may result in disciplinary action. Such actions must be administered in a manner consistent with the terms of the applicable collective bargaining agreement and the California Education code. Student infractions of CSU Information Security policies must be handled in accordance with the established student conduct process. Auxiliary employees who violate the CSU policies may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply with CSU policies may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the CSU.

6.4 The CSU may also refer suspected violations to appropriate law enforcement agencies.

Benjamin F. Quillian
Executive Vice-Chancellor/Chief Financial Officer

Approved: November 20, 2013
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus Software</td>
<td>Software that detects or prevents malicious software.</td>
</tr>
<tr>
<td>Application</td>
<td>A software program designed to perform a specific function for a user. Applications include, but are not limited to, word processors, database programs, development tools, image editing programs, and communication programs.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of confirming that a known individual is correctly associated with a given electronic credential; for example, by use of passwords to confirm correct association with a user or account name (is a term that is also used to verify the identity of network nodes, programs, or messages).</td>
</tr>
<tr>
<td>Authorized</td>
<td>The process of determining whether or not an identified individual or class has been granted access rights to an information asset, determining what type of access is allowed; e.g., read-only, create, delete, and/or modify.</td>
</tr>
<tr>
<td>Availability</td>
<td>Ensuring that information assets are available and ready for use when they are needed.</td>
</tr>
<tr>
<td>Biometric Devices</td>
<td>An instrument intended to validate the identity of an individual through comparison of a demonstrated intrinsic physical or behavioral trait with a record of the same information previously captured. Examples: fingerprint, retina scan, voice recognition.</td>
</tr>
<tr>
<td>Business Continuity Planning</td>
<td>See CSU BCP Executive Order.</td>
</tr>
<tr>
<td>Campus</td>
<td>For the purposes of the CSU Security Program, a “campus” is any CSU campus as defined in Section 89001 of the California Education Code to include satellite locations and the Chancellor’s Office.</td>
</tr>
<tr>
<td>Campus Limited Access Area</td>
<td>Physical area such as a human resources office, data center, or Network Operations Center (NOC) that has a defined security perimeter such as a card controlled entry door or a staffed reception desk.</td>
</tr>
<tr>
<td>Campus Managers</td>
<td>Responsible for (1) specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility and (2) ensuring that program staff and other users of the information asset are</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Catastrophic Event</td>
<td>An event that causes substantial harm or damage to significant CSU information assets. Examples: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.</td>
</tr>
<tr>
<td>Computer Security Incident Response Team (CSIRT)</td>
<td>The name given to the team that handles security incidents.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C, SEC. 3542]</td>
</tr>
<tr>
<td>Control</td>
<td>Countermeasures (administrative, physical, and technical) used to manage risks.</td>
</tr>
<tr>
<td>Critical Asset</td>
<td>An asset that is so important to the campus that its loss or unavailability is unacceptable.</td>
</tr>
<tr>
<td>CSU Network</td>
<td>Any CSU administratively controlled communications network that is within the CSU managed physical space. Such networks may interconnect with other networks or contain sub networks.</td>
</tr>
<tr>
<td>Data</td>
<td>Individual facts, statistics, or items of information represented in either electronic or non-electronic forms.</td>
</tr>
<tr>
<td>Data Center</td>
<td>A facility used to house information processing or telecommunications equipment that handle protected or critical information assets.</td>
</tr>
<tr>
<td>Data Owner</td>
<td>Person identified by law, contract, or policy with responsibility for granting access to and ensuring appropriate controls are in place to protect information assets. The duties include but are not limited to classifying, defining controls, authorizing access, monitoring compliance with CSU/campus security policies and standards, and identifying the level of acceptable risk for the information asset. A Data Owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of information within that unit.</td>
</tr>
<tr>
<td><strong>Data Steward</strong></td>
<td>(also known as “Data Custodian”) An individual who is responsible for the maintenance and protection of the data. The duties include but are not limited to performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in CSU/campus security policies and standards.</td>
</tr>
<tr>
<td><strong>DMZ</strong></td>
<td>DMZ (De-Militarized Zone) is a set of one or more information assets logically located outside of a protected network that is accessible from the Internet (open to the world) with limited controlled data exchanges with the protected environment.</td>
</tr>
<tr>
<td><strong>Electronic Media</strong></td>
<td>Electronic or optical data storage media or devices that include, but are not limited to, the following: magnetic disks, CDs, DVDs, flash drives, memory sticks, and tapes.</td>
</tr>
<tr>
<td><strong>Employee</strong></td>
<td>Any person who is hired by the CSU to provide services to or on behalf of the CSU and who does not provide these services as part of an independent business.</td>
</tr>
<tr>
<td><strong>Encrypted Protocol</strong></td>
<td>An agreed-to secure means of data transmission over a network (wired or wireless).</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>The process of encoding data so that it can be read only by the sender and the intended recipient.</td>
</tr>
<tr>
<td><strong>Excessive Authority</strong></td>
<td>Assignment of a single individual to overlapping administrative or management job functions for a critical information asset without appropriate compensating controls such as added reviews or logging.</td>
</tr>
<tr>
<td><strong>Hardening</strong></td>
<td>A defensive strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td>Physical devices including, but is not limited to, portable and non-portable workstations, laptops, servers, copiers, printers, faxes, and PDAs.</td>
</tr>
<tr>
<td><strong>Information Assets</strong></td>
<td>Information systems, data, and network resources to include automated files and databases.</td>
</tr>
<tr>
<td><strong>Information Security Program</strong></td>
<td>An organizational effort that includes, but is not limited: to security policies, standards, procedures, and guidelines plus administrative, physical, and technical controls. The effort may</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information Systems</td>
<td>A combination of hardware, network and other resources that are used to support applications and/or to process, transmit and store data.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</td>
</tr>
<tr>
<td>Least Privilege</td>
<td>A concept of information security by which users and their associated applications execute with the minimum amount of access required to perform their assigned duty or task.</td>
</tr>
<tr>
<td>Logical Access</td>
<td>The connection of one device or system to another through the use of software.</td>
</tr>
<tr>
<td>Lockout Time</td>
<td>The amount of time for which logins to an account are disabled. Usually invoked once a threshold of invalid login attempts has been reached.</td>
</tr>
<tr>
<td>Malicious Software</td>
<td>Software designed to damage or disrupts information assets.</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Devices containing electronic CSU data which are easily transported. Such devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), and “smart” phones.</td>
</tr>
<tr>
<td>Network Resources</td>
<td>Resources that include, but are not limited to: network devices (such as routers and switches), communication links, and network bandwidth.</td>
</tr>
<tr>
<td>Non-public</td>
<td>A service or information intended only for the internal use of the organization.</td>
</tr>
<tr>
<td>Notice-triggerring Information</td>
<td>Specific items of personal information identified in California Civil Code Sections 1798.29 and 1798.3.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Software that is primarily or entirely concerned with controlling a computer and its associated hardware, rather than with processing work for users</td>
</tr>
<tr>
<td>Patch (Patching)</td>
<td>The installation of a software update designed to fix problems, improve usability, or enhance performance.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Personally Identifiable</td>
<td>Any information that identifies or describes an individual, including, but not limited to name, Social Security number, physical description, address, phone number, financial matters, medical or employment history (California Information Practices Act).</td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Physical Access</td>
<td>Being able to physically touch, use, and interact with information systems and network devices.</td>
</tr>
<tr>
<td>Private IP Addresses</td>
<td>Defined by Request for Comment (RFC) 1918 as range of non-routable addresses.</td>
</tr>
<tr>
<td>Protected Asset</td>
<td>Information asset containing protected data.</td>
</tr>
<tr>
<td>Protected Data</td>
<td>Level 1 and Level 2 data which are defined in the CSU Data Classification Standard. This data has been categorized according to its risk to loss or harm from disclosure.</td>
</tr>
<tr>
<td>Public Information</td>
<td>Any information prepared, owned, used or retained by a campus and not specifically exempt from disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.</td>
</tr>
<tr>
<td>Remote Access</td>
<td>Any connection from an external, non-campus network to any campus information system, data, or network resource.</td>
</tr>
<tr>
<td>Risk</td>
<td>The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>A process by which quantitatively and/or qualitatively, risks are identified and the impacts of those risks are determined. The initial step of risk management.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>A structured process which identifies risks, prioritizes them, and then manages them to appropriate and reasonable levels.</td>
</tr>
<tr>
<td>Risk Mitigation</td>
<td>Reduce the adverse effect of an event by reducing the probability of the event occurring and/or limiting the impact of the event if it does occur</td>
</tr>
<tr>
<td>Security Awareness</td>
<td>Awareness of security and controls, in non-technical terms, conveyed to motivate and educate users about important security protections that they can either directly control or be subjected to.</td>
</tr>
<tr>
<td><strong>Security Incident</strong></td>
<td>An event that results in any of the following: Unauthorized access or modification to the CSU information assets. An intentional denial of authorized access to the CSU information assets. Inappropriate use of the CSU’s information systems or network resources. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Security Training</strong></td>
<td>Specific technical understanding of how to secure the confidentiality, integrity and availability of applications, operating systems and information assets to prevent or detect security incidents</td>
</tr>
<tr>
<td><strong>Screen Filter</strong></td>
<td>An item which can be used to limit the visibility of content displayed on a computer screen to those who are immediately in front of it.</td>
</tr>
<tr>
<td><strong>System Administrator</strong></td>
<td>(also known as “System Personnel” or “Service Providers”) Individuals, who manage, operate, support campus information systems; or manage networks.</td>
</tr>
<tr>
<td><strong>Third Parties</strong></td>
<td>For the purposes of the CSU Security Program, third parties include, but are not limited to, contractors, service providers, vendors, and those with special contractual agreements or proposals of understanding.</td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>A person or agent that can cause harm to an organization or its resources. The agent may include other individuals or software (e.g. worms, viruses) acting on behalf of the original attacker.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>Anyone or any system which accesses the CSU information assets. Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>A flaw within an environment which can be exploited to cause harm.</td>
</tr>
</tbody>
</table>
| **Asymmetric Cryptosystem** | A computer algorithm or series of algorithms which utilize two different keys with the following characteristics
- one key signs or decrypts content;
- one key verifies or encrypts content; and,
- the keys have the property that, even when one key is known, it is computationally infeasible to discover the other key. |
| **Asymmetric Key-Pair** | A private key and its corresponding public key in an asymmetric cryptosystem. Public keys can be used to verify a digital signature created with the corresponding private key and to encrypt content. |
| **Digital Certificate** | Also known as a public key certificate or identity certificate, a digital certificate is an electronic document which uses a digital signature to bind a public key with an identity, such as the name of a person or an organization and address. The certificate can be used to verify that a public key belongs to a person. |
| **Private Key** | The secret key of a key pair used to create a digital signature or decrypt data. |
| **Public Key** | The well-known key of a key pair used to verify a digital signature or to encrypt data. |
| **Public Key Cryptography** | An encryption method that uses an asymmetric key-pair. |
| **Signature Dynamics** | A measurement of the way a person writes his or her signature by hand on a flat surface, binding the measurements to a message through the use of cryptographic techniques. |
May 23, 2018

MEMORANDUM

TO: CSU Presidents
FROM: Timothy P. White
Chancellor

SUBJECT: The California State University Board of Trustees Policy on Disability Support and Accommodations – Executive Order 1111

Attached is a copy of Executive Order 1111 relating to disability support and accommodations, which supersedes Executive Order 926.

In accordance with policy of the California State University, the campus president has the responsibility for implementing executive orders where applicable and for maintaining the campus repository and index for all executive orders.

Questions should be addressed to the appropriate division within the Office of the Chancellor as specified in the appropriate section of this executive order.

TPW/LH/tl

Attachment

c: CSU Office of the Chancellor Leadership
Provosts and Vice Presidents, Academic Affairs
Vice Presidents, Administration and Finance
Vice Presidents, Student Affairs
Chief Information Officer/Technology Officers
Human Resources Officers
Associate Vice Presidents, Faculty Affairs
Discrimination, Harassment, Retaliation Administrators
Disability Leave Coordinators
Directors of Services to Students with Disabilities
Executive Facilities Officers
THE CALIFORNIA STATE UNIVERSITY
Office of the Chancellor
401 Golden Shore
Long Beach, California 90802-4210
(562) 951-4400

Executive Order: 1111
Effective Date: May 23, 2018
Supersedes: Executive Order 926
Title: The California State University Board of Trustees Policy on Disability Support and Accommodations

I. Policy Statement

The California State University (CSU) is committed to providing a diverse and supportive academic and work environment that facilitates learning, teaching, working and conducting research for all students, employees and visitors. It is CSU policy to ensure that individuals with disabilities shall have equal access to and the opportunity to participate in CSU programs, activities and services.

The CSU will provide access, support and accommodation to individuals with disabilities in compliance with the California Fair Employment and Housing Act (FEHA), Government Code Section 12920 et seq., the Americans with Disabilities Act of 1990, as amended, (ADA) 42 U.S.C. 12101 et seq., and Sections 504 and 508 of the Rehabilitation Act of 1973, 29 U.S.C. Section 701 et seq.

This policy applies to all CSU campuses and to the Office of the Chancellor. It applies, but is not limited to, academic programs and services, student services, human resources services, information resources and technologies, procurement of goods and services, and capital planning, design, and construction. Auxiliaries who operate on the university’s campuses are required to comply with this executive order.

II. Policy Compliance and Monitoring

A. The Chancellor’s Office maintains CSU systemwide policies and procedures that allow applicants for employment, employees, students, volunteers, independent contractors, vendors, and other members of the public to file complaints through CSU Executive Orders 1096 and 1097 Revised and successors for discrimination, harassment and retaliation based on a protected status, including disability. Campuses are required to ensure that such policies and procedures are posted on appropriate websites and that information regarding these policies and procedures are accessible and available to all students, employees, and visitors.
B. Each campus shall designate an employee to coordinate compliance with the ADA and this executive order. Campuses shall provide the contact information for this employee on campus websites.

C. Each campus and the Chancellor’s Office shall provide funding, resources, and training to members of its campus community to ensure compliance with this executive order. CSU campuses and the Chancellor’s Office may consult with Systemwide Professional Development in the Human Resources Division of the Chancellor’s Office for assistance in locating available resources and tools that will meet campus-specific needs.

D. Each campus and the Chancellor’s Office shall consult with the Office of General Counsel when issues arise regarding compliance with laws, regulations, and policy concerning disability support and accommodation.

III. Physical Access

The CSU will ensure that individuals with disabilities have access to CSU programs, services and activities required by FEHA, the ADA and Sections 504 and 508 of the Rehabilitation Act of 1973.

A. The Board of Trustees of the CSU is granted full authority and responsibility for the development, construction, and improvement of buildings and facilities on CSU campuses (California Education Code §66606).

B. New CSU construction is required to be designed and constructed in compliance with the accessibility standards described within the California Building Standards Code (Code) and the federal ADA guidelines. CSU shall obtain certification of design plans for major capital construction projects from the California Department of General Services, Division of the State Architect (DSA), or as otherwise may be specified by statute. For minor capital projects CSU shall review and ensure the design plans conform to access compliance code. The CSU shall ensure that construction projects are built according to CSU approved design plans.

C. Major capital projects shall be reviewed by a Certified Access Specialist (CASp), and findings shall be resolved prior to project close out and filing of the Notice of Completion (for each respective project).

D. Each campus shall assess existing architectural/physical barriers and conditions at variance with current California Code to identify steps to ensure program accessibility to individuals with disabilities. Each campus and the Chancellor’s Office shall prioritize the removal of physical barriers to access. Physical barrier removal may be funded through the capital outlay program for building renovations, minor capital projects, and building demolition, and from campus reserves.
E. The CSU is not required to make structural changes or remove current architectural/physical barriers as long as access to all programs, activities and services is provided in compliance with applicable state and federal law.

F. Pursuant to California Education Code § 67301(c), each campus and the Chancellor’s Office shall conduct biennial audits of parking spaces to determine whether spaces designated for use by individuals with disabilities comply with state building code requirements. California Code of Regulations, Title 24, Part 2, Volume 1 (California Building Code).

Following each biennial audit, each campus shall submit a parking audit report, which documents the audit findings and any actions taken as a result of the audit, to Systemwide Capital Planning, Design, and Construction. Each campus and the Chancellor’s Office shall retain a copy of the parking audit report until the next audit is completed.

IV. Information Resources and Technology Access

The CSU is required to make electronic and information technology accessible to all students, employees and the general public, including those individuals with disabilities. “Accessible” means a person with a disability is afforded the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services as a person without a disability in an equally effective and equally integrated manner, with substantially equivalent ease of use.

A. Information and Communication Technology access applies to all CSU programs, services, and activities provided to all students, staff, faculty, and the general public. This encompasses all technology products used to deliver academic programs and services, student services, information technology services, and auxiliary programs and services. Technology access for all students, staff, faculty, and the general public must provide comparable functionality, affordability, and timeliness.

B. The Academic and Student Affairs Division of the Chancellor’s Office, in consultation with the Office of General Counsel and campus stakeholder groups, shall issue and update compliance procedures in the form of Coded Memoranda.

The Coded Memoranda will address planning and implementation procedures, and will include reporting requirements that will measure the access to electronic and information technology by individuals with disabilities.

C. Ensuring accessibility is a shared responsibility and requires a coordinated, ongoing campus wide and systemwide effort to ensure its success. Toward that end:

1. Each campus president and the chancellor are responsible for the establishment and implementation of accessible electronic information and technology programs that have adequate administrative support and necessary resources to achieve the goals of the Accessible Technology Initiative (ATI).
2. Each campus president and the chancellor will appoint an Executive Sponsor to manage the ATI implementation at their institution.

3. The ATI Executive Sponsor shall be responsible for convening a campus ATI Steering Committee to ensure compliance with procedures in Coded Memoranda issued by the Academic and Student Affairs Division of the Chancellor's Office.

4. The CSU campuses and the Office of the Chancellor shall strive towards implementing Universal Design concepts and strategies which will reduce the need for, and costs associated with, individual accommodations for inaccessible technology products.

5. The CSU Office of the Chancellor has established the ATI to plan and support the implementation of universal access to Information and Communication Technology.

V. Disability Support and Accommodation for Students

The CSU is required to provide accommodations and support services to students with disabilities in accordance with Section 504 of the Rehabilitation Act of 1973 (Section 504) and the ADA. In addition, Section 504 and the ADA prohibits the University from discriminating against a person who has a disability which substantially limits one or more major life activity or is regarded as having such an impairment.

A. The Academic and Student Affairs Division of the Chancellor’s Office, in consultation with the Systemwide Advisory Committee for Services to Students with Disabilities, shall develop and maintain procedures to accommodate students with disabilities. These procedures shall be provided to students and prospective students and posted on the CSU Chancellor’s Office website and on the website of each CSU campus.

B. The CSU is required to conduct an interactive process with a student with a disability to assess the functional impact of a person’s disability and to identify reasonable accommodation(s) so the student has the opportunity to participate in University programs and activities in ways that are equal to that afforded others. While the CSU is not required to provide an accommodation requested by the student, the CSU must allow the student the same benefits and opportunity to reach the level of achievement provided to others. Further, the CSU may not charge the student for the cost of providing any reasonable accommodation, regardless of whether the program is state or self-supported.

C. The CSU has the right to maintain admission, academic, and conduct standards. A reasonable accommodation cannot result in a fundamental alteration to an academic program, course or activity.
D. Each campus is required to develop and maintain a written procedure by which a student with a disability may appeal a CSU determination to deny a specifically requested modification or accommodation. Each campus shall post the procedure for this appeal on the website of the office providing services to students with disabilities and shall ensure that this procedure is accessible to students with disabilities. It is recommended that campuses consult with CSU legal counsel in connection with student appeals.

E. Each campus shall maintain an office to provide specialized support and services to students with disabilities and a website to provide students with disabilities with information regarding available resources and accommodations as well as the procedure by which students may obtain these resources and accommodations.

F. Disability support services may include reasonable academic modifications and physical accommodations for students with disabilities.

G. Students with verified disabilities may receive a parking fee waiver based on financial need. The Student Financial Aid Department shall evaluate and certify a student’s financial need meets the requirement for a parking fee waiver.

VI. Disability Support and Accommodation in Employment

In accordance with the Americans with Disabilities Act (ADA) and the Fair Employment and Housing Act (FEHA), the CSU shall provide reasonable accommodations to employees with disabilities and to applicants with disabilities, unless doing so would impose an undue hardship on the University’s operations.

A. Each campus and the Chancellor’s Office shall maintain, and post on its Human Resources website, a written procedure by which applicants for employment and employees with disabilities may request and receive reasonable accommodations to allow them to apply for vacant positions and/or perform their job duties. This document should include a description of the interactive process.

B. Each campus and the Chancellor’s Office shall engage in a timely, good faith, interactive process with employees or applicants with disabilities to determine effective reasonable accommodations, if any, in response to a request for a reasonable accommodation.

C. Each campus and the Chancellor’s Office shall maintain the confidentiality of an employee’s request for reasonable accommodation of a disability. Documentation of the employee’s request for disability accommodation, medical verification, the interactive process and any associated procedures shall not be maintained in the employee’s personnel file but in a separate, distinct and secure location.

VII. Disability Support and Accommodation in Contracting

Any public solicitation process developed by a campus or the Chancellor’s Office shall be compliant with regulations and guidelines issued pursuant to ADA and California
Government Code § 11135, and shall not deny individuals with disabilities the opportunity to participate in the competition for the award of a contract.

VIII. Definitions

A. Accessible: means a person with a disability is afforded the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services as a person without a disability in an equally effective and equally integrated manner, with substantially equivalent ease of use.

B. Accessible Technology Initiative (ATI): CSU’s ongoing commitment to make information technology resources and services accessible to all CSU students, faculty, staff and the general public regardless of disability.

C. Disability:  
For employees and students, as defined in California Government Code § 12926 and California Education Code § 66260.5 means:
1. Having a physical or mental condition that limits a major life activity.  
   “Limits” means making the achievement of a major life activity difficult.  
   “Limits” is determined without regard to mitigating measures such as medications, assistive devices, prosthetics, or reasonable accommodations, unless the mitigating measure itself limits a major life activity. A “major life activity” is broadly construed and includes physical, mental, and social activities (such as walking, talking, seeing, hearing) and working; or
2. Having a known history of a qualifying impairment; or
3. Being regarded or treated as having or having had a qualifying impairment; or
4. Being regarded or treated as having or having had such an impairment that has not presently disabling effects but may become a qualifying impairment in the future.

D. Discrimination: an adverse action taken against an employee, third party or student by the CSU, a CSU employee or a student, because of a protected status.

E. Essential Functions: means the fundamental job duties of the employment position the individual with a disability holds or desires. “Essential functions” does not include the marginal functions of the position. A job function may be considered essential for any of several reasons, including, but not limited to, any one or more of the following:
1. The function may be essential because the reason the position exists is to perform that function,
2. The function may be essential because of the limited number of employees available among whom the performance of that job function can be distributed, and/or
3. The function may be highly specialized, so that the incumbent in the position is hired based on expertise or the ability to perform a particular function.
F. **Individual with a disability:** refers to:
   1. Any person who has a physical or mental impairment that limits one or more of the major life activities of such individual,
   2. Any person who has a record of such impairment, or
   3. Any person who is regarded as having such impairment.

G. **Information and Communication Technology:** this term encompasses electronic information and technology that includes, but is not limited to, the internet and intranet websites, web applications including mobile, content delivered in digital form, electronic books and electronic book reading systems, search engines and databases, learning management systems, classroom technology and multimedia, personal response systems ("clickers"), and office equipment such as classroom podiums, copiers and fax machines. It also includes any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, creation, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This term includes telecommunications products (such as telephones), information kiosks, Automated Teller Machines (ATMs) transaction machines, computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

H. **Interactive process:**
   *For employees:* a requirement under the ADA and FEHA for employers and employees to communicate to identify the limitations resulting from an employee’s disability and potential reasonable accommodations that could overcome those limitations.

   *For students:* collaborative process between the student and the university to determine reasonable accommodations that provide equitable opportunity for the student to participate in, while not fundamentally altering the CSU’s courses, programs, services, and activities.

I. **Reasonable accommodation:** a modification or adjustment to a job, the work environment, academic program, existing facilities, or the way things usually are done that enables a qualified individual with a disability to enjoy an equal employment where the individual may continue performing the essential functions of the job or academic opportunity to continue to complete assignments and participate fully in course work.

---

Timothy P. White, Chancellor

Dated: May 23, 2018
Resources

The following policies, contracts, executive orders, and manual define the mandates and support the intent of Executive Order 1111.

Academic Programs, Services and Activities


Human Resources


- Procedures in collective bargaining agreements available for each bargaining unit: [http://www.calstate.edu/hr/employee-relations/bargaining-agreements/](http://www.calstate.edu/hr/employee-relations/bargaining-agreements/)


- Compliance Training: [https://csyou.calstate.edu/divisions-orgs/hr/spd/compliance-training/Pages/default.aspx](https://csyou.calstate.edu/divisions-orgs/hr/spd/compliance-training/Pages/default.aspx)

Information Resources and Technologies

- Information technology resources as governed by California state law: [http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=11135](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=11135)

- Accessible Technology Initiative (ATI) website: [http://teachingcommons.cdli.edu/access/index.html](http://teachingcommons.cdli.edu/access/index.html)

• Accessible Technology Initiative (Coded Memorandum AA-2013-03): http://www.calstate.edu/AcadAffi/codedmemos/AA-2013-03.html

• Section 5228.00 Accessibility of Public Solicitations and Acquisition of Electronic and Information Technology (E&IT) Goods and Services (Effective 9/25/2016): https://csyou.calstate.edu/Policies/icsuam/FinalPDF/Section%205000%20PDF/Section5000.pdf

• Information and Technical Assistance on the Americans with Disabilities Act (ADA): https://www.ada.gov/access-technology/

Physical Access

• State University Administrative Manual (SUAM): www.calstate.edu/CPDC/SUAM

Contracts and Procurement

• Non-Discrimination Policy (Section 5220 of the Integrated CSU Administrative Manual) https://csyou.calstate.edu/Policies/icsuam/FinalPDF/Section%205000%20PDF/5220-00.pdf
The California State University
System-wide Information Security Standards Document

Contact:
Janice Lim
Senior Director for Information Security Management
California State University, Chancellor’s Office

6 May 2008

Developed by:
CH2M HILL
# Table of Contents

1.0 Introduction ......................................................................................... 1

2.0 Scope .................................................................................................. 1

3.0 Standards Management ....................................................................... 1

4.0 Glossary ............................................................................................. 1

5.0 Information Security Roles and Responsibilities .............................. 2

   5.1 Campus President ........................................................................... 2

   5.2 Chief Information Officer (CIO) ................................................... 2

   5.3 Information Security Officer (ISO) .............................................. 2

6.0 Risk Management ............................................................................... 3

   6.1 Risk Assessment ............................................................................ 3

   6.2 Risk Management Plan ................................................................. 5

7.0 Acceptable Use .................................................................................. 5

8.0 Personnel Security ............................................................................. 5

   8.1 Termination and Position Change ............................................... 5

   8.2 Personnel Vetting ......................................................................... 6

9.0 Privacy ............................................................................................... 6

   9.1 Web Site Privacy Notice ............................................................... 6

10.0 Security Awareness and Training .................................................... 7

   10.1 Content ....................................................................................... 7

   10.2 Awareness and Training Activities ............................................. 7

11.0 Third Party Services Security ......................................................... 8

   11.1 Third Party Users of CSU Resources .......................................... 8

   11.2 Contracted Relationships ........................................................... 8

12.0 Information Technology Security .................................................... 9

   12.1 Network Controls Management ............................................... 9

   12.2 Remote Access ........................................................................... 10

   12.3 Mobile Device Management .................................................... 10

   12.4 Boundary Protection and Isolation ......................................... 10

   12.5 Malicious Software Protection .............................................. 11

   12.6 Logging Elements ..................................................................... 11

   12.7 Intrusion Detection and Prevention ....................................... 12

   12.8 Secured Infrastructure ............................................................ 12

13.0 Configuration Management and Change Control ......................... 12

   13.1 Change Control ......................................................................... 12

   13.2 Resource Inventory Management ............................................ 14

14.0 Access Control ................................................................................ 14

   14.1 User Account Credentials Management .................................. 14

   14.2 Password Management ............................................................. 15

   14.3 Encryption ............................................................................... 15

   14.4 User Privilege Authorization and Management ....................... 16
# Table of Contents

15.0 Asset Management .......................................................... 16  
  15.1 Data Classification .................................................... 16  
  15.2 Data Handling ......................................................... 19  
  15.3 Data Retention ........................................................ 19  
  15.4 Data Disposal .......................................................... 19  

16.0 Management of Information Systems ................................ 19  
  16.1 Development Management ........................................ 19  
  16.2 Web Application Coding ........................................... 20  
  16.3 Database Coding ..................................................... 20  
  16.4 Life Cycle Management ............................................. 20  

17.0 Information Security Incident Management ....................... 21  
  17.1 Evidence Collection and Handling ............................... 21  
  17.2 Reporting .............................................................. 21  

18.0 Physical Security .......................................................... 22  
  18.1 Security Zones ........................................................ 22  
  18.2 Work Area Security .................................................. 23  

19.0 Business Continuity and Disaster Recovery ....................... 23  

20.0 Legal and Regulatory Compliance ................................... 23  
  20.1 PCI ................................................................. 23  
  20.2 HIPAA ............................................................. 23  

Appendix A – Initial List of Standards .................................... 24
1.0 Introduction

The California State University (CSU) is a public institution committed to the ideals of academic freedom and freedom of expression. To promote these ideals, the CSU uses and offers access to a variety of information systems, data, and network resources, hereafter referred to as information assets. These standards support and provide additional guidance for those implementing The California State University System-wide Information Security Policy. The unauthorized collection, modification, deletion, disclosure, or misuse of CSU information assets can compromise the mission of the University, violate individuals’ rights to privacy, or constitute a criminal act.

The CSU is committed to protecting the confidentiality, integrity, and availability of information assets entrusted to the University. This policy and associated standards provide direction and support to campuses for information security in accordance with university requirements, and relevant laws and regulations.

2.0 Scope

In support of The California State University System-wide Information Security Policy, these standards have the same scope of applicability.

These standards may be supplemented, but not superseded, by additional standards adopted by each campus. These standards must be regularly reviewed and revised as necessary in order to ensure that it meets the CSU information security goals and requirements.

3.0 Standards Management

These standards may be updated to reflect changes in the CSU’s academic, administrative, or technical environments, or applicable state, federal, or international laws and regulations. The CSU’s Senior Director for Information Security Management shall be responsible for reviewing and updating this document.

4.0 Glossary

Refer to the Glossary in The California State University System-wide Information Security Policy for an applicable list of terms and definitions.
5.0 Information Security Roles and Responsibilities

5.1 Campus President

Each CSU campus president must establish an information security program which is compliant and consistent with the CSU system-wide information security policy and standards. The details of each campus program is left to the president to determine, with the exception of items identified in the CSU information security policy and standards, which are meant to provide some degree of consistency of approach and application.

Each president (or his designee) must appoint an Information Security Officer (ISO).

The president (or his designee) must identify the specific duties and responsibilities for the ISO which, at a minimum, include those items identified below.

While the role of ISO may be an additional duty, the president must ensure the appointee has sufficient time to carry out the assigned duties and responsibilities.

Each president must review information security risks on at least annually.

Each president must annually report his or her current risk posture to the Chancellor’s Office and to the Board of Trustees in accordance with the Risk Management section of the policy and standards.

5.2 Chief Information Officer (CIO)

In addition to other duties as defined within the CSU, each campus CIO must:

- Work with the campus ISO regarding changes in the campus programs and systems to understand potential changes in risk.
- Consult with the ISO regarding campus operations and operations security.
- Work with the ISO to develop procedures and processes which implement the CSU information security policy and standards as directed by the campus president.

5.3 Information Security Officer (ISO)

The ISO must:

- Be the primary advisor to the president and his cabinet on all information security matters.
- Coordinate the campus information security program on behalf to the president.
- Work closely with campus administrators and executive officers on information security matters.
- Inform the president (or his designee) of high significant risks as they are identified.
- Serve as the campus representative on the CSU Information Security Advisory Committee.
- Oversee the campus information security awareness and training program.
- Oversee campus information security self-assessment activities.
- Oversee the campus information security incident response program coordinating among appropriate campus personnel.
- Provide inputs to the campus budget process regarding prioritization and required resources for security risk mitigation activities and inputs regarding security risks of other proposed projects.
6.0 Risk Management

6.1 Risk Assessment

Each campus must regularly perform a formal, documented risk assessment process that assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of campus’ information systems, data, or network resources.

At a minimum, each campus’ risk assessment process must include the following:

- Identification and prioritization of the threats to campus information systems, data, and network resources.
- Identification and prioritization of the vulnerabilities of campus information systems, data, and network resources.
- Identification and definition of current security measures used to protect the confidentiality, integrity, and availability of campus information systems, data and network resources.
- Assessment of the likelihood that a particular threat will exploit specific vulnerabilities on campus information systems, data and network resources.
- Identification of the potential impacts to the confidentiality, integrity, and availability of campus information systems, data, and network resources if a particular threat exploits a specific vulnerability.

Campuses must establish and document a method for categorizing and assessing identified risks. While each campus may identify their own methods, an example follows:

Likelihood of Occurrence

*High* – A threat is highly motivated and sufficiently capable, and controls to prevent a vulnerability from being exercised are ineffective.

*Medium* – A threat is motivated and capable, but controls are in place that may impede successful exercise of a vulnerability.

*Low* – A threat lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, a vulnerability from being exercised.

Magnitude of Impact

*High* – Exploitation of a vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede a campus’ mission, reputation, or interest; or (3) may result in human death or serious injury.

*Medium* – Exploitation of a vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury.

*Low* – Exploitation of a vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization’s mission, reputation, or interest.

The risk assessment must be conducted per the guidelines and process defined in NIST SP800-30 “Risk Management Guide for Information Technology Systems”. The process is outlined in Figure 1.
6.2 Risk Management Plan

Each CSU campus must develop and regularly update a formal, documented, risk management plan that addresses at a minimum:

- Scope
- Roles and responsibilities
- Campus leadership commitment
- Risk identification and tracking methodology
- Third party risk management
- Characterization of the campus' information systems based on their function and criticality

This plan does not have to be a separate document and may be combined with other campus planning documentation.

Each campus ISO must review the information security risks on at least annually. Significant risks must be presented to the campus president (or his designee) for his action or acceptance.

Each campus must develop and maintain a Plan of Action and Milestones (POAM) that describes campus information security initiatives. For each initiative, the POAM should at least contain:

- Identified Driving Risk(s)
- Proposed Initiative
- Initiative Owner/POC
- Resources Required
- Planned Completion
- Interim Milestones
- Status

On an annual basis, each campus president must submit an Information Security Risk Management Report to the Chancellor's Office and to the Board of Regents. This report must identify the significant risks which have been identified during the past year, which ones have been accepted, and which ones are in the process of being mitigated. This report may be combined with other required risk-related reports.

The CSU Senior Director for Information Security Management (SDISM) must develop the format and process for the Information Security Risk Management Report.

7.0 Acceptable Use

No standards defined at this time. The Policy will be supported by awareness training and campus specific guidelines.

8.0 Personnel Security

8.1 Termination and Position Change

Appropriate CSU or campus managers must promptly notify the appropriate human resources department and information technology (IT) group responsible for granting and revoking access privileges about all
employee terminations and job changes. If an employee is being terminated, the employee’s manager must ensure that the employee’s access privileges (logical and physical) are terminated by the employee’s last day of employment. If an employee is changing jobs, it is the responsibility of the employee’s new manager (if the job change involves a management change) or existing manager to identify and define the access privileges needed by the employee to perform their new job.

By the last day of employment, employees must return all campus and/or CSU supplied access devices to their manager. If an employee has used cryptography on data belonging to CSU and/or a campus, they must provide the cryptographic keys to their manager by their last day of employment.

A monthly report must be forwarded to each campus’ ISO by the appropriate Human Resources (HR) department that lists all campus employee terminations and job changes during the month and confirmation that logical and physical access privileges have been appropriately revoked or changed.

### 8.2 Personnel Vetting

Early in the process of defining a position, both the appropriate campus or CSU HR department and the hiring manager must identify and address the information security responsibilities of the position.

Each campus must ensure that accurate job descriptions are kept to up-to-date with employee responsibilities. The descriptions must indicate classifications of risk associated with any protected data or information systems managed by the employee.

Each campus must identify and define “positions of trust” within its campus that requires vetting of the employees who are in the positions. Positions of trust typically involve significant access to campus information systems which contain protected data. Vetting failure criteria for such positions must be formally defined.

Appropriate vetting must be performed on all new employees or contractors appointed to positions of trust. As appropriate, the vetting can include local criminal, national criminal, credit, education, and/or reference checks. Background check updates on existing employees in positions of trust must be performed at least every three years.

### 9.0 Privacy

#### 9.1 Web Site Privacy Notice

Consistent with the California Online Privacy Protection Act of 2003, each web site operated by a CSU campus must conspicuously post a privacy policy on that web site.

A privacy policy is considered conspicuously posted on a web site when:

- The privacy policy appears on the homepage of the web site.
- The privacy policy is directly linked to the homepage via an icon that contains the word “privacy,” and such icon appears in a color different from the background of the homepage.
- The privacy policy is linked to the homepage via a hypertext link that contains the word “privacy,” is written in capital letters equal to or greater in size than the surrounding text, is written in a type, font, or color that contrasts with the surrounding text of the same size, or is otherwise distinguishable from surrounding text on the homepage.
At a minimum, each privacy policy must contain at least the following features:

- A list of the categories of personally identifiable information the operator collects.
- A list of the categories of third parties with whom the operator may share such personally identifiable information.
- A description of the process (if any) by which the user can review and request changes to his or her personally identifiable information collected by the operator.
- A description of the process by which the operator notifies users of material changes to the operator’s privacy policy.
- The effective date of the privacy policy.

10.0 Security Awareness and Training

10.1 Content

Each campus’ information security awareness and training program must include, but is not limited to:

- All appropriate CSU and campus information security policies and standards.
- Significant campus information security controls or processes.
- User responsibilities and required actions.
- The secure use of campus information systems, data, and network resources (e.g., log-on procedures, allowed protocols).
- Likely security threats to campus information systems, data and network resources.
- CSU and the campus’ legal and regulatory responsibilities for protecting information systems, data and network resources.
- Information security best practices (e.g., how to construct a good password, how to prevent computer viruses).

10.2 Awareness and Training Activities

Each campus’ ISO and/or other managers designated by the campus president, will be responsible for developing and coordinating the campus’ information security awareness and training program. At a minimum, each campus’ program must include:

- Annual review with a refresh of content if necessary.
- Yearly acceptable use awareness activity for students.
- Information security awareness training for new employees within a timeframe established by each campus.
- Basic information security awareness refresher for all campus employees who interact with campus information systems, data, or network resources occurring at least every two years.
- Advanced information security training for privileged users (e.g., system and security administrators) who interact with information systems containing protected data occurring at least every two years.
- Advanced information security training for the ISO and other managers who are responsible for developing and coordinating the campus’ information security program and controls occurring at least every two years.
Ongoing security awareness outreach for all persons who use or access the campus’ information systems, data, or network resources. Information security awareness and training activities must be recorded and available for audit.

11.0 Third Party Services Security

11.1 Third Party Users of CSU Resources

The campus president must ensure that all users of campus information technology services have an established relationship which is consistent with the type and sensitivity of resources being used.

Examples:

1. Users of a public kiosk have an informal relationship defined by the placement of the kiosk with certain capabilities in a public space.
2. Users of CSU resources to contact alumni for fundraising have a relationship established by their participation in a group conducting the fundraising and that group’s relationship to the CSU campus.

All users accessing protected information must have a documented relationship with the associated CSU campus.

11.2 Contracted Relationships

Descriptions or Statements of Work must:

- Clearly state the security requirements for the vendors to ensure that their work is consistent with the CSU security policy and standards.
- Require the compliance with the CSU security policy and standards. Exceptions may only be granted by the campus president and must be reported to the Senior Director for Information Security Management.
- Include a clear description of the scope of services provided under the contract or purchase order.
- Clearly identify any and all types of protected data to be exchanged and managed by the vendor.
- Identify incident reporting requirements.
- Require immediate notification of any security breaches associated with protected information.
- Require notification within three days of any security breaches associated with all other information.
- Make provisions for CSU to have the ability to inspect and review vendor operations for potential risks to CSU operations or data.

Where practical, CSU contracting office must develop and incorporate common language addressing this standard into contract templates.
12.0 Information Technology Security

12.1 Network Controls Management

Each CSU campus must develop and maintain documentation on its network structure and configuration. At a minimum, the following information must be included:

- IP address management
  - Static IP addresses assignments
  - Dynamic address server (i.e., DHCP) settings showing:
    - Range of IP addresses assigned
    - Subnet mask, default gateway, DNS server settings, WINS server settings assigned
    - Lease duration time

- Network topology information containing:
  - The locations and IP addresses of all segments, subnets, and VLANs.
  - Identification of any established security zones on the network and devices that control access between them.
  - The locations of every network drop and the associated switch and port on the switch supplying that connection.
  - All subnets on the network and their relationships including the range of IP addresses on all subnets and netmask information.
  - All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices. A summary representation (e.g., drawing) of the logical design appropriate for managerial discussions.

- Configuration information on at least the following network devices:
  - Switches
  - Routers
  - Firewalls

- Configuration should include but not be limited to:
  - IP address
  - Netmask
  - Default gateway
  - DNS server IP addresses for primary and secondary DNS servers
  - Any relevant WINS server information

- Network connection information including:
  - Type of connection to the Internet or other WAN/MAN, including T1, T3, and frame relay.
  - Provider of Internet/WAN/MAN connection and contact information for sales and support.
  - Configuration information including netmask, network ID, and gateway.
  - Physical location of where the cabling enters the campus and circuit number.

Each campus may determine its specific methods for documentation using any combination of online network tools, databases, or hard copies; however, the resulting information must be in a form and format which is available for audit and review. Each campus must establish a method for self-review of network documentation such that each element is reviewed for accuracy and completeness at least once a year.
12.2 Remote Access

All remote access (wired or wireless) to non-public campus information systems, data, and network resources must be authenticated and authorized.

All remote access (wired or wireless) to non-public campus information systems, data, or network resources must pass through a campus-approved access control device (e.g., a firewall or access server).

All campus access control devices that allow remote access to non-public campus information systems, data or network resources must be capable of tracking and logging user activity consistent with documented campus procedures and processes for logging. All remote access to non-public campus information systems, data, and resources must be a secure encrypted protocol requiring unique user authentication such as a virtual private network (VPN).

Remote access to non-public CSU-shared resources (e.g., CMS) must, at a minimum, meet the same access criteria describe above for campus information systems and data.

Campuses must identify and communicate approved user practices for remote connections.

Campuses must identify and communicate approved methods and protocols for remote access.

Campuses must identify and communicate a process for user reporting of suspected compromise of their remote device.

Campuses mechanisms for remote access must include an appropriate method for terminating inactive or inappropriate remote connections.

12.3 Mobile Device Management

Each campus must maintain an inventory of authorized mobile devices which may contain protected data.

Campuses must provide a method for encrypting Level 1 protected data on authorized mobile devices.

Campuses must identify and communicate approved user practices for mobile device security.

As determined necessary by risk assessment, campus-provided mobile devices must be protected with appropriate security controls. Appropriate security controls can include, but are not limited to: access control, encryption, strong passwords, anti-virus software, and/or personal firewall.

Level 1 protected data must not be stored on a mobile device unless it is encrypted.

Campuses must identify and communicate a process for user reporting if they determine or suspect that their campus provided mobile device or a non-campus-provided (i.e., personal) mobile device which enables access to non-public campus information systems, data or network resources has been lost, stolen, or compromised.

12.4 Boundary Protection and Isolation

Each campus’ networks must be protected at all ingress and egress points by a device(s) which only permits authorized inbound and outbound traffic; all other traffic must be blocked. Campus Internet reachable information systems (i.e., web servers) must be deployed in a demilitarized zone (DMZ) that controls both ingress and egress from the Internet. A network access control device must be placed between any DMZ and a campus’ internal network.
Campuses must establish zoning or separation within its internal networks based on established trust relationships, authorized services, and data classification.

All unnecessary services (e.g., web server, SNMP) on any campus border device must be disabled. All management connections across a network to campus border devices must be encrypted and authenticated. Direct management connections (i.e., console connections) do not need to be encrypted. Each campus must develop and implement controls to filter and limit unsolicited e-mails (e.g., spam).

Each campus must have a formal, documented process for approving and testing configuration changes to its network and network control devices. Each campus must have formal, documented network configurations that define all open ports and services. All allowed services must have documented justification. Any risky protocols allowed (e.g., FTP or telnet) by a campus border device must be justified and documented. Border device configurations and rule sets must be reviewed and revised, as necessary, at least annually.

12.5 Malicious Software Protection

All campus information systems commonly affected by malicious software must have current versions of campus approved anti-virus software installed on them. Such software must be capable of detecting, removing, and protecting against malicious software including spyware and adware.

Such software must scan all data in “real time”, including data, which is both stored and received by the information system. Such scanning must take place before data files are opened and before software is executed. The software must be capable of tracking and reporting significant actions taken by the software.

Anti-virus software and signatures must be regularly updated.

Campuses must identify hardening guidelines for critical servers.

12.6 Logging Elements

Each campus must identify and implement appropriate logging and monitoring controls for its information systems, data, and network resources. These controls must take into consideration the technical capabilities of each resource. At a minimum and as appropriate, such controls must track and log the following events:

- Actions taken by any individual with root or administrative privileges
- Changes to system configuration
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Alarms raised by an access control system
- Activation and de-activation of controls, such as anti-virus software or intrusion detection system.
- Changes to, or attempts to change system security settings or controls

For each of the above events, the following must be recorded, as appropriate:

- User identification
- Type of event
- Date and time
- Success or failure indication
• Data accessed
• Program or utility used
• Origination of event (i.e., network address)
• Protocol
• Identity or name of affected data, information system or network resource

Each campus must establish procedures for the retention of log and monitoring information which must be consistent with any CSU data retention schedules and must take into consideration cost-effectiveness.

Each campus must establish methods for time synchronization of logging and monitoring activities.

12.7 Intrusion Detection and Prevention

<<Placeholder for May ISO meeting discussions>>

12.8 Secured Infrastructure

Public network jacks or wireless access points (WAP) at campuses must be isolated from internal campus information systems, data and network resources. Network jacks or WAPS that provide access to non-public campus information systems, data, network resources, segments or VLANs must not be made physically available in public areas of campuses.

13.0 Configuration Management and Change Control

13.1 Change Control

Changes to campus information systems, data, and network resources must be made in accordance with a formal, documented change control process. The process must include:

• Identification of a change control authority which may be vested in either individuals or groups as appropriate.
• Identification and documentation of significant changes.
• Assessment of the potential impact, including security implications, of significant changes.
• Methods for scheduling and appropriate notification of significant changes.
• Methods for notification of any changes to critical systems.
• Ability to terminate and recover from unsuccessful changes.
• Testing procedures to ensure the change is functioning as intended.
• Communication of completed change details to all appropriate persons.
• The updating of all appropriate system documentation upon the completion of a significant change.

Significant changes made to a common or shared CSU information system, data, or network resource (e.g., CMS) must be appropriately reviewed and approved by a centralized CSU change control oversight group.

Significant changes made to a campus-specific information system, data, or network resource must be appropriately reviewed and approved by the designated change control authority. Campuses must
establish and document a method for change management to manage changes to campus information systems, data, and network resources. While each campus may identify its own methods, an example follows:

<table>
<thead>
<tr>
<th>Description of Change</th>
<th>Low Impact Changes</th>
<th>Medium Impact Changes</th>
<th>High Impact Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A change intended to repair a fault in an information system or network resource. Such changes can include either the hardware or software components of information systems and network resources.</td>
<td>A change intended to update or upgrade an information system or network resource. Such changes can include major patches or significant changes to system configuration to meet a new policy, security guideline, or campus requirement. Such changes can include either the hardware or software components of information systems and network resources.</td>
<td>A change which will result in major changes to an information system or network resource. Such changes can include implementing new functions or replacing entire systems. Such changes can include either the hardware or software components of information systems and network resources.</td>
</tr>
<tr>
<td>Pre-change Requirements</td>
<td>A change plan, including back-out procedures, must be developed and approved.</td>
<td>A formal risk assessment must be conducted on the change. A change plan, including back-out procedures, must be developed and approved.</td>
<td>A formal risk assessment must be conducted on the change. A change plan, including back-out procedures, must be developed and approved. Information systems or network resources that are being changed must be fully backed up.</td>
</tr>
</tbody>
</table>
| Approval Required | • System owner  
• IT manager | • System owner  
• IT manager  
• ISO  
• Change control group | • System owner  
• IT manager  
• ISO  
• Change control group |
| Post-change Requirements | After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated. | After the change is made, appropriate information system or network resource documentation, operations processes and configuration documentation must be updated. Change results must be logged and reported to change control group. | After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated. Change results must be logged and reported to change control group. |
13.2 Resource Inventory Management

Each campus must develop and maintain an inventory of information systems. At a minimum, the inventory must include:

- System name
- Operating system and version
- Applications
- Installed patches (both OS and application)
- Administrator(s)

Each campus may determine its specific methods for creating and maintaining the inventory. The inventory may exist among multiple reports, data stores, or tools; however, the resulting information must be in a form and format which is available for audit and review.

13.3 Patch Management

Each campus must develop and maintain procedures and processes for the routine identification, evaluation, and application of software patches. These procedures and processes must include:

- Methods for checking with vendors and other resources for available patches.
- Methods for testing and evaluating available patches.
- Methods for making a recommendation to apply a patch. If the recommendation is not to install a patch (particularly a security related patch), then the rationale must be documented and reviewed by the campus ISO for inclusion in the campus risk management process.
- A nominal timeline for the patching process.

14.0 Access Control

14.1 User Account Credentials Management

Unless otherwise authorized, all users of campus’ information systems, data, or network resources, must be identified with a unique credential that establishes identity. This unique credential must not be shared with others. Users are responsible for all actions performed under the context of their identity. In addition to unique identification, all users of campus’ information systems, data, or network resources, must be required to use at least one factor of authentication (i.e., token, password or biometric devices).

Campuses must establish criteria for disabling inactive user accounts on campus information systems or network resources. The period of acceptable inactivity must be based upon the results of a risk assessment.

All “guest” or generic accounts on campus’ information systems or network resources must be disabled or removed unless specifically authorized based upon the results of a risk assessment.

Campuses must establish criteria for disabling user accounts on campus’ information systems or network resources after successive failed logon attempts.

Campuses must establish processes for reabling or resetting user accounts once they have been disabled. User identity must be appropriately verified prior to re-enabling or resetting user accounts. If automated, these processes must take into consideration the lockout time based on potential risk.
Administrators of campus’ information systems and network resources must have individual user accounts on the information systems and network resources they administer or use utilities such as “sudo” or “Run As” to perform system administration tasks. Administrator accounts must not be used for non-administrative uses (e.g., browsing the web while logged in as administrator).

Unless specifically authorized, workstation administrator accounts should not be used for non-administrative uses.

14.1.1 Access Documentation

Access to campus information systems, data, or network resources must include formal, documented (manually or electronically) approval before access or privileges are granted.

All changes to user accounts (i.e., account termination, creation, and changes to account privileges) on campus information systems or network resources (except for password resets) must be approved by appropriate campus personnel. Such approval must be formally documented.

14.2 Password Management

Campuses must identify and communicate acceptable password criteria. The criteria may vary by system or application at the campus’ discretion based upon a risk assessment. A sample criteria for strong passwords follows:

- Strong passwords are at least seven (7) characters in length and require the use of two out of four of the following:
  - Capital letters
  - Lower case letters
  - Numbers
  - Special characters

Campuses must identify and communicate a password change schedule. The schedule may vary by system or application at the campus’ discretion based upon a risk assessment. A sample schedule follows:

- Passwords on campus’ information systems must be changed every 90 days. Password reuse must be restricted to no more than once every four (4) uses. First-time passwords (e.g., passwords assigned by IT administrators upon account creation or during password resets) must be set to a unique value per user and changed immediately after first use.

Campus information systems and network resources must not display, transmit, or store passwords in clear text.

14.3 Encryption

When encryption is used to protect campus information systems, data, or network resources, the following minimum requirements must be met:

- Strong cryptography such as Triple-DES or AES must be used.
- Cryptographic strength of any encryption used must not be less than 128-bits.
- Formal procedures and responsibilities for key management must be established. The procedures must address key rotation, key storage, key selection, key escrow, and key handling.
14.4 User Privilege Authorization and Management

14.4.1 Access Authorization
Appropriate campus managers, data stewards, and/or their designated delegates, must define and approve user access to campus information systems, protected data, and network resources. Such authorizations must be tracked and logged following campus defined processes and should include information such as:

- Date and time of authorization
- Identification of person providing the authorization
- Brief description of access privileges granted
- Brief description of why access privileges granted

14.4.2 Access Establishment
- Authentication controls must be implemented for campus information systems, protected data, and network resources. Such campus defined controls should take into consideration as appropriate:
  - Validating user identity prior to granting access to system resources or data.
  - Uniquely identifying users and their corresponding logical access privileges.
  - Denying all logical access rights until rights are formally assigned.
  - Detecting and warning about repeated failed access attempts.
  - Allowing logical access rights to be promptly modified or revoked.
  - Allowing authentication credentials to be regularly changed.

14.4.3 Access Modification
At least annually, appropriate campus managers, data stewards, and/or their designated delegates must review and verify user access rights to campus information systems, protected data, and network resources. Such rights must be revised as necessary. All such revisions must be tracked and logged following campus defined processes and should include information such as:

- Date and time of revision
- Identification of person performing the revision
- Brief description of revision
- Brief description of why revision was made

15.0 Asset Management

15.1 Data Classification
Data stored on campus hardware or media (both paper and electronic) must be classified per CSU’s data classification system. The minimum classification levels are defined in the following table. Campuses may develop additional local categories, but they must not contradict the system-wide set.

Campuses may elect to move or add data elements from one classification level to another classification level with higher protection requirements, but never to a classification level with lower protection requirements. That is, a data element classified as Level 2 can be moved to a Level 1 classification but it cannot be moved to a Level 3 classification.
<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| **Level 1 Confidential** | Confidential Information is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential information is information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CUS's reputation, and legal action could occur. Level 1 information is intended solely for use within the CSU and limited to those with a “business need-to-know.” Statues, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information. | - Passwords or credentials  
- PINs (Personal Identification Numbers)  
- Birth date combined with last four of SSN and name  
- Credit card numbers with cardholder name  
- Tax ID with name  
- Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name  
- Social Security number and name  
- Medical records related to an individual  
- Psychological Counseling records related to an individual  
- Bank account or debt card information  
- Vulnerability/security information related to a campus or system |
| **Level 2 Internal Use** | Internal use information is information which must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU’s reputation, violate an individual's privacy rights or legal action could occur. | **Identity Validation Keys**  
- Birth date (full: mm-dd-yy)  
- Birth date (partial: mm-dd only)  
- Mother's maiden name  

**Student Information**  
- Educational records (Excludes directory information)  
  - Grades  
  - Courses taken  
  - Schedule  
  - Test Scores  
  - Advising records  
  - Educational services received  
  - Disciplinary actions  
- Non-directory student information may not be released except under certain prescribed conditions  

**Employee Information**  
- Employee net salary  
- Employment history  
- Home address  
- Personal telephone numbers  
- Personal email address  
- Parents and other family members names  
- Payment History  
- Employee evaluations |
<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Level 3 Public | This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard. Knowledge of this information does not expose the CSU to financial loss or jeopardize the security of CSU's information assets. Level 3 information may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure. | • Background investigations  
• Biometric information  
• Electronic or digitized signatures  
• Private key (digital certificate)  
• Birthplace (City, State, Country)  
• Ethnicity  
• Gender  
• Marital Status  
• Personal characteristics  
• Physical description  
• Photograph  

Other  
• Linking a person with the specific subject about which the library user has requested information or materials.  
• Legal investigations conducted by the University.  
• Sealed bids  
• Trade secrets or intellectual property such as research activities  
• Location of assets  

Campus Identification Keys  
• Campus identification number  
• User ID (do not list in a public or a large aggregate list, protection of SPAM, where it is not the same as the student email address)  

Student Information  
• Educational directory information (FERPA)  
• Employee Information  
• Employee Title  
• Employee public email address  
• Employee work location and telephone number  
• Employing department  
• Employee classification  
• Employee gross salary  
• Name (first, middle, last) (except when associated with protected information)  
• Financial budget information  
• Signature (non-electronic) |

The Senior Director of Information Systems (SDIS), within the Office of the Chancellor, must establish a process for the review and maintenance of the data classification.

The SDIS must review the classification standard on an annual basis.

The SDIS must determine what data will be designate Level 1 data and must identify appropriate minimum controls.

Each data owner must determine the classification of their data following the standards provided. If additional guidance is needed, then the campus ISO should be consulted.
Each data owner must establish a method to approve the use of their data. A data owner may declare their data available for general use.

Aggregates of data must be classified based upon the most secure classification level. That is, when data of mixed classification exist in the same file, document, report or memorandum, the classification of that file, document, report or memorandum should be of the highest applicable level of classification.

15.2 Data Handling

Data stored on campus hardware or media must be appropriately labeled and protected according to its classification.

When protected data is electronically sent, it must be sent via a method that uses strong encryption.

When Protected Level 2 data is electronically sent, it should be protected using approved campus processes.

Each campus must identify which applications and systems contain or have access to protected Level 1 or Level 2 data.

15.3 Data Retention

With the passage of time, data stored on campus hardware or media (electronic or paper) may no longer be required for organizational purposes. As appropriate, the storage of data must be kept to the minimum necessary.

All data on campus hardware or media (electronic or paper) must be retained per CSU Executive Order 1031.

15.4 Data Disposal

Campus electronic and non-electronic media and hardware which contains protected data no longer required for legitimate organizational purposes, must be disposed of. The following disposal methods must be used:

- Non-electronic media must be cross-cut shredded, incinerated, or pulped.
- Electronic media must be purged, degaussed, shredded, or otherwise physically destroyed so that the protected data cannot be reconstructed. If a data deletion program is used, it must write random data for at least one complete pass across the entire media.
- Campus back-up (i.e., tape, optical) media must be physically destroyed or degaussed.

Campuses must track the disposal of equipment which may have contained protected data. At a minimum, such tracking identify:

- Date and time of disposal
- Brief description of items being disposed of
- Name and title of person(s) performing the disposal

16.0 Management of Information Systems

16.1 Development Management

Each campus must have a formal, documented process for developing and procuring applications and information systems. The process must ensure that sufficient risk-based information security controls are
built into applications and information systems developed or procured by a campus. The process must include, but is not limited to:

- A needs assessment and justification for development or procurement.
- Definition of requirements for functionality, performance, reliability, interoperability with other information systems, security, and recovery prior to start of development or procurement.
- Identification of security risks, development of associated security controls, and documentation of resulting residual risk.
- A clear separation of duties between development, test, and production environments.
- Use of secure coding guidelines (e.g., OWASP, SCARE, SPSMM).
- Appropriate change control.

Campuses must conduct appropriate testing of all developed or procured applications and information systems before deployment in a production environment. Such applications and information systems must be appropriately documented prior to deployment in a production environment.

As determined necessary by risk assessment, application code created by a campus must be appropriately reviewed before being used in a production environment.

### 16.2 Web Application Coding

Web software applications created by campuses must be developed per secure coding guidelines such as the Open Web Application Security Project (OWASP) guidelines. Before being placed into a campus production environment, such applications must be reviewed and tested to help prevent the following vulnerabilities:

- Un-validated input
  - Inadequate access control
  - Inadequate authentication and session management
  - Cross-site scripting (XSS) attacks
  - Buffer overflows
  - Injection flaws
  - Improper error handling
  - Insecure storage
  - Denial of service
  - Insecure configuration management

### 16.3 Database Coding

<<Placeholder for May ISO meeting discussions>>

### 16.4 Life Cycle Management

Each campus must develop and maintain appropriate procedures and processes for the acquisition, upgrade, and maintenance of information systems. At a minimum, these procedures and processes must consider including methods for:

- Determination of the classification of data being processed.
- Determination of user access being provided.
- Identification, coordination, and approval of security requirements.
- Protection of campus data during development and test.
- Documentation and validation of security controls.
- Secure transition to operations to include backout planning.
- Routine inspection to ensure the configuration integrity of the operational environment.
- Secure disposition and disposal of information systems and data at their end of life.

Each campus must develop and communicate appropriate processes for testing of information systems and applications prior transition to operations. In particular, these processes should address compensating controls required to mitigate the specific risks of a test environment.

17.0 Information Security Incident Management

17.1 Evidence Collection and Handling

Each campus must develop and maintain procedures and processes for evidence handling in support of incident handling. At a minimum, the campus must address their access to forensic resources (either internal or through external arrangements) and their criteria for contacting law enforcement.

If a campus chooses to maintain its own forensic capability, the campus must develop and maintain procedures and processes for:

- A method for labeling all items to include:
  - Date/time collected
  - Name and contact information for collection agent
  - Location of collection
  - Unique identification scheme
  - Detailed description of the item

- A method for logging all evidence collected

- Identification of a secure location for evidence storage

- A method for tracing evidence custody to include at a minimum the following information:
  - Date/time evidence removed from storage
  - Date/time evidence returned to storage
  - Name/contact information of handler
  - Disposition of evidence (e.g., forensic exam or court)

17.2 Reporting

Each campus must formally define a point of contact (POC) for information security incident reporting. A campus’ POC can be an individual (i.e., ISO) or an organization (i.e., Information Technology Help Desk or Computer Security Incident Response Team (CSIRT)). A formal, centralized method (i.e., email or phone number) for reporting information security incidents to campus POCs must be provided to users.

Each campus must develop appropriate procedures and processes for investigating and documenting information security events and incidents.
Each campus must identify and communicate means for users and third parties to report suspected incidents. This information must be part of routine security awareness activities.

Each campus must inform the Chancellor’s Office of any security incidents requiring notification of users (i.e., violations of California information privacy laws). The notification process must include the following steps:

- The campus ISO must contact the Office of the Chancellor and ITS.
- The campus president must contact the Chancellor.
- A description of the incident must be sent to the The Senior Director of Information Systems (SDIS).
- If the incident will be made public, then the campus must:
  - Prepare a press release
  - Send the press release to the SDIS who will forward it to the ISO/ITAC
- Document lessons learnt of the incident so the Sr. Director information security could share with ISO/CSIRT.

Each campus’ POC must implement feedback processes to ensure that those reporting information security incidents are appropriately acknowledged.

### 18.0 Physical Security

#### 18.1 Security Zones

Each campus must regularly review all of its physical areas and identify them per the table below.

<table>
<thead>
<tr>
<th>Zone</th>
<th>Brief Description</th>
<th>Necessary Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>No critical systems are located in the area.</td>
<td>None. Access to this area can be unrestricted.</td>
</tr>
<tr>
<td>Shared Access</td>
<td>An area containing at least one critical system. Persons in the area of the system includes those who do not have authorization to the system or the information it contains.</td>
<td>Appropriate physical access controls and construction must be implemented to restrict access from the public area to the Campus Limited Access Area. Access to the Campus Limited Access Area must be limited to only persons having a need for specific access in order to accomplish a legitimate task.</td>
</tr>
</tbody>
</table>
| Campus Limited Access Area    | An area containing at least one critical system (usually multiple). Persons accessing the area are limited to those who have authorization to the system or the information it contains. All others are restricted. | Appropriate physical access controls and construction must be implemented that limit access to the area to only persons having a need for specific access in order to accomplish a legitimate task. The controls must enforce the principles of need to know and least possible privilege. All physical access to such areas must be tracked and logged. At a minimum, such tracking and logging must provide:
  - Date and time of access
  - User ID performing access

Visitors to such areas must sign a visitor’s log prior to being granted physical access. The log must document the visitor’s name, the authorizing employee, and the date and time for ingress and egress.
18.2 Work Area Security

Campuses must establish and communicate user guidelines for securing protected data in work areas. The guidelines must address:

- Leaving protected data unattended.
- Limiting the viewing of protected data unauthorized users.
- Time-based application or system locking.

19.0 Business Continuity and Disaster Recovery

TBD

20.0 Legal and Regulatory Compliance

20.1 PCI

TBD

20.2 HIPAA

TBD
Appendix A – Initial List of Standards

This section identifies the initial list of proposed standards and their original objectives. Its contents are not planned to be updated.

This list is intended to be used as a working aide during the standards development and will be deleted as the standards are finalized.

<table>
<thead>
<tr>
<th>Security Policy Topic</th>
<th>Potential Standards</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Roles &amp; Responsibilities</td>
<td>Description of Duties for: Campus President Campus Information Technology Administrator Information Security Officer</td>
<td>Describe the minimum expectations for each of these roles in support or the CSU Information Security program.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Risk Assessment</td>
<td>Identification of the minimum elements required for review.</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td>Identification of the minimum process required for the review and the process for a campus president to delegate his/her risk acceptance authority.</td>
</tr>
<tr>
<td>Acceptable Use</td>
<td>Login Warning Banners</td>
<td>Identify wording for login banners.</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>Termination and Position Change Personnel Vetting</td>
<td>May already be sufficiently covered by existing HR materials.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Web Site Privacy</td>
<td>Identify minimum common language for web site privacy notification.</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>Content</td>
<td>Identify the minimum content for security training.</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training Activities</td>
<td>Identify who needs training and how often is should be received.</td>
</tr>
<tr>
<td>Third Party Services Security</td>
<td>Third Party Use of CSU Resources Contracted Relationships</td>
<td>Creation of a common approach for defining and managing relationships.</td>
</tr>
<tr>
<td>Security Policy Topic</td>
<td>Potential Standards</td>
<td>Objective</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information Technology</td>
<td>Approved Products List (APL)</td>
<td>Create a framework and a process for the identification and/or selection of security products. The products could be &quot;approved&quot; because they are known to meet the minimum technical requirements or because the CSU has established preferred pricing. Candidate product areas: encryption, firewalls, intrusion detection, virus scanning <strong>Selection of actual products are not part of the standards work.</strong></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Controls Management</td>
<td>Identify the minimum documentation of equipment inventory, network documentation, and identification of technical controls.</td>
<td></td>
</tr>
<tr>
<td>Remote Access</td>
<td>Identify minimum features, capabilities, and configurations for remote access to CSU resources.</td>
<td></td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>Identify the minimum processes for the control of mobile devices accessing CSU resources.</td>
<td></td>
</tr>
<tr>
<td>Boundary Protection and Isolation</td>
<td>Identify minimum features, capabilities, and policies to be enforced.</td>
<td></td>
</tr>
<tr>
<td>Malicious Software Protection</td>
<td>Identify minimum features, capabilities and configurations.</td>
<td></td>
</tr>
<tr>
<td>Wireless Access Points</td>
<td>Identify minimum features, capabilities and configurations.</td>
<td></td>
</tr>
<tr>
<td>Logging Elements</td>
<td>Identify the minimum set of elements which should be recorded to support investigations and troubleshooting.</td>
<td></td>
</tr>
<tr>
<td>Security Policy Topic</td>
<td>Potential Standards</td>
<td>Objective</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration Management and Change Control</td>
<td>Change Management</td>
<td>Identify the minimum process required for the creation, test, approval, and implementation of a change to the technical baseline (i.e. hardware or software modifications).</td>
</tr>
<tr>
<td></td>
<td>Baseline Management</td>
<td>Indentify the minimum process for tracking software and hardware and software and making sure they are kept current.</td>
</tr>
<tr>
<td>Access Control</td>
<td>User Account Credentials</td>
<td>Minimum processes for the control of user credentials to include items such as account expiration, credential sharing, number of invalid login attempts.</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>Minimum characteristics for passwords to include length, composition, and change schedule.</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>Minimum guidance for encryption of protected data.</td>
</tr>
<tr>
<td></td>
<td>User Privilege Authorization and Management</td>
<td>Minimum processes for the control of user access to include items such as authorization, revalidation, and revocation.</td>
</tr>
<tr>
<td>Asset Management</td>
<td>Data Classification</td>
<td>Categorization of protected information. Will be based on the previous ISO work.</td>
</tr>
<tr>
<td></td>
<td>Data Handling</td>
<td>Identify the minimum protections for handling protected data.</td>
</tr>
<tr>
<td></td>
<td>Data Retention</td>
<td>Identify the minimum process for maintaining data.</td>
</tr>
<tr>
<td></td>
<td>Data Disposal</td>
<td>Identify the minimum process or technology for the disposal of excess data and its associated media.</td>
</tr>
<tr>
<td></td>
<td>Clean Desk</td>
<td>Identify the minimum process for desk area &quot;housekeeping&quot;; especially for areas containing protected data.</td>
</tr>
<tr>
<td>Management of Information Systems</td>
<td>Development Management</td>
<td>Identify minimum coding standards, project management processes, and project acceptance processes.</td>
</tr>
<tr>
<td></td>
<td>Web Application Coding</td>
<td>Identify minimum coding requirements; especially for Internet facing servers.</td>
</tr>
<tr>
<td></td>
<td>Life Cycle Management</td>
<td>Identify the minimum processes associated with technology refresh and decommissioning.</td>
</tr>
<tr>
<td>Security Policy Topic</td>
<td>Potential Standards</td>
<td>Objective</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information Security Incident Management</td>
<td>Evidence Collection</td>
<td>Identify the minimum process and techniques required.</td>
</tr>
<tr>
<td></td>
<td>Reporting</td>
<td>Identify the minimum elements for an incident response reporting requirements.</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Security Zones</td>
<td>Define different protection zones and their associated controls.</td>
</tr>
<tr>
<td></td>
<td>Secured Entrance</td>
<td>Identify the minimum entrance controls based on data protection levels. Need to keep in mind that CSU is a public institution.</td>
</tr>
<tr>
<td></td>
<td>Secured Infrastructure</td>
<td>Identify the minimum controls for critical infrastructure areas to include network closets, ports, etc.</td>
</tr>
<tr>
<td></td>
<td>Viewing Controls</td>
<td>Identify screen lock time outs and proper screen positioning to minimize shoulder surfing.</td>
</tr>
<tr>
<td></td>
<td>Data Center Access</td>
<td>Identify the minimum process for controlling access to data centers.</td>
</tr>
<tr>
<td>Business Continuity and Disaster Recovery</td>
<td>(See Applicable EO)</td>
<td></td>
</tr>
<tr>
<td>Legal and Regulatory Compliance</td>
<td>PCI</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>HIPAA</td>
<td>TBD</td>
</tr>
</tbody>
</table>
Electronic Recording Delivery System
Baseline Requirements & Technology Standards Handbook
Addendum to the following ERDS Handbooks:
Vendor of ERDS Software Certification
Computer Security Auditor
System Certification

Office of the Attorney General
California Department of Justice

November 2016
# TABLE OF CONTENTS

1 INTRODUCTION 5

1.1 OVERVIEW 5

1.1.1 FOCUS OF SECURITY 5

1.1.2 RESPONSIBILITIES OF THE COUNTY RECORDER 5

1.1.3 STATUTORY, INDUSTRY AND TECHNICAL TERMINOLOGY 6

1.1.4 FISCAL IMPACT 6

1.1.5 USE OF VENDORS 6

1.2 APPROACHES 7

1.2.1 TYPE 1 ERDS 7

1.2.2 TYPE 2 ERDS 7

1.2.3 TYPE 1 AND TYPE 2 ERDS 8

1.2.4 CONTENT INSPECTIONS 8

1.3 THE ERDS BOUNDARY 8

1.3.1 USERS 9

1.3.2 FUNCTIONALITY 9

1.3.3 ERDS IMPLEMENTATION 10

1.3.4 APPROACH DESCRIBED IN THIS DOCUMENT 10

1.3.5 ERDS OPERATING PROCEDURES 10

2 DATA ARCHITECTURE 12

2.1 THE ERDS PAYLOAD 12

2.2 ERDS PAYLOAD STRUCTURE 12

2.3 TYPE 1 AND/OR TYPE 2 INSTRUMENTS 13

2.4 UNIFORM INDEX INFORMATION 14

2.5 ELECTRONIC SIGNATURE OF A NOTARY 14

3 ERDS PROCESSES 15

3.1 ERDS LOGIN PROCESS 15

3.2 ERDS PAYLOAD SUBMISSION PROCESS 16

3.3 ERDS PAYLOAD RETRIEVAL PROCESS 18

3.4 PROCESSING MULTIPLE TRANSACTIONS 19

4 SECURITY REQUIREMENTS 20

4.1 INTRODUCTION 20

4.1.1 CONCEPTUAL OVERVIEW 20

4.2 MINIMUM SECURITY REQUIREMENTS 22

4.2.1 DATA INTEGRITY 22

4.2.2 PAYLOAD PROTECTION 23

4.2.2.1 Payload Confidentiality 23

4.2.2.2 Payload Integrity 23

4.2.2.3 Payload Authenticity 23

4.2.3 CRYPTOGRAPHIC KEY GENERATION 23
4.2.4 CERTIFICATE AUTHORITY AND PKI
4.2.5 SECURING ERDS PAYLOADS
4.2.6 VALIDATING ERDS PAYLOADS
4.2.7 WORKSTATION SECURITY
4.2.8 MEDIA SECURITY

4.3 ADDITIONAL SECURITY REQUIREMENTS FOR TYPE 1 ERDS

4.3.1 ACCESS CONTROL
4.3.1.1 Identification Requirements
4.3.1.2 Authentication Requirements
4.3.1.3 Authorization Requirements
4.3.1.3.1 Role-Based Access Control
4.3.1.3.2 Authorized Submitter and Agent
4.3.1.4 Accountability Requirements
4.3.1.4.1 Session Activities
4.3.1.4.2 Unauthorized Activities
4.3.1.4.3 Transaction Activities
4.3.1.4.4 Accountability Failures
4.3.1.5 Administration Requirements

4.3.2 SERVER SECURITY
4.3.2.1 Proxy Server
4.3.2.2 ERDS Server Security
4.3.2.3 Server Hardening
4.3.2.4 Server Events

4.3.3 NETWORK SECURITY
4.3.3.1 Transmission Security/Confidentiality
4.3.3.1.1 Transmission Integrity
4.3.3.2 Unauthorized Network Traffic
4.3.3.3 Alternative Transmission Methods
4.3.3.4 Network Events

4.3.4 PHYSICAL SECURITY

4.4 SECURITY CHECKLISTS

4.5 INCIDENT RESPONSE
4.5.1 INCIDENT REPORTING
4.5.2 INCIDENT RESPONSE PROCEDURES

4.6 SUBSTANTIVE MODIFICATIONS

5 AUDIT REQUIREMENTS

5.1 NATURE OF ERDS COMPUTER SECURITY AUDITS

5.2 COMPUTER SECURITY AUDITS
5.2.1 INITIAL SYSTEM AUDIT
5.2.2 BIENNIAL AUDIT
5.2.3 MODIFIED SYSTEM AUDIT
5.2.4 MODIFIED SYSTEM INCIDENT AUDIT
5.2.5 AUDIT AND LOCAL INSPECTION SCHEDULE

5.3 SECURITY AUDIT REPORT FORMAT
5.4 PROPRIETARY SOFTWARE

6 ESCROW REQUIREMENTS
6.1 APPROVED ESCROW FACILITY
6.2 LETTER OF DEPOSIT
6.3 REQUIREMENTS FOR SUBMISSION
6.4 DEPOSIT OF SOFTWARE MODIFICATIONS INTO ESCROW
6.5 INTEGRITY OF MATERIALS
6.6 RETENTION AND DISPOSITION OF MATERIALS
6.7 ACCESS TO MATERIALS
6.8 STATE NOT LIABLE FOR ANY COSTS OR ANY OTHER'S ACTIONS

7 ACRONYMS AND DEFINITIONS

8 REQUIREMENTS MATRIX
8.1 HOW TO READ THE MATRIX

TABLE OF FIGURES

Figure 1 - Conceptual ERDS Boundary .......................................................... 10
Figure 2 - ERDS Payload Structure ................................................................ 12
Figure 3 - Login Process .............................................................................. 15
Figure 4 - Payload Submission Process ......................................................... 17
Figure 5 - Payload Retrieval Process ............................................................... 18
Figure 6 - Conceptual Security Infrastructure ................................................. 20
Figure 7 - Securing ERDS Payloads ................................................................. 24
Figure 8 - Validating ERDS Payloads ............................................................... 25

TABLE OF TABLES

Table 1 - Instrument Types ............................................................................ 13
Table 2 - Login Process Description ................................................................. 16
Table 3 - Payload Submission Process Description ........................................ 17
Table 4 - Payload Retrieval Process Description ............................................ 18
Table 5 - Conceptual Security Infrastructure Descriptions .............................. 21
Table 6 - Role Descriptions ........................................................................... 28
Table 7 - Incident Response Criteria and Reporting Requirements ................ 36
1 INTRODUCTION

The purpose of this document is to establish the minimum baseline technological guidelines, requirements, procedures, and standards in the areas of security, reliability, and uniformity following the enactment of the Electronic Recording Delivery Act (ERDA) of 2004, to establish an Electronic Recording Delivery System (ERDS) as provided for in the California Code of Regulations (CCR), Title 11, Division 1, Chapter 18, Articles 1 through 9. As such, this document uses technical terms to describe information technology and is intended for Computer Security Auditors, Vendors of ERDS Software, and individuals having technical responsibilities for an ERDS. This document does not, however, specify design details that may be necessary to fully implement an ERDS meeting the intent of the ERDA. While this document includes requirements for the security, audit, and escrow of an ERDS, it should be referenced in conjunction with the ERDS handbooks pertaining to the Vendor of ERDS Software, Computer Security Auditor, and System Certification.

1.1 OVERVIEW

A County Recorder may, in lieu of written paper, accept for recording digital electronic records and digitized electronic records, subject to specified conditions. The ERDS Program has established baseline technological and procedural specifications that detail the conditions for delivering, and, when applicable, returning digital electronic records and digitized electronic records. Nothing in these specifications shall be construed to administer any of the processes or procedures relating to the business of a County Recorder of the State of California. Specifications established by the ERDS Program are intended to assure that the ERDS is secure and that ERDS operating procedures are sufficient to assure the continuing security and lawful operation of the ERDS. Additionally, these specifications do not address prevention for any tampering or fraudulent documents prior to transmitting via an ERDS.

1.1.1 Focus of Security

An ERDS is a system to deliver for recording, and, when applicable, return to the party requesting recording, digitized or digital electronic records. Considering the requirements for security and the openness of the Internet, each ERDS shall focus on protecting the confidentiality and integrity of digital electronic records and digitized electronic records during the process of transmission and storage using an ERDS. In addition to the delivery, and, when applicable, the return of digital electronic records or digitized electronic records, this document addresses the handling of uniform index information and information about the electronic signature of a notary.

1.1.2 Responsibilities of the County Recorder

The County Recorder shall be responsible for ensuring an ERDS meets the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. With respect to an ERDS, the County Recorder may delegate tasks to designees and representatives, assign responsibility by contract or agreement, and grant authority through policies and procedures; however, the overall safety and security of an ERDS shall remain the responsibility of the County Recorder. Where the term “County Recorder” is used in this document, the County Recorder shall determine the necessary resources and means to meet the requirement.
1.1.3 Statutory, Industry and Technical Terminology

These specifications do not limit the content or format of digital electronic records and/or digitized electronic records. Because the state of technology is such that digital electronic records and digitized electronic records are not reliably distinguishable by automated means, additional precautions shall be taken to meet the requirements of the Electronic Recording Delivery Act (ERDA) of 2004.

The ERDA refers to two types of instruments that may be delivered, and, when applicable, returned as digital electronic records and/or digitized electronic records. For the purposes of an ERDS, these instruments are categorized as “Type 1” and “Type 2”. A “Type 1” instrument is defined to mean an instrument affecting a right, title, or interest in real property. A “Type 2” instrument is defined to mean an instrument of reconveyance, substitution of trustee, or assignment of deed of trust. The real estate industry refers to Type 1 and Type 2 instruments as “front-end” and “back-end” documents, respectively. Because these terms do not necessarily reflect the method of delivery (digital or digitized) or the characteristics of computer-generated files, the County Recorder shall establish ERDS operating procedures and/or incorporate features within the ERDS design in order to restrict the instrument type to meet the requirements of the ERDA. A summary of the relationships among statutory, industry and technology terms is provided in Table 1 - Instrument Types.

1.1.4 Fiscal Impact

All ERDS shall be designated as Type 1 or Type 2 or Type 1 and 2 and whether a return function is included, when applicable. For each ERDS, the types of instruments and the characteristics of computer-generated files depend on the business requirements of the County Recorder. For this reason, the types of instruments submitted, and, when applicable, returned, as well as the characteristics of computer-generated files transmitted via an ERDS, are at the discretion of the County Recorder. If the County Recorder allows for the delivery of Type 1 and/or Type 2 instruments electronically, then the transmission of those instruments shall meet all of the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

To provide options in implementing an ERDS, several approaches are described in this document. Current information technologies offer a wide variety of approaches. For illustrative purposes, the approaches described in Section 1.2, Approaches, provide examples of architectures suitable for meeting the requirements of the ERDA. The examples are not intended to either specify or limit the design of, or technologies employed for, an ERDS. Rather, the examples are given to illustrate how technologies can be employed to meet the requirements of the ERDA while providing options that limit the fiscal impact on County Recorders.

1.1.5 Use of Vendors

A County Recorder may employ a Vendor of ERDS Software, use in-house resources, or enter into an agreement with another public entity in establishing an ERDS. Computer Security Auditors, Authorized Submitters, Agents, and Vendors of ERDS Software shall be separate entities. Authorized Submitters may employ a third-party vendor as an Agent provided that the third-party vendor is neither a Computer Security Auditor nor a Vendor of ERDS Software. (For further clarification, refer to the definitions for “Agent” and “Vendor of ERDS Software” contained in Section 7, Acronyms and Definitions.)
1.2 **Approaches**

Ensuring the secure delivery and integrity of Type 1 and Type 2 instruments is achieved by using the minimum baseline security requirements as defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 and outlined in Section 4.2, Minimum Security Requirements. Specific architectural details are ERDS-design dependent and may not be fully explained in this document. The selection of specific technical design approaches shall be at the discretion of the County Recorder.

Irrespective of the ERDS design, the minimum security requirements, as specified in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 and outlined in Section 4.2, Minimum Security Requirements, shall be met by protecting the payload structure and content for both Type 1 and Type 2 instruments. All ERDS for either Type 1 or Type 2 payloads shall be protected by the use of encryption, both in transmission and storage, until decrypted by the intended recipient. Once decrypted by the intended recipient, the security of the contents shall become the responsibility of the intended recipient. The roles and responsibilities of ERDS participants, including, but not limited to, Agents and Vendors of ERDS Software, shall be consistent with Section 4.3.1.3, Authorization Requirements and Section 7, Acronyms and Definitions. While the ERDS Regulations allow flexibility in approach, the security and testing requirements shall be met.

1.2.1 **Type 1 ERDS**

This illustrative approach requires fingerprinting of each AuthorizedSubmitter and offers robust security. Only those individuals granted permissions under the role of “Secure Access” (Refer to Section 4.3.1, Access Control) shall be permitted access to a Type 1 ERDS. Type 1 instruments shall be submitted as digitized electronic records. One or more servers are employed to guide an AuthorizedSubmitter through ERDS processes and store the ERDS payloads.

Confidentiality, integrity and authenticity are preserved by encrypting and “signing” a data structure called the “ERDS payload”. Data confidentiality is preserved by encrypting the ERDS payload. Data integrity and authenticity are preserved by “signing” the ERDS payload. Delivery occurs via commonly available secure transfer protocols, such as Transport Layer Security (TLS) or a Virtual Private Network (VPN) to a Type 1 ERDS.

The identity of each AuthorizedSubmitter and County Recorder Designee who accesses the Type 1 ERDS is verified using two factors: (1) a user ID and password, and (2) a digital certificate validated by a certificate authority employing public key cryptography methods. The actual contents of Type 1 ERDS payloads shall be verified to ensure adherence to restrictions of instrument type.

1.2.2 **Type 2 ERDS**

This illustrative approach does not require the fingerprinting of an AuthorizedSubmitter and makes the most use of existing information technology. In this approach, the transport mechanism is electronic mail; however, only Type 2 instruments shall be submitted by individuals granted permissions under the role of “Authorized Access”. (Refer to Section 4.3.1, Access Control)

Confidentiality, integrity and authenticity are preserved by encrypting and “signing” e-mail. Data confidentiality is preserved by encrypting an attachment to an electronic mail message. Data integrity is preserved by “signing” the attachment. The attachment is a data structure called the “ERDS payload”. (Refer to Section 2, Data Architecture.) Authenticity is preserved by “signing”
the electronic mail message itself. Delivery occurs via commonly available electronic mail transfer protocols, such as the Simple Mail Transfer Protocol (SMTP).

The identity of each Authorized Submitter and County Recorder Designee, who sends a Type 2 ERDS payload, is verified using a digital certificate validated by a certificate authority employing public key cryptography methods. The actual contents of Type 2 ERDS payloads shall be verified to ensure adherence to restrictions of instrument type.

1.2.3 Type 1 and Type 2 ERDS

This illustrative approach requires fingerprinting of each Authorized Submitter with a role of "Secure Access", but not any Authorized Submitter with a role of "Authorized Access", and offers robust security and separation of Type 1 instruments from Type 2 instruments. Individuals granted permissions under the role of "Secure Access", "Authorized Access", or "County Recorder Designee" (refer to Section 4.3.1, Access Control) shall be permitted access. One or more servers are employed to guide an Authorized Submitter through ERDS processes and store the ERDS payloads. The combination of a role-based access control system and an application server separates Type 1 instruments from Type 2 instruments.

Confidentiality, integrity, and authenticity are preserved and identity verified in the same manner as for Secure Access to a Type 1 ERDS.

An application server processes functions based on the role authorized in the role-based access control system. If an individual is granted permissions under the role of "Authorized Access", only Type 2 instruments may be submitted. If an individual is granted permissions under the role of "Secure Access", both Type 1 and Type 2 instruments may be submitted; however, Type 1 instruments shall be limited to digitized electronic records. In either case, the ERDS payloads are delivered to a Type 1 ERDS.

1.2.4 Content Inspections

Regardless of approach, the County Recorder shall make no assumptions about the content delivered via an ERDS. Until technology reliably distinguishes digital electronic records from digitized electronic records, the County Recorder shall have ERDS operating procedures that include inspection to determine that the content delivered via an ERDS meets the requirements of the ERDA. Specifically, if the County Recorder cannot assure, with 100 percent certainty, that the contents of a digital electronic record cannot be delivered as a digitized electronic record, and vice versa, and that a Type 1 instrument cannot be delivered as a Type 2 instrument, and vice versa, then the contents of all Type 1 and Type 2 instruments shall be inspected before being accepted.

1.3 The ERDS Boundary

This section describes the boundary of an ERDS. The boundary of an ERDS is defined to include that hardware, software, network connections and storage media specifically designed and/or designated for the delivery, and, when applicable, return of Type 1 and/or Type 2 instruments. Such hardware, software, storage media, and network connections shall be designated by the County Recorder establishing the ERDS and shall be included in system certifications, audits, local inspections, and reviews.

As such, hardware, software, storage media, and network connections not designated by the County Recorder shall:
1. Not be considered part of an ERDS.
2. Not be employed for the delivery of Type 1 or Type 2 instruments.
3. Not be included in system certifications, audits, local inspections or reviews.

1.3.1 Users

The ERDS shall support the ability of the County Recorder to grant access to any Authorized Submitter. The details of implementing processes such as establishing and deleting accounts, enabling encryption and decryption, and assigning roles are ERDS-design dependent and shall be implemented using resources at the discretion of the County Recorder.

Once granted access, an Authorized Submitter shall be able to submit Type 1 and/or Type 2 instruments depending on specific privileges granted by a County Recorder. An Authorized Submitter may be granted access to more than one ERDS; however, access to each ERDS shall remain under management control of the County Recorder establishing and responsible for the ERDS.

A County Recorder shall clearly define roles and responsibilities to ensure Type 1 and Type 2 instruments are correctly and securely submitted, delivered, and when applicable, returned to the intended recipients. Textual disclaimers or verbal disclaimers alone shall not be sufficient to control access to Type 1 and Type 2 instruments under the control of an ERDS.

1.3.2 Functionality

An ERDS is used by an Authorized Submitter to deliver Type 1 and/or Type 2 instruments to a County Recorder. An ERDS is also used by a County Recorder to return Type 1 and/or Type 2 instruments to an Authorized Submitter, when applicable. When Type 1 and Type 2 instruments are returned to an Authorized Submitter via an ERDS, the security requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met. Any other responses or notifications transmitted via an ERDS shall not be required to meet the security requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

When implemented, each ERDS may consist of hardware, software, storage media, and network connections that securely exchange messages and data.

A County Recorder may collaborate with another County Recorder and make use of a single ERDS. ERDS servers, if employed, shall be designated as "Single-County" or "Multi-County." ERDS servers designated as Single-County shall be dedicated to serving a single county. ERDS servers designated as Multi-County shall serve more than one county as established by mutual agreement among County Recorders. Refer to the System Certification Handbook for procedures to apply for system certification of a Multi-County ERDS. Whether designated as a Single-County or Multi-County ERDS, all ERDS will be identified as either being Type 1, Type 2, or Type 1 and 2, and whether a return function is included, when applicable.

Servers employed for the purpose of implementing an ERDS may be dedicated to ERDS functions or integrated with other servers. Separate physical servers dedicated to performing an ERDS-server function are not required provided ERDS-server functions can be isolated from other server functions, as evidenced by audit. (Refer to Section 4.3.2, Server Security for more information.)
1.3.3 ERDS Implementation

In considering the characteristics of an ERDS and for illustrative purposes only, a conceptual ERDS boundary is depicted in Figure 1 - Conceptual ERDS Boundary. The components required to implement an ERDS may be installed and maintained on one or more servers designated for the purpose of implementing an ERDS. Components may be deployed to existing information technology in order to take advantage of available capabilities, but only if such deployment is necessary for the operation of an ERDS, and preserves the safety and security of the ERDS.

![Diagram](image)

Figure 1 - Conceptual ERDS Boundary

For example, ERDS components may be deployed to a separate proxy server in order to take advantage of the ability to establish secure connections via the Internet and act as a proxy for an Authorized Submitter. As another example, an ERDS may take advantage of the existing network infrastructure of a County Recorder, provided the infrastructure is protected from unauthorized access. As a final example, the nature of web-based applications means at least some ERDS components may be deployed to workstations.

1.3.4 Approach Described in this Document

The specifications outlined in this document assume implementation of an ERDS operated via the Internet. Where an ERDS makes use of the processes or technologies outlined in this document, the standards specified shall apply. Irrespective of an ERDS design, the minimum requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met. For example, the approach described in Section 1.2.2, Type 2 ERDS, does not necessarily require a login process or even a dedicated server. However, the processes for protecting the ERDS payloads, i.e. encrypting and signing, shall conform to Section 4.2, Minimum Security Requirements. An ERDS that employs a login process shall also conform to Section 4.3.1, Access Control. An ERDS employing one or more servers shall also conform to Section 4.3, Additional Security Requirements for Type 1 ERDS.

1.3.5 ERDS Operating Procedures

The County Recorder shall have ERDS operating procedures prepared, maintained, and followed that explain the proper operation, management, administration, content restrictions,
and use of their ERDS. ERDS operating procedures shall provide additional details where required by the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. Additionally, ERDS operating procedures shall identify, define, or otherwise explain ERDS-design dependent details that are not specifically addressed in this document. ERDS operating procedures shall be sufficient for a Computer Security Auditor to conduct computer security audits.
2 DATA ARCHITECTURE

This section defines the payload contents and structure to be delivered, and when applicable, returned via an ERDS. An ERDS not only includes mechanisms for transporting Type 1 and/or Type 2 instruments, but also provides for the transport of uniform index information, as well as, information about the electronic signature of a notary. An ERDS also provides for the return, when applicable, of Type 1 and/or Type 2 instruments. Irrespective of the ERDS design, the minimum security requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met by protecting the ERDS payload structure and content.

2.1 THE ERDS PAYLOAD

All ERDS shall employ a modular payload structure, termed the “ERDS payload”, as shown in Figure 2 - ERDS Payload Structure. Modular construction shall allow any content within Type 1 and/or Type 2 instruments. A County Recorder shall list any restrictions on content in each contract with an Authorized Submitter.

![Figure 2 - ERDS Payload Structure](image)

2.2 ERDS PAYLOAD STRUCTURE

The standard structure of an ERDS payload shall consist of three components. The ERDS payloads may contain more components, but, at a minimum, standard ERDS payloads shall contain a component for each of the following:

1. Uniform index information.
2. One or more Type 1 or Type 2 instruments.
3. Information about the electronic signature of a notary.

Each ERDS payload shall be used to generate the Digital Signature of the individual preparing the ERDS payload. When the ERDS payloads are being prepared for delivery to a County Recorder, the Digital Signature shall be of the Authorized Submitter. When the ERDS payloads are being returned to an Authorized Submitter, the Digital Signature shall be of the County Recorder Designee. (Refer to Table 6 - Role Descriptions) This digital signature should not be
confused with the electronic signature of a notary or information about the electronic signature of a notary, but shall be transmitted and stored with the ERDS payload to which it pertains.

The ERDS payloads shall be constructed using a technology suitable for encrypting (as described in Sections 3, ERDS Processes and 4, Security Requirements), transmitting and storing the entire ERDS payload with the digital signature of the AuthorizedSubmitter or the County Recorder Designee preparing the ERDS payload.

Regardless of the ERDS design:

1. All ERDS payloads shall contain the standard components defined in this section.

2. The entire ERDS payload shall be used to generate the digital signature of the AuthorizedSubmitter or the County Recorder Designee.

3. The digital signature of the AuthorizedSubmitter or the County Recorder Designee shall be transmitted and stored with the ERDS payload to which it pertains.

Note: While the ERDS payload structure shall include uniform index information and information about the electronic signature of a notary, their use is detailed in Sections 2.4, Uniform Index Information and 2.5, Electronic Signature of A Notary, respectively.

2.3 **Type 1 and/or Type 2 Instruments**

These specifications do not limit the content or format of Type 1 and/or Type 2 instruments. An ERDS may be used to deliver any industry-standard or non-standard file format acceptable to the County Recorder; including, but not limited to: TIFF, GIF, JPEG, WMV, DOC, PDF, TXT, HTML, XML, or any other file format. Content restrictions shall be defined in the County Recorder's ERDS operating procedures and/or provided for in the ERDS design. Issues such as file format or size, color (versus black and white), graphics resolution, and other characteristics of Type 1 and Type 2 instruments are ERDS-design dependent and shall be at the discretion of the County Recorder.

The ERDA refers to two types of instruments that may be delivered as Type 1 and/or Type 2 instruments. For the purposes of ERDS, these instruments are categorized as "Type 1" and "Type 2." A "Type 1" instrument is defined to mean an instrument affecting a right, title, or interest in real property. A "Type 2" instrument is defined to mean an instrument of reconveyance, substitution of trustee, or assignment of deed of trust. The real estate industry refers to Type 1 and/or Type 2 instruments as "front-end" and "back-end" documents, respectively. Because these terms do not necessarily reflect the method of delivery (digital or digitized), the payload structure, or the file format of the document, the County Recorder shall establish ERDS operating procedures and/or incorporate features within the ERDS design in order to restrict the instrument type to meet the requirements of the ERDA. A summary of the relationships among statutory, industry, and technology terms is provided in Table 1 - Instrument Types.

<table>
<thead>
<tr>
<th>Instrument Type</th>
<th>Type 1</th>
<th>Type 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statute</td>
<td>ERDA Government Code Section 27395</td>
<td>ERDA Government Code Section 27397.5(a)</td>
</tr>
<tr>
<td>Purpose</td>
<td>Affect a right, title, or interest in real property</td>
<td>Instrument of reconveyance, substitution of trustee, or assignment of deed of trust</td>
</tr>
<tr>
<td>Industry Term</td>
<td>Front-end</td>
<td>Back-end</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Method</td>
<td>Digitized</td>
<td>Digital or Digitized</td>
</tr>
<tr>
<td>File Format</td>
<td>ERDS-design dependent</td>
<td>ERDS-design dependent</td>
</tr>
<tr>
<td>Criminal Record</td>
<td>Requires fingerprinting</td>
<td>Does not require fingerprinting</td>
</tr>
<tr>
<td>Background Check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payload Structure</td>
<td>Encrypted and hashed</td>
<td>Encrypted and hashed</td>
</tr>
</tbody>
</table>

The content of Type 1 and Type 2 instruments shall be as follows:

1. Type 1 Instruments; those affecting a right, title, or interest in real property, shall be delivered as digitized electronic records.

2. Type 2 Instruments; instruments of reconveyance, substitution of trustee, or assignment of deed of trust, shall be delivered as digitized electronic records or digital electronic records.

2.4 Uniform Index Information

All Type 1 or Type 2 instruments delivered via an ERDS, shall be capable of including uniform index information in the ERDS payload. The County Recorder shall decide on the contents of the uniform index information.

2.5 Electronic Signature of a Notary

The ERDS payloads shall be capable of including information about the electronic signature of the notary regardless of how the electronic signature of a notary is affixed by the notary, according to other applicable laws. When a signature is required to be accompanied by a notary’s seal or stamp, that requirement is satisfied if the electronic signature of the notary contains all of the following:

1. The name of the notary.

2. The words “Notary Public”.

3. The name of the county or other administrative district of a state where the bond and oath of office of the notary are filed.

4. The sequential identification number assigned to the notary, if given.

5. The sequential identification number assigned to the manufacturer or vendor of the notary’s physical and/or electronic seal, if available.
3 ERDS Processes

This section describes the processes for handling the ERDS payloads (i.e. login and transactions). Processes that are employed shall conform to the requirements described in this section. ERDS that include one or more servers shall conform to all of the process requirements in this section. Authorized Access ERDS that do not include a server shall, at a minimum, conform to Sections 3.2, ERDS Payload Submission Process and 3.3, ERDS Payload Retrieval Process. ERDS that include automated processing shall also conform to Section 3.4, Processing Multiple Transactions. Regardless of how an ERDS is implemented, the security and testing requirements outlined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met.

For each of the diagrams in this section, a gray hexagonal shape represents an interaction between a user and an ERDS. A white rounded rectangle indicates a process performed within an ERDS. The numbers correspond to the descriptions given in the tables following each diagram.

3.1 ERDS Login Process

An ERDS login process is depicted in Figure 3 - Login Process and described in Table 2 - Login Process Description. The login process is substantially the same for both the Authorized Submitter and the County Recorder Designee, to include the use of digital signatures for the purpose of authenticating users. (Refer to Sections 4.2.4, Certificate Authority and PKI and 4.3.1.2, Authentication Requirements for more information about ERDS authentication requirements.)

![Figure 3 - Login Process](image)

While the login process described in this document refers to the actions of, and subsequent responses to, a single user, the design of an ERDS may support multiple, simultaneous connections to and from multiple users. Each individual user shall be limited to one, and only one, active login session under a single ERDS user account. An individual user may have multiple screens active and displayed simultaneously, but all screens active for a user account shall be attributable to an active login session associated with that user account.
### Table 2 - Login Process Description

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Start</td>
<td>A user navigates to an ERDS. The identity of the user has not yet been established.</td>
</tr>
<tr>
<td>2 Establish Connection</td>
<td>ERDS establishes a secure connection with the user. Even though the identity of the user has not yet been established, this connection is intended to protect the user's password.</td>
</tr>
<tr>
<td>3 Authenticate Individual</td>
<td>Once a secure Internet session is established, the user is prompted for a user ID and password. ERDS provides a login screen and authenticates credentials entered by the user. If authentication fails, ERDS returns to the login screen and indicates that access is not authorized. If the user ID and password are authenticated, the user is prompted to confirm their identity using a digital signature. A proxy connection is established between the user and the ERDS server. Credentials and control of the session are transferred to the ERDS server. The ERDS server shall control authentication of the digital signature.</td>
</tr>
<tr>
<td>4 Assign Role</td>
<td>If the digital signature is authenticated, the identity of the user has been established. ERDS determines what role the user is authorized. Having determined a role, ERDS assigns privileges associated with that role for the duration of the session.</td>
</tr>
<tr>
<td>5 Create Interface</td>
<td>ERDS application software starts. ERDS builds an interface for the session based on the assigned role of the user.</td>
</tr>
<tr>
<td>6 Login Complete</td>
<td>The interface created for the session is presented to the user. The login process has completed. The ERDS server starts a timer for the session. If another command is not received before the timer reaches a timeout limit, the session shall be terminated.</td>
</tr>
<tr>
<td>Logout</td>
<td>Secure sessions shall be terminated if the authenticated user logs out or after a preset timeout limit, whichever occurs first. (For preset timeout limit criteria, refer to Section 4.5.2, Incident Response Procedures.)</td>
</tr>
</tbody>
</table>

### 3.2 ERDS Payload Submission Process

An ERDS payload submission process is depicted in Figure 4 - Payload Submission Process and described in Table 3 - Payload Submission Process Description. The process of an Authorized Submitter submitting an ERDS payload is substantially the same as a County Recorder Designee returning an ERDS payload. For the purposes of this section, a user is described as either a Sender or Recipient. A Sender is a user who is submitting an ERDS payload via the ERDS. A Recipient is a user who is retrieving ERDS payloads from the ERDS.
Table 3 - Payload Submission Process Description

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Submit Payload</td>
<td>The Sender indicates that a Type 1 or Type 2 instrument is ready to be submitted. Prior to this event, the Sender enters, selects or otherwise indicates the contents to be placed in an ERDS payload. For the return process, this step indicates that a Type 1 or Type 2 instrument is ready to be returned.</td>
</tr>
<tr>
<td>8 Assemble Payload</td>
<td>The ERDS interface collects the content into an ERDS payload structure.</td>
</tr>
<tr>
<td>9 Hash Payload</td>
<td>The ERDS payload is hashed to generate a message digest. This digest shall be used to (1) generate the digital signature of the Sender and (2) detect unauthorized changes that occur either during transmission to, or while in storage on, the ERDS server. The digital signature shall be submitted together with the ERDS payload. Note: The digital signature of the Sender is created by using the private key of the Sender to encrypt the message digest. Using the private key of the Sender assures the Recipient that the message digest was generated by the Sender.</td>
</tr>
<tr>
<td>10 Encrypt Payload</td>
<td>The ERDS interface encrypts the ERDS payload together with the digital signature of the Sender.</td>
</tr>
<tr>
<td>11 Transmit Payload</td>
<td>The ERDS interface relays the encrypted ERDS payload to the ERDS server.</td>
</tr>
<tr>
<td>12 Payload Submitted</td>
<td>For the Sender, the ERDS server acknowledges receipt of the encrypted ERDS payload and the ERDS interface indicates that transmission to, and storage on, the ERDS Server was successfully completed. If either transmission or storage failed, the ERDS interface indicates that transmission or storage failed. (Specific reasons for failure, transmission timeout and storage limits, and the text of error messages are ERDS-design dependent.) For a Recipient, this event indicates an ERDS payload has been submitted by a Sender and is ready for inspection.</td>
</tr>
</tbody>
</table>
3.3 ERDS Payload Retrieval Process

An ERDS payload retrieval process is depicted in Figure 5 - Payload Retrieval Process and described in Table 4 - Payload Retrieval Process Description. The process of retrieving a payload is substantially the same for both the Authorized Submitter and County Recorder Designee. For the purposes of this section, a user is described as either a Sender or Recipient. A Sender is a user who is submitting an ERDS payload to the ERDS. A Recipient is a user who is retrieving the ERDS payloads from the ERDS.

**Figure 5 - Payload Retrieval Process**

**Table 4 - Payload Retrieval Process Description**

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 Payload Submitted</td>
<td>For the Sender, the ERDS server acknowledges receipt of the encrypted ERDS payload and the ERDS interface indicates that transmission to, and storage on, the ERDS server was successfully completed. If either transmission or storage failed, the ERDS interface indicates that transmission or storage failed. (Specific reasons for failure, transmission timeout and storage limits, and the text of error messages are ERDS-design dependent.) For a Recipient, this event indicates an ERDS payload has been submitted by a Sender and is ready for inspection.</td>
</tr>
<tr>
<td>14 Retrieve Payload</td>
<td>If authorized, the Recipient indicates that an ERDS payload should be retrieved. The ERDS interface downloads the ERDS payload to a location indicated by the Recipient.</td>
</tr>
<tr>
<td>15 Decrypt Payload</td>
<td>The ERDS interface decrypts the ERDS payload together with the digital signature of the Sender. If the decryption fails, the ERDS interface indicates that the decryption failed. (Specific reasons for failure and the text of error messages are ERDS-design dependent.)</td>
</tr>
<tr>
<td>16 Authenticate Hash</td>
<td>The ERDS interface uses the public key of the Sender to decrypt the digital signature of the Sender and recover the digest of the ERDS payload. The ERDS interface hashes the ERDS payload and generates a second digest to compare with the digest recovered from the digital signature of the Sender. If the two digests are not identical, the ERDS interface indicates that a hash failure occurred. If an active session is still connected to the ERDS server, the ERDS interface transmits a message back to the ERDS server indicating a hash failure occurred.</td>
</tr>
<tr>
<td>PROCESS</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>17 Disassemble Payload</td>
<td>If the two digests are identical, the ERDS interface extracts the contents of the ERDS payload and performs a validity check to ensure the contents are free of malware. The anti-malware interface warns the Recipient if the contents are not free of malware. (Specific anti-malware interfaces, the text of error messages, and actions allowed in response to a malware warning are ERDS-design dependent.) If the contents are free of malware, the ERDS interface prompts the Recipient for a location to store the contents.</td>
</tr>
<tr>
<td>18 Payload Delivered</td>
<td>The ERDS interface indicates that the ERDS payload was successfully delivered.</td>
</tr>
</tbody>
</table>

3.4 **PROCESSING MULTIPLE TRANSACTIONS**

In implementing an ERDS, the County Recorder may add capabilities to process multiple Type 1 or Type 2 instruments. As examples, and for illustrative purposes only, an ERDS may be designed to process multiple Type 1 or Type 2 instruments in any or all, of the following ways:

1. By inserting multiple Type 1 or Type 2 instruments into a single ERDS payload.
2. By repeated processing of Type 1 or Type 2 instruments from a single source, such as a scanner or directory.
3. By repeated processing of Type 1 or Type 2 instruments based on a list of file locations.

The automated processing of multiple Type 1 or Type 2 instruments is subject to the following restrictions:

1. Repeated processing from a single source or a list of files shall result in separate ERDS payloads — one for each file.

Additionally, a County Recorder may establish an automated process that retrieves, decrypts, and checks the contents of submitted ERDS payloads. The details of implementing such an automated process are ERDS-design dependent; however, the security and testing requirements outlined in this document shall be met.
4 SECURITY REQUIREMENTS

This section describes the security requirements for protecting an ERDS. Processes and technologies employed in implementing an ERDS, pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, shall conform to the requirements as defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. All ERDS shall conform to Section 4.2, Minimum Security Requirements. Regardless of how an ERDS is implemented, the security and testing requirements outlined in this document shall be met.

This section details the baseline requirements and standards for administrative, physical and technical security controls.

4.1 INTRODUCTION

The security of any system is implemented through a combination of administrative, physical, and technical controls. Administrative controls protect the security of systems by implementing management policies and procedures. Physical controls protect the security of systems by limiting physical access to hardware and media. Technical controls protect the security of systems by limiting logical access to software and data. For an ERDS, technical controls protect the integrity of system configurations and the security of information contained in Type 1 and Type 2 instruments.

4.1.1 Conceptual Overview

ERDS shall protect the security of data, both in transmission and storage, on ERDS-designated components, as well as, provide mechanisms to detect unauthorized changes and verify the integrity of information contained in the ERDS payloads.

For illustrative purposes, a diagram showing the major components of an ERDS are depicted in Figure 6 - Conceptual Security Infrastructure and described in Table 5 - Conceptual Security Infrastructure Descriptions. Actual ERDS implementations may vary from the configuration depicted in Figure 6 - Conceptual Security Infrastructure. Implementation details are at the discretion of the County Recorder; however, all requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be required for system certification.

![Figure 6 - Conceptual Security Infrastructure](image-url)
<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Type 1 and/or Type 2 instruments</td>
<td>Type 1 and/or Type 2 instruments prepared for submission. The preparation of Type 1 and/or Type 2 instruments is not a process within an ERDS.</td>
</tr>
<tr>
<td>2 Workstation</td>
<td>A computer used to connect to, and interact with, an ERDS</td>
</tr>
<tr>
<td>3 Authorized Submitter</td>
<td>A party and his/her employees that has entered into a contract with a County Recorder and assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Authorized Submitter may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.</td>
</tr>
<tr>
<td>4 Authorized Submitter Network</td>
<td>The network an Authorized Submitter uses to connect to an ERDS. Networks shall meet the minimum security requirements described in Section 4.3.3, Network Security.</td>
</tr>
<tr>
<td>5 The Internet</td>
<td>A global network of computer systems interconnected through the use of commonly accepted protocols standardized through the Internet Engineering Task Force.</td>
</tr>
<tr>
<td>6 Certificate Authority</td>
<td>A certificate authority issues digital certificates for the purpose of establishing secure Internet sessions between an Authorized Submitter and an ERDS. Certificate authorities also validate digital certificates presented as proof of identity.</td>
</tr>
<tr>
<td>7 County Recorder Network</td>
<td>The network a County Recorder Designee uses to connect to an ERDS. Networks shall meet the minimum security requirements described in Section 4.3.3, Network Security.</td>
</tr>
<tr>
<td>8 Proxy Server</td>
<td>Server that functions as the interface between an Authorized Submitter and an ERDS server.</td>
</tr>
<tr>
<td>9 ERDS Server</td>
<td>Computer hardware, software, and storage media used by the County Recorder to implement an ERDS. The ERDS server executes the primary functionality of the ERDS application software. It includes software for encrypting, decrypting, hashing, submitting, and when applicable, returning the ERDS payloads. It also includes storage media for the ERDS payloads in the process of being delivered to the County Recorder or, when applicable, being returned to the Authorized Submitter. Separate physical servers dedicated to performing ERDS server functions are not required provided that ERDS server functions can be isolated from other server functions, as evidenced by audit</td>
</tr>
<tr>
<td>10 ERDS Payloads</td>
<td>An electronic structure designed for the purpose of delivering digital electronic records or digitized electronic records to a County Recorder via an ERDS. The structure is also used to return, when applicable, digital electronic records or digitized electronic records to an Authorized Submitter via an ERDS.</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11</td>
<td>County Recorder Designee</td>
</tr>
<tr>
<td></td>
<td>A Secure Access role assigned by the County Recorder to retrieve and when applicable, return submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting</td>
</tr>
<tr>
<td>12</td>
<td>Public Record</td>
</tr>
<tr>
<td></td>
<td>The repository of Type 1 and Type 2 instruments. An ERDS shall have no capabilities to modify, manipulate, insert, or delete information in the public record. The public record is outside of the ERDS boundary and is depicted for illustrative purposes only.</td>
</tr>
</tbody>
</table>

### 4.2 MINIMUM SECURITY REQUIREMENTS

All ERDS, for Type 1 and Type 2 instruments, shall employ the minimum security requirements described in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. Additional security requirements for Type 1 ERDS are contained in Section 4.3, Additional Security Requirements for Type 1 ERDS.

All ERDS:

1. Shall employ up-to-date anti-malware software.
2. Shall employ cryptography, including hashing, encryption, and decryption.
3. May not employ either compromised or weak encryption algorithms.
4. May not contain known vulnerabilities.
5. May not be susceptible to published exploits.

Standards and guidelines established in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 included in this document are based on Federal Information Processing Standards (FIPS) and National Institute of Standard and Technology (NIST) publications including: NIST Special Publication 800-88, Guidelines for Media Sanitization (publication date September 2008); FIPS 180-4, Secure Hash Standard (publication date March); FIPS 140-2, Security Requirements for Cryptographic Modules (publication data May 2001 with a change notice dated December 2002); FIPS 197, Advanced Encryption Standard (publication date November 2001); FIPS 198-1, the Keyed-Hash Message Authentication Code (HMAC) (publication date July 2008); NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date August 2013); NIST Special Publication 800-70 Revision 2, National Checklist Program for IT Products-Guidelines for Checklist Users and Developers (publication date February 2011); FIPS 186-4, Digital Signature Standard (DSS) (publication date, July 2013).

### 4.2.1 Data Integrity

All ERDS for either Type 1 or Type 2 instruments shall assure submitted documents do not contain content that draws data or images from sources external to the digital electronic record and/or digitized electronic record. Prior to submitting, or when applicable, returning an ERDS payload, content shall be scanned and or reviewed for active content including; but, not limited to, the following:

1. Viruses
2. Worms
3. Trojan Horses
4. Spyware
5. Adware
6. ActiveX components
7. Java Script
8. Java components
9. HTML encoded hyperlinks
10. Any other executable software

All ERDS shall employ up-to-date anti-malware software on all workstations and servers employed for processing ERDS payloads. Active content detected by anti-malware shall be removed as soon as it is detected. Active content that cannot be removed shall be disabled. The technologies employed and the points in the delivery process where active content is removed and/or disabled are ERDS-design dependent.

4.2.2 Payload Protection

4.2.2.1 Payload Confidentiality

4.2.2.2 All ERDS for Type 1 or Type 2 instruments, shall employ encryption both in transmission and storage, until decrypted by the intended recipient to protect the confidentiality of ERDS payloads. The encryption algorithms approved for ERDS are specified in CCR Title 11, Division 1, Chapter 18, § 999.137 (a). Payload Integrity

All ERDS for Type 1 or Type 2 instruments, shall use hashing to protect the integrity of the ERDS payloads. The hash function approved for the ERDS payloads is the Secure Hash Algorithm (SHA) defined in CCR Title 11, Division 1, Chapter 18, § 999.137 (b).

4.2.2.3 Payload Authenticity

All ERDS for Type 1 or Type 2 instruments, shall use Digital Signatures to assure the authenticity of ERDS payloads. Hash values that are encrypted using asynchronous techniques are known as Digital Signatures. The signing functions approved for ERDS payloads are defined in the CCR Title 11, Division 1, Chapter 18, § 999.137 (c).

4.2.3 Cryptographic Key Generation

Cryptographic modules used for generating encryption keys shall meet the requirements of Security Level 2 defined in FIPS 140-2, "Security Requirements for Cryptographic Modules" (publication date May 2001, with a change notice dated December 2002).

4.2.4 Certificate Authority and PKI

The County Recorder shall establish a Public Key Infrastructure (PKI) to ensure all ERDS users are uniquely identified and to protect the integrity and authenticity of ERDS payloads. The County Recorder shall determine and implement a PKI strategy based on the following guidelines:

1. The RSA Algorithm using a minimum key-length of 1024 bits.
2. The Advanced Encryption Algorithm using a minimum key-length of 128 bits as defined in FIPS 197, Advanced Encryption Standard (publication date November 2001).
A public/private key-pair shall be generated for each user authorized a role in handling ERDS payloads. In a PKI, public and private keys are used in encryption, decryption and signing processes. Cryptographically-related keys are referred to as a public/private key pair.

For Type 1 instruments, the private key in the pair shall be issued to the user and employed to create digital signatures, both for use during login and for assuring the integrity of the ERDS payloads. The public key shall be used to authenticate the user during login and to verify the integrity and authenticity of the ERDS payloads.

For Type 2 instruments, the private key in the pair shall be issued to the user and employed to create digital signatures and for assuring the integrity of the ERDS payloads. The public key shall be used to authenticate the user and to verify the integrity and authenticity of the ERDS payloads.

For Type 1 instruments, authentication shall consist of two factors: (1) the user ID and password associated with an approved user account and (2) the user's PKI identity credentials. For Type 2 instruments, authentication shall be based on the user's PKI identity credentials.

Resources and means for establishing a PKI for either Type 1 or Type 2 instruments shall be at the discretion of the County Recorder, but, commercially available certificate authorities, if employed, may be on the list of certification authorities approved by the California Secretary of State. The California Secretary of State maintains an approved list of digital signature certification authorities at [http://www.sos.ca.gov/digssig/digssig.htm](http://www.sos.ca.gov/digssig/digssig.htm).

### 4.2.5 Securing ERDS Payloads

The process of securing ERDS payloads for Type 1 or Type 2 instruments during submission is shown in Figure 7 - Securing ERDS Payloads. The process of securing the ERDS payloads during and when applicable, the return, is identical except for the use of encryption keys. The configuration and algorithms depicted in Figure 7 are for illustration purposes only; however, all ERDS shall encrypt the ERDS payloads.

After an Authorized Submitter has created an ERDS payload, the ERDS payload is hashed using SHA. The resulting hash value, called a digest, is encrypted using RSA and the private key of the Authorized Submitter — creating the digital signature of the Authorized Submitter.

![Figure 7 - Securing ERDS Payloads](image)

The ERDS payload and digital signature of the Authorized Submitter are encrypted using AES and the ERDS Payload Key, delivered from an ERDS server. The ERDS Payload Key is stored on an ERDS server so that a County Recorder Designee can decrypt the ERDS payload.

Electronic Recording Delivery System  
Baseline Requirements and Technology Standards Handbook  
Page 24 of 56  
February 2015
(Note: In an ERDS, the Payload Key is the public key of a County Recorder public/private key-pair.)

The encrypted ERDS payload is transmitted to and stored on an ERDS server. Encrypted ERDS payloads are relayed through the proxy server which acts as a proxy between the Authorized Submitter and the ERDS server. The ERDS server receives and stores encrypted ERDS payloads, so that a County Recorder Designee can use the ERDS Payload Key to decrypt the ERDS payload. (Note: In an ERDS, the County Recorder Designee shall need to use the private key of a County Recorder public/private key-pair.)

4.2.6 Validating ERDS Payloads

The process of validating the ERDS payloads for Type 1 or Type 2 instruments is shown in Figure 8 - Validating ERDS Payloads. The process of validating the ERDS payloads during return, when applicable, is identical except for the use of encryption keys. The configuration and algorithms depicted in Figure 8 are for illustration purposes only.

![Diagram of ERDS Payload Validation](image_url)

Figure 8 - Validating ERDS Payloads

The decryption, hash authentication and validity checking of the ERDS payloads are ERDS-design dependent. Decryption and hash authentication processes complement the corresponding encryption and signing processes, respectively. Validity checking is based on the contents of the ERDS payload. However, all ERDS shall generate and log errors for decryption, hash authentication and validity check failures.

4.2.7 Workstation Security

For all ERDS that serve Type 1 or Type 2 instruments, the County Recorder shall ensure that all endpoints are secure. As such, workstations used to submit, retrieve, or if applicable, return the ERDS payloads are protected from unauthorized use and access. At a minimum, all workstations shall meet all the following requirements:

1. Anti-malware software configured to start on system boot-up.
2. Operating system software with the most up-to-date patches and hot-fixes.
3. Host-base firewall configured to restrict inbound and outbound connections.

For ERDS that serve Type 1 instruments only, installed applications shall be limited to the purpose of performing the necessary operational needs of the recording process as defined by the County Recorder. The County Recorder shall include this requirement as a mandatory
provision in all contracts with Authorized Submitters whom shall ensure that an Agent, if any, complies with these requirements. The contents of the contract provision are subject to audits and local inspections.

4.2.8 Media Security

The ERDS payloads and encryption keys for either Type 1 or Type 2 instruments shall be encrypted when stored on any storage media. The encryption employed for protecting the ERDS payloads and encryption keys in storage, shall conform to the standards for transmitting the ERDS payloads as described in Section 4.2.2, Payload Protection.

Storage media includes, but is not limited to, fixed disks, removable disks and portable devices. Fixed and removable disks for either Type 1 or Type 2 instruments, shall be sanitized as defined in NIST Special Publication 800-88, “Guidelines for Media Sanitization” publication date September 2006, prior to reallocating ERDS hardware or storage media to other purposes.

Unauthorized access or changes to storage media and improper sanitization of storage media shall be reported as required in Section 4.5.2, Incident Response Procedures.

4.3 ADDITIONAL SECURITY REQUIREMENTS FOR TYPE 1 ERDS

This section describes additional security requirements that shall be implemented for Type 1 ERDS. ERDS that include one or more servers shall conform to all of the security requirements in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

This section describes the security requirements that shall be implemented for Type 1 ERDS that delivers Type 1 instruments. Pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, Type 1 instruments shall meet the security requirements in Section 4.2, Minimum Security Requirements, and additionally meet the requirements specific to Type 1 instruments described in this Section. ERDS that serve both Type 1 and Type 2 instruments shall be required to meet the additional security requirements of Type 1 instruments.

4.3.1 Access Control

A combination of security mechanisms shall be applied to protect the safety and security of the ERDS. Access control failures shall be logged and/or documented and reported according to Section 4.5.2, Incident Response Procedures.

4.3.1.1 Identification Requirements

Pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, ERDS that serve Type 1 and Type 2 instruments shall be required to meet the following additional identification security requirements required for Type 1 instruments. For ERDS that serve Type 1 instruments, authentication shall consist of two factors: (1) the user ID and password associated with an approved user account and (2) the user’s PKI identity credentials (as defined in Section 4.2.4, Certificate Authority and PKI).

User accounts may be implemented as part of a network authentication and authorization system, available to the County Recorder as an integral part of an ERDS server, or by other means at the discretion of the County Recorder as long as the following requirements are met:

1. Each ERDS user shall be uniquely identified.
2. Shared user accounts and identity credentials shall be prohibited.
3. User IDs shall either be based on the verified name of the user or a pseudonym approved by the County Recorder.
4. User accounts shall be associated with ERDS roles.

4.3.1.2 Authentication Requirements

Pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9, ERDS that serve Type 1 and Type 2 instruments shall be required to meet all of the additional authentication security requirements required for Type 1 instruments. The standard for electronic authentication shall be based on NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013). NIST defines electronic authentication as "the process of establishing confidence in user identities electronically presented to an information system."

Authentication shall meet the following requirements:

1. The standard for electronic authentication shall employ two factors: (a) a token containing a cryptographic key (e.g. a digital certificate) issued to the user and (b) a password associated with the user ID.

2. Authentication assurance shall meet Level 3 or higher, as defined in NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013).

3. Any of the token methods described in NIST Special Publication 800-63-2, Electronic Authentication Guideline (publication date, August 2013), may be used provided that authentication assurance Level 3 or higher is achieved.

Password creation, protection, maintenance, processing and handling shall adhere to the Password Policy contained in the "California Counties 'Best Practices' Information Security Program" (publication date March 2002).

4.3.1.3 Authorization Requirements

Access to the ERDS payloads shall be based on the authorization standards defined in this section. The ERDS payloads submitted by an Authorized Submitter or Agent shall be retrievable by any County Recorder Designee.

4.3.1.3.1 Role-Based Access Control

Access to an ERDS that serve either Type 1 or Type 2 instruments shall be controlled using a role-based access control system. Textual disclaimers or verbal disclaimers alone shall not be sufficient to control access to digital electronic records and digitized electronic records under the control of an ERDS. A role is defined as a security mechanism, method, process or procedure that defines specific privileges controlling the level of access to an ERDS. ERDS roles are described in Table 6 - Role Descriptions.
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Access</td>
<td>A role assigned by the County Recorder to an Authorized Submitter and Agent, if any, who is authorized to use ERDS for only Type 2 instruments. This role does not require fingerprinting.</td>
</tr>
<tr>
<td>Computer Security Auditor</td>
<td>(1) DOJ approved computer security personnel hired by the County Recorder to perform independent audits. (2) A role assigned by the County Recorder to the Computer Security Auditor who is authorized to review transaction logs and conduct tests on computer security mechanisms. A Computer Security Auditor may not be an Authorized Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software. This role requires fingerprinting. A Computer Security Auditor shall be issued a certificate of approval by the ERDS Program.</td>
</tr>
<tr>
<td>County Recorder Designee</td>
<td>A Secure Access role assigned by the County Recorder to retrieve, and, when applicable, return of the submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.</td>
</tr>
<tr>
<td>ERDS Account Administrator</td>
<td>A secure access role assigned by the County Recorder to an individual who is authorized to configure accounts, assign roles, and issue credentials. An ERDS Account Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.</td>
</tr>
<tr>
<td>ERDS System Administrator</td>
<td>A secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software, network settings, and to maintain ERDS security functions. An ERDS System Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent, or Vendor of ERDS Software. This role requires fingerprinting.</td>
</tr>
<tr>
<td>Physical Access</td>
<td>Access granted to an individual who has physical access to an ERDS server. This level of access requires fingerprinting with the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls.</td>
</tr>
<tr>
<td>Secure Access</td>
<td>A role assigned by the County Recorder to an individual which requires fingerprinting to: 1) an Authorized Submitter and Agent, if any, who are authorized to use an ERDS for both Type 1 and 2 instruments (excludes Type 2 instruments only) or Type 1 instruments only; 2) a Computer Security Auditor hired by the County Recorder to perform independent audits; 3) an ERDS System Administrator who is authorized to configure hardware, software, and network settings; 4) an ERDS Account Administrator who is authorized to configure accounts, assign roles, and issue credentials; 5) an individual who is granted physical access to an ERDS server; 6) a County Recorder Designee authorized to retrieve, and, when applicable, return the submitted ERDS payloads.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vendor of ERDS Software (or</td>
<td>A person and personnel, supporting and/or acting on behalf of the certified Vendor of ERDS Software who sells, leases, or grants use of, with or without compensation therefore, a software program for use by counties for establishing an ERDS. A Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, County Recorder Designee, or internal county resource used as a Developer of an ERDS in lieu of a Vendor. This role requires fingerprinting.</td>
</tr>
</tbody>
</table>

Irrespective of design, the access control system shall control the following characteristics:

1. Whether or not a session may be established with an ERDS.

2. What ERDS payloads will be displayed.

3. Whether or not the ERDS payloads may be submitted, retrieved, and, when applicable, returned.

4. Whether Type 1 or Type 2 instruments may be included within an ERDS payload.

The County Recorder may define limits, if any, on the day of the week and time of day ERDS transactions can be conducted. Limits may be implemented as part of the access control system or be set by contract or agreement.

The County Recorder shall also be responsible for controlling the assignment of user accounts and identity credentials. User accounts and identity credentials shall be issued to the person, and a role shall be assigned to control transactions performed under that user account. The security system shall be capable of controlling this electronic access based on the roles authorized at the time a user successfully logs into an ERDS. Persons granted access shall be subject to fingerprinting depending on the role requested.

Shared user accounts may not be issued. At no time shall more than one person be authorized access to an ERDS using a single ERDS user account or set of identity credentials. Each person shall be uniquely identified. If a user's status changes, so that access to an ERDS is no longer required, the user's ERDS account and identity credentials shall be disabled and revoked for the purposes of an ERDS. ERDS user accounts and identity credentials are non-transferable.

Identity credentials shall be recognized across ERDS provided that the County Recorders involved have consented, by mutual agreement, to recognize the credentials. The details of the agreements shall be at the discretion of the County Recorders, however, the agreement shall be made part of the ERDS operating procedures of all County Recorders who are party to the agreement.

ERDS users may be authorized multiple roles. The security system shall be capable of controlling access based on the roles authorized at the time a user successfully logs into an ERDS. Whereas one ERDS may be used in a collaborative system, the security system of a Multi-County ERDS shall be capable of controlling access based on the county to which the ERDS payloads are to be delivered and, when applicable, returned. (Refer to Section 1.3.2, Functionality, for more information about Multi-County ERDS.)

With the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls, persons granted physical access to an ERDS server shall be subject to fingerprinting, but may not be assigned a login role and may
not be granted access to the ERDS payloads unless authorized by the County Recorder. (Refer to Section 4.3.4, Physical Security.)

4.3.1.3.2 Authorized Submitter and Agent
An Authorized Submitter and Agent, if any, shall be limited to those privileges granted by the County Recorder. The Authorized Submitter and Agent are prohibited from submitting the ERDS payloads on behalf of another Authorized Submitter or Agent, unless the details of the agreement are specified in the contract with the County Recorder. Regardless of the details of the agreement, shared user accounts may not be issued.

An Agent named in more than one contract with a County Recorder shall be required to indicate which Authorized Submitter is represented in a transaction. An ERDS shall control Agent transactions through the use of unique credentials (user ID, password, and token) or other means, provided that an accounting of transactions can be provided to the Authorized Submitter on whose behalf the Agent is acting.

Authorized Submitters may employ a third-party vendor as an Agent provided that the third-party vendor is neither a Computer Security Auditor nor a Vendor of ERDS Software. (Refer to the definition of “Agent” in Section 7, Acronyms and Definitions)

4.3.1.4 Accountability Requirements
Auditable ERDS events shall be logged for purposes of audit, local inspection and review, incident response and reporting. Auditable events may be logged using automated or manual processes. Logs shall be safely stored and maintained in a manner that ensures their availability for a period of at least 24 months, or at least one computer security audit, whichever occurs later. Incident response and reporting requirements are detailed in Section 4.5.2, Incident Response Procedures.

4.3.1.4.1 Session Activities
For Type 1 instruments, the following authorized activities shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. Login successes and failures.
2. Sessions starts and ends.
3. Session timeout (e.g. inactive in excess of 30 minutes).
4. The ERDS payload transactions submittals, retrievals, and when applicable, returns (as described in Section 4.3.1.4.3, Transaction Activities).

4.3.1.4.2 Unauthorized Activities
For Type 1 instruments, the following unauthorized activities shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

Unauthorized access attempts, including, but not limited to:

1. Unauthorized users attempting access, either physical or logical to ERDS storage areas.
2. Any user attempting to use ERDS software and/or interfaces in a non-ERDS manner.

For Type 1 and Type 2 instruments, the use of expired or revoked credentials shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

4.3.1.4.3 Transaction Activities
For Type 1 and Type 2 instruments submitted, retrieved and when applicable, returned, the following transaction activity information shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. Unique name of the ERDS payload.
2. Dates and times the ERDS payload was submitted, retrieved, and when applicable, returned.
3. Identity of the individual who submitted, retrieved and when applicable, returned the ERDS payload.
4. Name of the organization that the individual represented while submitting, retrieving and when applicable, returning the ERDS payload.
5. Success or failure of decryption, hash failure, and validation.

Note: The unique name of the ERDS payload is ERDS-design dependent.

4.3.1.4.4 Accountability Failures

Auditable events shall never overwrite other logged events. Additionally, ERDS servers shall not accept Type 1 or Type 2 instruments if:

1. Auditable events cannot be logged.
2. Logs consume 95% or more of the storage space allocated for logging.
3. Logs cannot be safely stored.

4.3.1.5 Administration Requirements

A County Recorder shall establish ERDS operating procedures for, and have responsibility over, the day-to-day administration of ERDS accounts, roles and cryptographic keys. ERDS administration shall be performed by one or more individuals assigned as the ERDS System Administrator and/or ERDS Account Administrator.

The following administration activities for Type 1 instruments shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. ERDS account creation, modification, deletion, suspension, termination or revocation, whether authorized or not.
2. Hardware and software configuration changes.

Hardware and software configuration changes shall be based on the inventory of all hardware and software installed on, or attached to, an ERDS since the most recent audit.

4.3.2 Server Security

Servers employed for the purpose of implementing an ERDS may be dedicated to ERDS functions or integrated with other servers. Separate physical servers dedicated to performing ERDS server functions are not required, provided that the ERDS server functions can be isolated from other server functions, as evidenced by audit.

4.3.2.1 Proxy Server

An ERDS shall employ an ERDS proxy server. The purpose of the proxy server shall be to provide a public interface to an ERDS and provide proxy services between the Authorized Submitter and the ERDS server.

The proxy server shall:
1. Establish secure Internet sessions.
2. Authenticate user ID and password credentials.
3. Transfer and/or relay ERDS requests received via authenticated secure Internet sessions to the ERDS Server.
4. Be physically and logically separated from the ERDS server.
Proxy servers may not execute an ERDS functionality except as described above.

4.3.2.2 ERDS Server Security

The ERDS server shall communicate via secure sessions through the proxy server when interoperating via the Internet. At a minimum, sessions between the proxy server and the ERDS server shall be protected using a secure protocol, as defined in Section 4.3.3.1, Transmission Security/Confidentiality. Direct logins from the Internet to an ERDS server is prohibited.

The ERDS server shall:
1. Run the ERDS application software.
2. Store the ERDS payloads.
3. Authenticate the ERDS credentials.
4. Control the ERDS access based on assigned roles.
5. Log the ERDS transactions.

4.3.2.3 Server Hardening

ERDS servers shall be configured to prevent unauthorized access, modification or use. The County Recorder shall establish standards for “hardening” servers by selecting a checklist or guideline and customizing it to meet the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

The County Recorder shall ensure that all county servers used for an ERDS are “hardened” according to one of the following checklists or guidelines:

1. NIST Special Publication 800-70 Revision 2, Security Configuration Checklists Program for IT Products-Guidelines for Checklist User and Developers (publication date, February 2011).
2. Manufacturer's recommended guidelines for securing their products to afford the highest level of protection.

At a minimum, ERDS servers shall:
1. Be “hardened” according to the standards establish by the County Recorder.
2. Have a host-based file integrity checking system configured to alert the ERDS System Administrator of an operating system file change to the ERDS server.
3. Have anti-malware software installed and operating to protect the server.

4.3.2.4 Server Events

The following server events shall be logged and reported according to Section 4.5.2, Incident Response Procedures:
1. Server failures, including, but not limited to, hardware, software, and network component failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.

2. Events for which the ERDS System Administrator is alerted of possible or actual intrusion.

3. Unauthorized changes to the ERDS operational configuration.

4. Hardware or software configuration changes.

5. For Type 1 only, unauthorized access attempts, including, but not limited to: unauthorized users attempting access, either physical or logical, to ERDS storage areas.

6. Use of expired or revoked credentials.

7. For Type 1 only, privilege elevation.

8. For Type 1 only, unauthorized visitor access to an ERDS server or a logged-in session.

9. ERDS accounts locked out and/or disabled due to failed consecutive login attempts.

10. Auditable events overwrite other logged events.

11. For Type 1 only, ERDS account creation, modification, deletion, suspension, termination or revocation whether authorized or not.


15. Type 1 or Type 2 instrument submitted unencrypted.

16. Type 1 instrument submitted as a Type 2 instrument or vice versa.

17. Type 1 instrument submitted via an Authorized Access ERDS.

18. Unauthorized transactions submitted via ERDS, including but not limited to, instruments that are neither Type 1 nor Type 2.

19. For Type 1 only, network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.

20. Inability to obtain and employ cryptography, including hashing, encryption and decryption.

21. For Type 1 only, discovery of newly published vulnerability existing on a certified ERDS.

22. Discovery of susceptibility to newly published exploit.

23. Inability to obtain and employ the most up-to-date patches and hot-fixes.

24. Any other event that compromises the safety or security of an ERDS.

4.3.3 Network Security

The integrity and reliability of an ERDS depends on security measures applied at the network level. An ERDS shall use a combination of networks, including the Internet. ERDS components shall be protected from unauthorized network activity as described in this section.
4.3.3.1 Transmission Security/Confidentiality

ERDS transactions via any network shall be protected using encryption. Data packets transmitted via networks are easily captured and compromised, if unencrypted. Two basic processes that shall be protected during any ERDS session are the login sequence and the transfer of the ERDS payloads.

Prior to beginning a login sequence, a secure connection shall be established in order to protect passwords. The standard for establishing secure connections is the Transport Layer Security (TLS) protocol as described in NIST Special Publication 800-63-2, “Electronic Authentication” (publication date, August 2013). At a minimum, 128-bit encryption shall be used to establish secure TLS sessions, as described in FIPS 197, “Advanced Encryption Standard” (publication date November 2001). ERDS may not employ “Basic” or Hypertext Transport Protocol referred to commonly as “HTTP” authentication to transmit passwords.

Once a secure connection is established and the user authenticated, a proxy connection is established between the user and the ERDS server. Credentials and control of the session are transferred to the ERDS server.

Once established, the secure connection shall be maintained as long as ERDS transactions are conducted. Secure connections shall be terminated if the authenticated user logs out or after a preset timeout limit of not more than 30 minutes, whichever occurs first. (For preset timeout limit criteria, refer to Section 4.5.2, Incident Response Procedures.)

The County Recorder shall ensure digital certificates are available to establish secure connections between users and the proxy server and between the proxy server and the ERDS server.

4.3.3.1.1 Transmission Integrity

An ERDS shall employ message authentication codes (MAC) to assure the authenticity of encrypted ERDS packets. MACs shall conform to the standard defined in FIPS 198-1, “The Keyed-Hash Message Authentication Code (HMAC)” (publication date, July 2008).

4.3.3.2 Unauthorized Network Traffic

Network security controls shall be implemented to prevent unauthorized network traffic from reaching the ERDS components. At a minimum, network devices shall do all of the following:

1. Employ stateful packet inspection.
2. Block unauthorized connections by limiting connection attempts addressed to the ERDS components to those necessary for ERDS operation.
3. Be designed and configured to fail “closed” rather than “open”.
4. Detect possible intrusions; and, if a possible intrusion is detected, alert the ERDS System Administrator and take action to prevent the intrusion.

4.3.3.3 Alternative Transmission Methods

An ERDS may employ alternative transmission methods, which shall meet one of the following standards:

1. Virtual Private Networks (VPNs).
2. “Dedicated circuits” as employed in existing government systems.
Irrespective of an ERDS design, the security and testing requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met.

4.3.3.4 Network Events

For Type 1 instruments, the following network events shall be logged and reported according to Section 4.5.2, Incident Response Procedures:

1. Network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.
2. Events for which the ERDS System Administrator is alerted of possible or actual intrusion
3. Unauthorized changes to the ERDS operational configuration.

4.3.4 Physical Security

The site housing the ERDS server shall be protected from unauthorized physical access. The server shall be locked in such a manner as to prevent unauthorized physical access. Disks and backup tapes containing ERDS software and/or data (including encryption keys) shall be locked in a cabinet or other container when not in use.

The County Recorder shall ensure precautions are employed to protect the ERDS server, software, and data from theft, damage and/or unauthorized access or use. Precautions may be defined in a County Recorder's ERDS operating procedures or may be established by mutual agreement between the County Recorder and the entity housing the ERDS server.

At a minimum, ERDS operating procedures and/or agreements shall provide for the following:

1. All requests for physical access to an ERDS server are subject to disapproval by the County Recorder. For an ERDS involving a shared, multi-purpose server, the County Recorder may not have overall authority to approve physical access; however, the County Recorder shall retain disapproval authority in an agreement involving shared multi-purpose servers.
2. Persons who are authorized physical access to an ERDS server require fingerprinting.
3. An inventory that accounts for all keys, whether physical or electronic, used for locking and unlocking physical access to an ERDS server, software and/or data shall be completed at least every 90 calendar days.
4. During audits, the Computer Security Auditor shall be allowed to inspect all access requests and inventory reports that occurred within a 2-year period prior to the start of an audit.
5. During local inspections, ERDS Program staff shall be allowed to inspect all access requests and inventory reports that occurred within a 2-year period prior to the start of a local inspection.

4.4 Security Checklists

The County Recorder shall select checklists for hardening ERDS components through the "NIST Special Publication 800-70 Revision 2 National Checklist Program for IT Products- Guidelines for Checklist Users and Developers" (publication date February 2011). Selected checklists shall be consistent with the ERDS design.
4.5 INCIDENT RESPONSE

For the purposes of this Section, the following definitions apply:

1. "Auditable" means an auditable ERDS event, as referenced in Section 4.3.1.4, Accountability Requirements.
2. "Incident" means an event that may have compromised the safety or security of an ERDS.
3. "Reportable" means an incident that has resulted in the compromise of the safety or security of an ERDS and shall be reported to the ERDS Program

4.5.1 Incident Reporting

Any incident that compromises the safety or security of an ERDS shall be reported by the County Recorder to the County Board of Supervisors, District Attorney(s), Computer Security Auditor and the ERDS Program according to procedures outlined in the ERDS System Certification Handbook. All incidents shall be documented for inclusion as part of a computer security audit.

4.5.2 Incident Response Procedures

The County Recorder shall establish an ERDS operating procedures for handling and responding to incidents. The ERDS operating procedures shall conform to the requirements listed in Table 7 - Incident Response Criteria and Reporting Requirements. Reportable incidents, as indicated in Table 7, shall result in a Modified System Incident Audit, as defined in Section 5.2.4, Modified System Incident Audit.

Table 7 - Incident Response Criteria and Reporting Requirements

<table>
<thead>
<tr>
<th>A. SESSION ACTIVITIES</th>
<th>AUDITABLE</th>
<th>INCIDENT</th>
<th>REPORTABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Login successes and failures.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2 Sessions starts and ends.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3 Session timeout (e.g. inactive in excess of 30 minutes).</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4 ERDS payload submittals, retrievals and when applicable, returns (as described in 4.3.1.4.3, Transaction Activities).</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. SESSION FAILURES</th>
<th>AUDITABLE</th>
<th>INCIDENT</th>
<th>REPORTABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 If an ERDS transaction is not conducted within a preset timeout limit, the session will be terminated. Criteria for setting the timeout limit shall be established by the County Recorder; however, the maximum preset timeout limit is 30 minutes.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2 If an ERDS session is terminated within a preset timeout limit without receiving a logout command, an incident shall be logged by the ERDS Server.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>C. Unauthorized Activities (Section 4.3.1.4.2)</td>
<td>Auditable</td>
<td>Incident</td>
<td>Reportable</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>1 Unauthorized access attempts, including, but not limited to:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Unauthorized users attempting access to, either physical or logical, ERDS storage areas.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
</tr>
<tr>
<td>2 Use of expired or revoked credentials.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
</tr>
<tr>
<td>D. Unauthorized Access</td>
<td>Auditable</td>
<td>Incident</td>
<td>Reportable</td>
</tr>
<tr>
<td>1 For Type 1 only, privilege elevation (e.g. &quot;Authorized Access&quot; role performing &quot;Secure Access&quot; tasks).</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2 For Type 1 only, unauthorized visitor access to an ERDS server or a logged-in session.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
</tr>
<tr>
<td>3 For Type 1 only, unauthorized access attempts, including, but not limited to: unauthorized users attempting access, either physical or logical, to ERDS storage areas.</td>
<td>Yes</td>
<td>Yes</td>
<td>If fraud is suspected</td>
</tr>
<tr>
<td>E. Authentication Failures</td>
<td>Auditable</td>
<td>Incident</td>
<td>Reportable</td>
</tr>
<tr>
<td>1 If authentication fails, ERDS returns to the login screen and indicates that access is not authorized.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2 If an individual fails to authenticate on consecutive login attempts, the ERDS account shall be locked-out and an incident shall be logged by the ERDS Server. Criteria for setting the login failure limit and lock-out duration shall be established by the County Recorder; however, the maximum preset limit is five attempts.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if intrusion is suspected</td>
</tr>
<tr>
<td>F. Authorization Failures</td>
<td>Auditable</td>
<td>Incident</td>
<td>Reportable</td>
</tr>
<tr>
<td>1 If ERDS cannot determine a role for, or assign privileges associated with a role to, an authenticated user, the session shall be terminated and an incident shall be logged by the ERDS Server.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>G. Accountability Failures (Section 4.3.1.4.4)</td>
<td>Auditable</td>
<td>Incident</td>
<td>Reportable</td>
</tr>
<tr>
<td>1 Auditable events overwrite other logged events.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if intrusion is suspected</td>
</tr>
<tr>
<td>2 Auditable events cannot be logged.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>3 Logs consume 95% or more of the storage space allocated for logging.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>4 Logs cannot be safely stored.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>H.</td>
<td><strong>ADMINISTRATION REQUIREMENTS (SECTION 4.3.1.5)</strong></td>
<td>AUDITABLE</td>
<td>INCIDENT</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>1</td>
<td>ERDS account creation, modification, deletion, suspension, termination, or revocation, whether authorized or not.</td>
<td>Yes</td>
<td>Only if not authorized</td>
</tr>
<tr>
<td>2</td>
<td>Hardware or software configuration changes.</td>
<td>Yes</td>
<td>Only if not authorized</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I.</th>
<th><strong>TRANSACTION ACTIVITIES (SECTION 4.3.1.4.3)</strong></th>
<th>AUDITABLE</th>
<th>INCIDENT</th>
<th>REPORTABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unique name of the ERDS payload.  (Note: This unique name is ERDS-design dependent.)</td>
<td>Yes</td>
<td>Only if out of sequence</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Dates and times the ERDS payload was submitted, retrieved and when applicable, returned.</td>
<td>Yes</td>
<td>Only if not current</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>Identity of the individual who submitted, retrieved and when applicable, returned the ERDS payload.</td>
<td>Yes</td>
<td>Only if not authorized</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>Name of the organization that the individual represented while submitting, retrieving and when applicable, returning the ERDS payload.</td>
<td>Yes</td>
<td>Only if not authorized</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>Success or failure of decryption, validation and hash.</td>
<td>Yes</td>
<td>Refer to &quot;Transaction Failures&quot;</td>
<td>Only if fraud is suspected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>J.</th>
<th><strong>TRANSACTION FAILURES</strong></th>
<th>AUDITABLE</th>
<th>INCIDENT</th>
<th>REPORTABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>For Type 1 only, a transmission failure shall display a transmission failure message and generate an auditable event log entry. (Section 3.2, ERDS Payload Submission Process, Table 3, Item 12)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>For Type 1 only, a storage failure shall display a storage failure message and generate an auditable event log entry. (Section 3.2, ERDS Payload Submission Process, Table 3, Item 12)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>A decryption failure shall display a decryption failure message and generate an auditable event log entry. (Section 3.3, ERDS Payload Retrieval Process, Table 4, Item 15 and Section 4.2.2.1, Payload Confidentiality)</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
</tr>
<tr>
<td>4</td>
<td>A hash failure shall display a hash failure message and generate an auditable event log entry. (Section 3.3, ERDS Payload Retrieval Process, Table 4, Item 16, and Sections 4.2.2.2, Payload Integrity and 4.2.2.3, Payload Authenticity)</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
</tr>
<tr>
<td>5</td>
<td>A validity check failure shall display error and/or warning messages and generate an auditable event log entry. (Section 3.3, ERDS Payload Retrieval Process, Table 4, Item 17 and Section 4.2.1, Data Integrity)</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
</tr>
<tr>
<td>K. Unauthorized Transactions</td>
<td>AUDITABLE</td>
<td>INCIDENT</td>
<td>REPORTABLE</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>1   Type 1 or Type 2 instrument submitted unencrypted. (Section 4.2.2.1, Payload Confidentiality)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>2   Type 1 instrument submitted as a Type 2 instrument or vice versa. (Sections 2.3, Type 1 and/or Type 2 Instruments and 3.4, Processing Multiple Transactions)</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
<td></td>
</tr>
<tr>
<td>3   Type 1 instrument submitted via an Authorized Access ERDS.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
<td></td>
</tr>
<tr>
<td>4   Unauthorized components that draw data or images from sources external to the digital electronic record or digitized electronic record. (Sections 4.2.1, Data Integrity)</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if intrusion is suspected</td>
<td></td>
</tr>
<tr>
<td>5   Unauthorized transactions submitted via an ERDS, including but not limited to, instruments that are neither Type 1 nor Type 2. (Section 2.3, Type 1 and/or Type 2 Instruments)</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if fraud is suspected</td>
<td></td>
</tr>
<tr>
<td>L. Server Events (Section 4.3.2.4)</td>
<td>AUDITABLE</td>
<td>INCIDENT</td>
<td>REPORTABLE</td>
<td></td>
</tr>
<tr>
<td>1   For Type 1 only, server failures, including, but not limited to, hardware, software, and network component failures, that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if intrusion is suspected</td>
<td></td>
</tr>
<tr>
<td>2   For Type 1 only, events for which ERDS System Administrators are alerted of possible or actual intrusion.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if intrusion is suspected</td>
<td></td>
</tr>
<tr>
<td>3   For Type 1 only, hardware or software configuration changes.</td>
<td>Yes</td>
<td>Only if not authorized</td>
<td>Only if not authorized</td>
<td></td>
</tr>
<tr>
<td>M. Network Events (Section 4.3.3.4)</td>
<td>AUDITABLE</td>
<td>INCIDENT</td>
<td>REPORTABLE</td>
<td></td>
</tr>
<tr>
<td>1   For Type 1 only, network failures that cause the ERDS to be unavailable or that expose the ERDS server directly to the Internet.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if intrusion is suspected</td>
<td></td>
</tr>
<tr>
<td>2   For Type 1 only, events for which an ERDS System Administrator is alerted of possible or actual intrusion.</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if intrusion is suspected</td>
<td></td>
</tr>
<tr>
<td>3   Unauthorized changes to the ERDS operational configuration.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>N. Security Events</td>
<td>AUDITABLE</td>
<td>INCIDENT</td>
<td>REPORTABLE</td>
<td></td>
</tr>
<tr>
<td>1   Inability to obtain and employ up-to-date anti-malware software. (Sections 4.2, Minimum Security Requirements; 4.2.8, Media Security; and 4.3.2.3, Server Hardening)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inability to obtain and employ cryptography, including hashing, encryption and decryption. (Sections 4.2.2.2, Payload Integrity and 4.2.3, Cryptographic Key Generation)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>3</td>
<td>Inability to obtain and employ the most up-to-date patches and hot-fixes. (Sections 4.2.8, Media Security and 4.3.2.3, Server Hardening)</td>
<td>Yes</td>
<td>No</td>
<td>Only if intrusion is suspected</td>
</tr>
<tr>
<td>O.</td>
<td><strong>OTHER EVENTS</strong></td>
<td><strong>AUDITABLE</strong></td>
<td><strong>INCIDENT</strong></td>
<td><strong>REPORTABLE</strong></td>
</tr>
<tr>
<td>1</td>
<td>Unauthorized access or changes to storage media, and improper sanitization of storage media. (Section 4.2.8, Media Security)</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if compromise is suspected</td>
</tr>
<tr>
<td>2</td>
<td>Any other event that compromises the safety or security of an ERDS. (Section 1.1, Overview)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
4.6 **SUBSTANTIVE MODIFICATIONS**

Substantive modifications, as defined in this section, shall result in a Modified System Audit, as defined in Section 5.2.3, Modified System Audit. A substantive modification is defined as any change that affects the functionality of an ERDS. Substantive modifications include, but are not limited to, the following:

1. Changes to source code that lead to new or different functional behaviors.
2. Changes to call signatures in source code interfaces to purchased components.
3. Changes of data structures or structural database objects.
4. Changes that require modification of deployment procedures.
5. A new version of a compiler that requires source code changes in order to compile existing source code error and warning free.
6. Changes to purchased components or components that are part of software libraries.
7. Relocation of an ERDS server to a different network segment.
8. Changing an ERDS server from single-purpose to multi-purpose.
9. Changing an ERDS server from Single-County to Multi-County.
10. Hardware maintenance involving the complete replacement of an ERDS server.
11. Software maintenance releases that correct, perfect, enhance or otherwise affect the functionality of an ERDS.
12. When changing an instrument type.
13. Changing to a return capability.

The term “substantive modification” excludes the following:

1. Day-to-day administration of ERDS accounts, roles or cryptographic keys.
2. Hardware maintenance that does not affect the functionality of an ERDS and does not involve the complete replacement of an ERDS server.
3. The Off-loading of ERDS server logs to long-term storage.
4. Updating anti-malware software with the most up-to-date releases.
5. Updating operating system software with the most up-to-date patches and hot-fixes.
6. Maintaining backups for software and data.
7. The addition and/or deletion of roles, whether or not fingerprinting or notification to the ERDS Program, is required.
5 AUDIT REQUIREMENTS

5.1 NATURE OF ERDS COMPUTER SECURITY AUDITS

The County Recorder shall establish a disciplined and structured process to monitor the effectiveness of the security controls for the ERDS. The primary process for monitoring the effectiveness of security controls shall be a computer security audit a systematic, measurable, technical assessment of how the baseline security requirements required by the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are applied to an ERDS.

The processes and technologies that are employed in an ERDS shall conform to the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. Regardless of how an ERDS is implemented, the security and testing requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be met.

Refer to the System Certification Handbook for the submission of an audit report.

5.2 COMPUTER SECURITY AUDITS

A Computer Security Auditor shall conduct a security audit of an ERDS for the purpose of (1) assessing the safety of the system; (2) verifying that the system is secure from vulnerabilities and unauthorized penetration; (3) ensuring ERDS operating procedures are in place, and are being followed; and (4) that an ERDS has no capability to modify, manipulate, insert, or delete information in the public record. While the requirements, standards, and guidelines in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 assure the safety and security of an ERDS, design variations, advances in technology, new threats, and vulnerabilities require a regular and systematic audit program. ERDS security audits shall be conducted in accordance with security checklists selected by the County Recorder and tailored to reflect local conditions. (Refer to Section 4.4, Security Checklists.)

The facility(ies) of a Type 2 only Authorized Submitter is exempt from a physical security audit when the Computer Security Auditor has validated that all the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 have been met, including certification by the County Recorder and the ERDS Program that the method of submission allowed under the system will not permit an Authorized Submitter or its employees and agents, or any third party, to modify, manipulate, insert or delete information in the public record, maintained by the County Recorder, or information in Type 1 documents which are submitted for electronic recording.

Based on the Computer Security Auditor's findings, the ERDS Program reserves the right to conduct a physical audit of a Type 2 only Authorized Submitter's facility(ies) if intrusion, fraud or good cause has been found.

5.2.1 Initial System Audit

To obtain initial system certification a full system audit is required. "Initial" is defined as the "first time" application for certification of an ERDS for either a Single-County or a Multi-County. This audit shall be performed prior to activating an ERDS for production and operation and shall be completed by a Computer Security Auditor. The initial audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. A successful initial system audit shall be sufficient to meet the first year audit requirement.

An initial system audit report shall include, but is not limited to, all of the following:
1. A Description of Deposit Materials showing that the source code has been deposited in escrow with an approved escrow facility.

2. Demonstration of the proposed system in its intended production and operational environments. The audit shall show the following:
   a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the ERDS system.
   b. Transmissions only occur between authorized parties.
   c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).
   d. Authorized and unauthorized users are limited in terms of roles assigned to operate the ERDS.
   e. Auditable events are logged correctly.
   f. Known vulnerabilities have been eliminated or mitigated.
   g. The ERDS is not susceptible to published exploits.
   h. ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.
   i. ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

3. Testing and review shall include all of the following:
   a. A review of the system design that includes all servers, workstations, and network devices employed for, or in support of, the proposed system.
   b. A review of source code, either selected software components or all software.
   c. An inventory of hardware, software and network devices comprising the proposed system.
   d. An inventory of all users and roles authorized to access and operate the proposed system.
   e. A mapping or diagram of the production/operational environment that identifies the servers, workstations and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.
   f. A review of the ERDS operating procedures proposed by the County Recorder.
   g. A review of all security checklists proposed for auditing the ERDS.
   h. A review of contracts with Authorized Submitters.
   i. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.2 Biennial Audit

To meet the ongoing oversight of an existing certified Single-County ERDS or a Multi-County ERDS, a biennial audit and a local inspection is required in alternating years. The biennial audit is a full system audit that shall be performed in the production and operational environments and shall be completed by a Computer Security Auditor and submitted to the County Recorder. A local inspection shall be performed by an ERDS Program representative in the alternating years of all Single-county ERDS and the Lead County of a Multi-County ERDS. Sub-Counties
will be initially inspected and will then be subject to random scheduled inspection thereafter by an ERDS Program representative. The biennial audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. Local inspection procedures are detailed in the System Certification Handbook.

A biennial audit report shall include, but is not limited to, all of the following:

1. Description of Deposit Materials showing that the source code has been deposited in escrow with an approved escrow facility.

2. Demonstration of the ERDS in its production and operational environments. The audit shall show the following:
   a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.
   b. Transmissions only occur between authorized parties.
   c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).
   d. Authorized and unauthorized users are limited in terms of roles assigned to operate the system.
   e. Auditable events are logged correctly.
   f. Known vulnerabilities have been eliminated or mitigated.
   g. The ERDS is not susceptible to published exploits and that published updates to the standards and guidelines as described in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 shall be implemented within two years.
   h. ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.
   i. ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

3. Testing and review shall include all of the following:
   a. A review of the system design that includes all servers, workstations, and network devices employed for, or in support of, the system.
   b. A review of source code, either selected software components or all software.
   c. An inventory of hardware, software and network devices comprising the system.
   d. An inventory of all users and roles authorized to access and operate the system.
   e. A mapping or diagram of the production and operational environments that identifies the servers, workstations, and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.
   f. A review of the ERDS operating procedures established by the County Recorder.
   g. A review of all security checklists established for auditing the ERDS.
   h. A review of contracts with Authorized Submitters.
   i. A review of collected audit data showing auditable events are collected for audit and audit data correlates to actual activities.
   j. A review of incident reports and determination that the cause of each incident has been eliminated or mitigated.
k. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.3 Modified System Audit

A Modified System Audit is required to obtain approval for making a substantive modification to an existing certified Single-County ERDS or a Multi-County ERDS. The definition of a substantive modification is detailed in Section 4.6, Substantive Modifications. A modified system audit shall pertain to only the components that are proposed to be modified and/or changed in the production environment and shall be performed prior to activating the modification and/or change in the ERDS operational environment. This modified system audit shall be completed by a Computer Security Auditor and submitted to the County Recorder. Upon receipt of the successful modified system audit, the County Recorder may place the proposed substantive modification in the production environment on a provisional basis. Within 15 business days of the provisional implementation, a copy of the successful modified system audit report shall be submitted to the ERDS Program as an attachment to an Application for a Request for Approval of Substantive Modification(s) (Form # ERDS0013). The modified system audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. A successful modified system audit may not replace the biennial audit requirement.

A modified system audit report shall include, but is not limited to, all of the following:

1. A Description of Deposit Materials showing that modified source code has been deposited in escrow with an approved escrow facility.

2. Demonstration of the ERDS in its intended production and operational environments. The audit shall focus on functions of the substantive modification and show the following:
   a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.
   b. Transmissions only occur between authorized parties.
   c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).
   d. Authorized and unauthorized users are limited in terms of roles assigned to operate the system.
   e. Auditable events are logged correctly.
   f. Known vulnerabilities have been eliminated or mitigated.
   g. The ERDS is not susceptible to published exploits.
   h. The ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.
   i. ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

3. Testing and review shall include all of the following:
   a. A review of the system design that includes all servers, workstations and network devices employed for, or in support of, the proposed system.
   b. A review of source code, either selected software components or all software.
c. An inventory of hardware, software and network devices comprising the proposed system.

d. An inventory of all users and roles authorized to access and operate the system.

e. A mapping or diagram of the production and operational environments that identifies the servers, workstations, and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.

f. A review of the ERDS operating procedures established by the County Recorder.

g. A review of all security checklists established for auditing the ERDS.

h. A review of contracts with Authorized Submitters.

i. A review of collected audit data showing auditable events are collected for audit and audit data correlates to actual activities.

j. A review of incident reports and determination that the cause of each incident has been eliminated or mitigated.

k. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.4 Modified System Incident Audit

A Modified System Incident Audit is required to meet the audit requirement resulting from an incident that compromises the safety or security of an ERDS. The definition of an incident is detailed in Section 4.5.2, Incident Response Procedures. A modified system incident audit shall pertain to only the components that were found to compromise the production environment and shall be performed prior to activating the correction in the ERDS for production and operation. This modified system incident audit shall be completed by a Computer Security Auditor and submitted to the County Recorder. The County Recorder shall submit a copy of the successful modified system incident audit report to the ERDS Program. The modified system incident audit requirements are detailed in this Section. The report format is detailed in Section 5.3, Security Audit Report Format. A successful modified system incident audit may not replace the biennial audit requirement.

A modified system incident audit report shall include, but is not limited to, all of the following:

1. Demonstration of the ERDS in its intended production and operational environments. The audit shall focus on the cause of the incident of fraud and show the following:

a. The ERDS payloads are neither transmitted nor stored in an unencrypted format anywhere in the system.

b. Transmissions only occur between authorized parties.

c. Remnants of sessions, transmissions and the ERDS payloads are not stored once the user initiating the session and transmitting the ERDS payloads has logged out or been disconnected (either physically or logically).

d. Authorized and unauthorized users are limited in terms of roles assigned to operate the system.

e. Auditable events are logged correctly.

f. Known vulnerabilities have been eliminated or mitigated.

g. The ERDS is not susceptible to published exploits and that the published updates to the standards and guidelines as described in the ERDS regulations shall be implemented within two years.
h. ERDS operating procedures and/or features within the ERDS design have been incorporated in order to restrict the instrument type and content to meet the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9.

i. ERDS shall have no capabilities to modify, manipulate, insert or delete information in the public record.

2. Testing and review shall include all of the following:

a. A review of the system design that includes all servers, workstations and network devices employed for, or in support of, the system.

b. A review of source code, either selected software components or all software.

c. An inventory of hardware, software and network devices comprising the system.

d. An inventory of all users and roles authorized to access and operate the system.

e. A mapping or diagram of the production and operational environments that identifies the servers, workstations, and network devices visible from an ERDS server and the ERDS servers visible from a non-ERDS workstation or server.

f. A review of the ERDS operating procedures established by the County Recorder.

g. A review of all security checklists established for auditing the ERDS.

h. A review of contracts with Authorized Submitters.

i. A review of collected audit data showing auditable events are collected for audit and audit data correlates to actual activities.

j. A review of incident reports and determination that the cause of each incident has been eliminated or mitigated.

k. That the requirements of the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 are met.

5.2.5 Audit and Local Inspection Schedule

The audit schedule is as follows:

- Year 1 – Initial System Audit
- Year 2 – Local Inspection
- Year 3 – Biennial Security Audit
- Year 4 – Local Inspection if selected
- Subsequent years – alternate Biennial Audit and Local Inspection

5.3 Security Audit Report Format

The format of a security audit report shall include, but is not limited to, all of the following:

1. A summary of recommendations in a task-list format.


3. A section for detailed technical observation and recommendation.

4. A diagram depicting results, where applicable.

5. Results of testing and reviews as outlined in Section 5.2, Computer Security Audits.
6. Recommendations for any additional precautions needed to ensure that the system is secure.

7. A copy of the list of all users for secure and/or authorized access.

5.4 PROPRIETARY SOFTWARE

The Computer Security Auditor may not be required to conduct a source code review on any software identified as proprietary by the Vendor of ERDS Software, unless such software affects the safety and security of an ERDS.

Prior to conducting a source code review, the County Recorder shall ensure all of the following:

1. The County Recorder has agreed to allow the Vendor of ERDS Software to include proprietary source code as part of the ERDS.

2. The Vendor of ERDS Software has identified proprietary source code as part of the ERDS.

3. The Computer Security Auditor advises the County Recorder that the safety and security of an ERDS cannot be verified without a source code review.

4. The Computer Security Auditor shall agree to abide by confidentiality requirements of the Vendor of ERDS Software.

5. The Vendor of ERDS Software shall agree that the Computer Security Auditor shall reveal any results of the source code review, conclusions as to the safety and security of an ERDS, findings and recommendations in the audit report.

6. The County Recorder, Computer Security Auditor, and Vendor of ERDS Software shall all agree on methods for including the results, conclusions and recommendations about proprietary source code reviews made by the Computer Security Auditor in the audit report.
6 ESCROW REQUIREMENTS

ERDS source code materials shall be placed into an approved escrow facility when an ERDS is developed for a County Recorder. For each submission, the materials placed in escrow shall be sufficient to maintain the ERDS of every County Recorder that employs those source code materials. This section establishes the escrow requirements to be met.

For the purposes of this section, the phrase "source code materials" includes, but is not limited to, all of the following:

1. A copy of all source code materials that implements an ERDS functionality.
2. A copy of the compiler needed to compile the ERDS source code in escrow.
3. Instructions for installation and use of the ERDS source code compiler.
4. Instructions that facilitate source code reviews, modification and/or recompiling the ERDS source code.

The processes and technologies that are employed in an ERDS shall conform to the requirements defined in the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9. For the purpose of this section, the term "developer" is defined to mean a Vendor of ERDS Software or public entity that develops software and provides source code materials for an ERDS. Regardless of how an ERDS is implemented, if source code is developed, the escrow requirements outlined in this section shall be met.

6.1 APPROVED ESCROW FACILITY

It is not the intent of the ERDS Program to approve nor certify escrow facilities because this is deemed duplicative of the approval process currently in place by the Secretary of State’s office in support of its "escrow of ballot tally software program source codes". In carrying out its function, the Secretary of State provides a list of facilities approved for use in California on an annual basis, and within ten days of any change affecting the list, to each County Board of Supervisors. In support of protecting ERDS source code, a County Recorder shall select an escrow company from the current Secretary of State's list as obtained from the County's Board of Supervisors.

6.2 LETTER OF DEPOSIT

Within a timeframe established by the County Recorder of a submission of original, changed or modified source code to an approved escrow facility, the Vendor of ERDS Software shall notify, in writing, each affected County Recorder that such source code has been placed in escrow. The letter of deposit shall include a description of submitted source code materials sufficient to distinguish them from all other submissions.

The letter of deposit shall state all of the following:

1. That all source code materials are included in the deposit.
2. The name of the approved escrow company and the location of the escrow facility where the source code materials have been placed in escrow.
3. The escrow company, its officers and directors shall not hold or exercise a direct or indirect financial interest(s) in the Vendor of ERDS Software or the County Recorder.
6.3 **Requirements for Submission**
Source code materials shall be submitted to an approved escrow company for placement in the escrow facility. The content of source code materials shall be in a form and include the tools and documentation to allow complete and successful restoration of an ERDS, in its production and operational environments, with confirmation by a verification test by qualified personnel using only this content.

6.4 **Deposit of Software Modifications into Escrow**
Substantive modifications, as defined in Section 4.6, Substantive Modifications, shall require updates to source code materials in escrow. Prior to being used to deliver a Type 1 and/or Type 2 instrument in an ERDS, all source code changes or modifications shall be submitted into escrow in the same manner and under the same conditions in which the source code materials were originally placed in escrow.

6.5 **Integrity of Materials**
No person having access to ERDS source code materials shall interfere with or prevent the escrow representative from monitoring the security and integrity of the ERDS source code materials.

6.6 **Retention and Disposition of Materials**
Records maintained by the escrow company pursuant to the CCR, Title 11, Division 1, Chapter 18, Articles 1 through 9 and other applicable law, shall be retained for the term of the escrow agreement. The escrow agreement shall provide for the disposition of source code materials in the event the escrow agreement terminates.

6.7 **Access to Materials**
Escrow agreements shall allow for access to ERDS source code materials by a Computer Security Auditor hired for the purpose of conducting a computer security audit.

6.8 **State Not Liable for Any Costs or Any Other’s Actions**
Neither the Attorney General nor the State of California shall be responsible for the fees claimed by the Vendor of ERDS Software, County Recorder or escrow company to establish the escrow contract. Further, neither the Attorney General nor the State of California is a party to the agreement and may not incur any liability for the actions of the parties involved in the escrow agreement.
# Acronyms and Definitions

This section defines general terms and phrases used in this document as well as other ERDS handbooks.

<table>
<thead>
<tr>
<th>Acronym, Term or Phrase</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>A representative and his/her employees who are authorized to submit documents on behalf of an Authorized Submitter who has entered into a contract with a County Recorder and assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Agent may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software. (Refer to the definition of “Vendor of ERDS software (or Developer)” within this section.)</td>
</tr>
<tr>
<td>Approved Escrow Company</td>
<td>An escrow company approved pursuant to the California Code of Regulations, Title 2, Division 7, Chapter 6, Article 3, D, List of Approved Companies and Facilities, Section 20639.</td>
</tr>
<tr>
<td>Attorney General</td>
<td>The Attorney General of the State of California.</td>
</tr>
<tr>
<td>Authorized Access</td>
<td>A role assigned by the County Recorder to an Authorized Submitter and Agent, if any, who is authorized to use ERDS for only Type 2 instruments. This role does not require fingerprinting.</td>
</tr>
<tr>
<td>Authorized Submitter</td>
<td>A party and his/her employees that has entered into a contract with a County Recorder and assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Authorized Submitter may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.</td>
</tr>
<tr>
<td>CCISDA</td>
<td>California County Information Services Directors Association</td>
</tr>
<tr>
<td>CCR</td>
<td>California Code of Regulations</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>A certificate authority that issues digital certificates for the purpose of establishing secure Internet sessions between an Authorized Submitter and an ERDS. Certificate authorities also validate digital certificates presented as proof of identity.</td>
</tr>
<tr>
<td>CFE</td>
<td>Certified Fraud Examiner</td>
</tr>
<tr>
<td>CIA</td>
<td>Certified Internal Auditor</td>
</tr>
<tr>
<td>CISA</td>
<td>Certified Information Systems Auditor</td>
</tr>
<tr>
<td>CISSP</td>
<td>Certified Information Systems Security Professional</td>
</tr>
<tr>
<td>Acronym, Term or Phrase</td>
<td>Definitions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Computer Security Auditor</td>
<td>(1) DOJ approved computer security personnel hired by the County Recorder to perform independent audits. (2) A role assigned by the County Recorder to the Computer Security Auditor who is authorized to review transaction logs and conduct tests on computer security mechanisms. A Computer Security Auditor may not be an Authorized Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software. This role requires fingerprinting. A Computer Security Auditor shall be issued a certificate of approval by the ERDS Program.</td>
</tr>
<tr>
<td>County Recorder</td>
<td>A public official responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.</td>
</tr>
<tr>
<td>County Recorder Designee</td>
<td>A Secure Access role assigned by the County Recorder to retrieve, and, when applicable, return submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.</td>
</tr>
<tr>
<td>Developer</td>
<td>Refer to Vendor of ERDS Software.</td>
</tr>
<tr>
<td>Digital Electronic Record</td>
<td>A record containing information that is created, generated, sent, communicated, received or stored by electronic means, but not created in original paper form.</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>A set of electronic symbols attached to, included in, or logically associated with one or more Type 1 and/or Type 2 instruments, inclusive of information related to and intended for association with the Type 1 and/or Type 2 instruments, that is the result of a process, or processes, designed and employed for the purpose of verifying the integrity, accuracy or authenticity of the Type 1 and/or Type 2 instruments with related information. For the purpose of an ERDS, a digital signature is generated by encrypting the hash value of an ERDS payload.</td>
</tr>
<tr>
<td>Digitized Electronic Record</td>
<td>A scanned image of the original paper document.</td>
</tr>
<tr>
<td>DOJ</td>
<td>The California Department of Justice</td>
</tr>
<tr>
<td>Electronic Signature of the Notary</td>
<td>A field or set of fields, containing information about the electronic signature of the notary who notarized a Type 1 or Type 2 instrument.</td>
</tr>
<tr>
<td>ERDS</td>
<td>Electronic Recording Delivery System – An ERDS Program certified system to deliver digitized Type 1 and/or Type 2 instruments to a County Recorder, and, when applicable, return to the Authorized Submitter.</td>
</tr>
<tr>
<td>Acronym, Term or Phrase</td>
<td>Definitions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERDS Account Administrator</td>
<td>A secure access role assigned by the County Recorder to an individual authorized to configure accounts, assign roles and issue credentials. An ERDS Account Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.</td>
</tr>
<tr>
<td>ERDS Payload</td>
<td>An electronic structure designed for the purpose of delivering Type 1 or Type 2 instruments to a County Recorder via an ERDS. The structure is also used to return, and, when applicable, Type 1 or Type 2 instruments to an Authorized Submitter via an ERDS.</td>
</tr>
<tr>
<td>ERDS Program</td>
<td>The program within DOJ designated by the Attorney General to certify, implement, regulate and monitor an ERDS.</td>
</tr>
<tr>
<td>ERDS Server</td>
<td>Computer hardware, software and storage media used by the County Recorder to implement an ERDS. The ERDS server executes the primary functionality of the application software associated with an ERDS. The ERDS Server includes software for encrypting, decrypting, hashing, submitting, and, when applicable, returning the ERDS payloads. It also includes storage media for the ERDS payloads in the process of being delivered to the County Recorder or, when applicable, being returned to the Authorized Submitter. Separate physical servers dedicated to performing ERDS server functions are not required provided that the ERDS server functions can be isolated from other server functions, as evidenced by audit.</td>
</tr>
<tr>
<td>ERDS System Administrator</td>
<td>A secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software, network settings and to maintain ERDS security functions. An ERDS System Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>GIAC</td>
<td>Global Information Assurance Certification</td>
</tr>
<tr>
<td>GSNA</td>
<td>GIAC Systems and Network Auditor</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hash Message Authentication Code</td>
</tr>
<tr>
<td>Incident</td>
<td>An event that may have compromised the safety or security of an ERDS.</td>
</tr>
<tr>
<td>Instrument</td>
<td>A &quot;Type 1&quot; instrument is defined to mean an instrument affecting a right, title or interest in real property. Type 1 instruments shall be delivered as digitized electronic records. Individuals given role-based privileges for a Type 1 instrument shall be fingerprinted. A &quot;Type 2&quot; instrument is defined to mean an instrument of reconveyance, substitution of trustee or assignment of deed of trust. Type 2 instruments may be delivered as digitized electronic records or digital electronic records. Individuals given role-based privileges for a Type 2 only instrument shall not be fingerprinted.</td>
</tr>
<tr>
<td>Lead County</td>
<td>The County Recorder in a Multi-County ERDS responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.</td>
</tr>
<tr>
<td>Acronym, Term or Phrase</td>
<td>Definitions</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Live Scan</td>
<td>A DOJ system used for the electronic submission of applicant fingerprints. This system is outside of the ERDS Program.</td>
</tr>
<tr>
<td>Logged</td>
<td>An auditable ERDS event.</td>
</tr>
<tr>
<td>Logical</td>
<td>The way data or systems are organized. For example, a logical description of a file is that it is a collection of data stored together.</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Codes</td>
</tr>
<tr>
<td>Multi-County</td>
<td>An ERDS application where County Recorders collaborate and make use of a single ERDS serving multiple counties.</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>Non-Substantive Modification</td>
<td>A change that does not affect the functionality of an ERDS.</td>
</tr>
<tr>
<td>ORI</td>
<td>Originating Agency Identifier</td>
</tr>
<tr>
<td>Physical Access</td>
<td>Access granted to an individual who has physical access to an ERDS server. This level of access requires fingerprinting with the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls.</td>
</tr>
<tr>
<td>Public Entity</td>
<td>Includes the State, the Regents of the University of California, a county, city, district, public authority, public agency, any other political subdivision or public corporation in the State and federal government entities.</td>
</tr>
<tr>
<td>PKI</td>
<td>A Public Key Infrastructure is a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority, which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensure that messages have not been tampered with.</td>
</tr>
<tr>
<td>Reportable</td>
<td>An incident that has resulted in the compromise of the safety or the security of an ERDS and shall be reported to the ERDS Program.</td>
</tr>
<tr>
<td>RSA</td>
<td>A public-key encryption technology developed by Rivest, Shamir and Adelman (RSA). The RSA algorithm has become the de facto standard for industrial-strength encryption especially for data sent over the Internet.</td>
</tr>
<tr>
<td>Role</td>
<td>A security mechanism, method, process or procedure that defines specific privileges controlling the level of access to an ERDS.</td>
</tr>
<tr>
<td>SANS Institute</td>
<td>Systems and Network Security Institute</td>
</tr>
<tr>
<td>Acronym, Term or Phrase</td>
<td>Definitions</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Secure Access</td>
<td>A role assigned by the County Recorder to an individual which requires fingerprinting to: 1) an Authorized Submitter and Agent, if any, who are authorized to use an ERDS for both Type 1 and 2 instruments (excludes Type 2 instruments only) or Type 1 instruments only; 2) a Computer Security Auditor hired by the County Recorder to perform independent audits; 3) an ERDS System Administrator authorized to configure hardware, software and network settings; 4) an ERDS Account Administrator authorized to configure accounts, assign roles and issue credentials; 5) an individual who is granted physical access to an ERDS server; 6) a County Recorder Designee authorized to retrieve, and, when applicable, return submitted ERDS payloads.</td>
</tr>
<tr>
<td>Security Testing</td>
<td>An independent security audit by a Computer Security Auditor, including, but not limited to, attempts to penetrate an ERDS for the purpose of testing the security of that system.</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>Source Code</td>
<td>A program or set of programs, readable and maintainable by humans, translated or interpreted into a form that an ERDS can execute.</td>
</tr>
<tr>
<td>Source Code Materials</td>
<td>Source Code Materials must include, but, are not limited to: 1) a copy of all source code that implements ERDS functionality; 2) a copy of the compiler needed to compile the ERDS source code in escrow; 3) instructions for installation and use of the ERDS source code compiler; and 4) instructions that facilitate reviews, modification and/or recompiling the source code.</td>
</tr>
<tr>
<td>Sub-County</td>
<td>The collaborating County Recorder(s) in a Multi-County ERDS operation.</td>
</tr>
<tr>
<td>Substantive Modification</td>
<td>A change that affects the functionality of an ERDS.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security (formerly known as Secure Socket Layer)</td>
</tr>
<tr>
<td>Uniform Index Information</td>
<td>Information collected by a County Recorder in the recording process. Every Type 1 and Type 2 Instruments delivered through an ERDS shall be capable of including uniform index information. The County Recorder shall decide on the content of uniform index information.</td>
</tr>
<tr>
<td>User</td>
<td>A person who uses a computer to access, submit, retrieve, or, when applicable, return an ERDS payload.</td>
</tr>
<tr>
<td>Vendor of ERDS Software (or Developer)</td>
<td>A person and personnel, supporting and/or acting on behalf of the certified Vendor of ERDS Software who sells, leases, or grants use of, with or without compensation therefore, a software program for use by counties for establishing an ERDS. A Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, County Recorder Designee, or internal county resources used as a Developer of an ERDS in lieu of a Vendor. This role requires fingerprinting.</td>
</tr>
<tr>
<td>Workstation</td>
<td>A computer used to connect to and interact with an ERDS.</td>
</tr>
</tbody>
</table>
8 REQUIREMENTS MATRIX

The ERDS Program has provided a spreadsheet that illustrates the minimum requirements for each type of ERDS (Type 1 or Type 2 or Type 1 and 2). The Requirements Matrix is an abstracted version of this document so that the minimum requirements are easily referenced. To obtain a copy of the matrix, download it from the ERDS Program web page at http://ag.ca.gov/erds1 or contact the ERDS Program.

8.1 HOW TO READ THE MATRIX

The contents of this document were converted to a Requirements Matrix in order to highlight specific requirements within this document. The column labeled “Title or Requirement” in the Requirements Matrix identifies the actual requirement, whereas the columns labeled “Type 1”, “Type 2” are designated with an “X” to signify which type of ERDS the requirement corresponds to. Only those columns with an “X” in Type 1, or Type 2 are requirements for Type 1, or Type 2 ERDS respectively.
Note to Readers on the Update

Version 1.1 of this Cybersecurity Framework refines, clarifies, and enhances Version 1.0, which was issued in February 2014. It incorporates comments received on the two drafts of Version 1.1. Version 1.1 is intended to be implemented by first-time and current Framework users. Current users should be able to implement Version 1.1 with minimal or no disruption; compatibility with Version 1.0 has been an explicit objective.

The following table summarizes the changes made between Version 1.0 and Version 1.1.

Table NTR-1 - Summary of changes between Framework Version 1.0 and Version 1.1.

<table>
<thead>
<tr>
<th>Update</th>
<th>Description of Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarified that terms like “compliance” can be confusing and mean something very different to various Framework stakeholders</td>
<td>Added clarity that the Framework has utility as a structure and language for organizing and expressing compliance with an organization’s own cybersecurity requirements. However, the variety of ways in which the Framework can be used by an organization means that phrases like “compliance with the Framework” can be confusing.</td>
</tr>
<tr>
<td>A new section on self-assessment</td>
<td>Added Section 4.0 <em>Self-Assessing Cybersecurity Risk with the Framework</em> to explain how the Framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.</td>
</tr>
<tr>
<td>Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes</td>
<td>An expanded Section 3.3 <em>Communicating Cybersecurity Requirements with Stakeholders</em> helps users better understand Cyber Supply Chain Risk Management (SCRM), while a new Section 3.4 Buying Decisions highlights use of the Framework in understanding risk associated with commercial off-the-shelf products and services. Additional Cyber SCRM criteria were added to the Implementation Tiers. Finally, a Supply Chain Risk Management Category, including multiple Subcategories, has been added to the Framework Core.</td>
</tr>
<tr>
<td>Refinements to better account for authentication, authorization, and identity proofing</td>
<td>The language of the Access Control Category has been refined to better account for authentication, authorization, and identity proofing. This included adding one Subcategory each for Authentication and Identity Proofing. Also, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.</td>
</tr>
<tr>
<td>Better explanation of the relationship between Implementation Tiers and Profiles</td>
<td>Added language to Section 3.2 <em>Establishing or Improving a Cybersecurity Program</em> on using Framework Tiers in Framework implementation. Added language to Framework Tiers to reflect integration of Framework considerations within organizational risk management programs. The Framework Tier concepts were also refined. Updated Figure 2.0 to include actions from the Framework Tiers.</td>
</tr>
<tr>
<td>Consideration of Coordinated Vulnerability Disclosure</td>
<td>A Subcategory related to the vulnerability disclosure lifecycle was added.</td>
</tr>
</tbody>
</table>

As with Version 1.0, Version 1.1 users are encouraged to customize the Framework to maximize individual organizational value.


Acknowledgements

This publication is the result of an ongoing collaborative effort involving industry, academia, and government. The National Institute of Standards and Technology (NIST) launched the project by convening private- and public-sector organizations and individuals in 2013. Published in 2014 and revised during 2017 and 2018, this Framework for Improving Critical Infrastructure Cybersecurity has relied upon eight public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with stakeholders from across all sectors of the United States along with many sectors from around the world.

The impetus to change Version 1.0 and the changes that appear in this Version 1.1 were based on:

- Feedback and frequently asked questions to NIST since release of Framework Version 1.0;
- 105 responses to the December 2015 request for information (RFI), Views on the Framework for Improving Critical Infrastructure Cybersecurity;
- Over 85 comments on a December 5, 2017 proposed second draft of Version 1.1;
- Over 120 comments on a January 10, 2017, proposed first draft Version 1.1; and
- Input from over 1,200 attendees at the 2016 and 2017 Framework workshops.

In addition, NIST previously released Version 1.0 of the Cybersecurity Framework with a companion document, NIST Roadmap for Improving Critical Infrastructure Cybersecurity. This Roadmap highlighted key “areas of improvement” for further development, alignment, and collaboration. Through private and public-sector efforts, some areas of improvement have advanced enough to be included in this Framework Version 1.1.

NIST acknowledges and thanks all of those who have contributed to this Framework.
Executive Summary

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company’s bottom line. It can drive up costs and affect revenue. It can harm an organization’s ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization’s overall risk management.

To better address these risks, the Cybersecurity Enhancement Act of 2014¹ (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.” This formalized NIST’s previous work developing Framework Version 1.0 under Executive Order (EO) 13636, “Improving Critical Infrastructure Cybersecurity” (February 2013), and provided guidance for future Framework evolution. The Framework that was developed under EO 13636, and continues to evolve according to CEA, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the

Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework offers a flexible way to address cybersecurity, including cybersecurity’s effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework’s outcomes serve as targets for workforce development and evolution activities.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework’s five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about “compliance” with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization’s own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like “compliance with the Framework” can be confusing and mean something very different to various stakeholders.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with the private sector and government agencies at all levels. As the Framework is put into greater practice, additional lessons learned will be integrated into future versions. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Expanded and more effective use and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation’s critical infrastructure – providing evolving guidance for individual organizations while increasing the cybersecurity posture of the Nation’s critical infrastructure and the broader economy and society.
# Table of Contents

Note to Readers on the Update .................................................................................. ii
Acknowledgements ...................................................................................................... iv
Executive Summary ...................................................................................................... v
1.0 Framework Introduction ......................................................................................... 1
2.0 Framework Basics .................................................................................................. 6
3.0 How to Use the Framework .................................................................................... 13
4.0 Self-Assessing Cybersecurity Risk with the Framework ........................................... 20
Appendix A: Framework Core ....................................................................................... 22
Appendix B: Glossary ................................................................................................... 45
Appendix C: Acronyms .................................................................................................. 48

# List of Figures

Figure 1: Framework Core Structure ........................................................................... 6
Figure 2: Notional Information and Decision Flows within an Organization ............... 12
Figure 3: Cyber Supply Chain Relationships ................................................................ 17

# List of Tables

Table 1: Function and Category Unique Identifiers ....................................................... 23
Table 2: Framework Core ............................................................................................ 24
Table 3: Framework Glossary ...................................................................................... 45
1.0 Framework Introduction

The United States depends on the reliable functioning of its critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company’s bottom line. It can drive up costs and affect revenue. It can harm an organization’s ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization’s overall risk management.

To strengthen the resilience of this infrastructure, the Cybersecurity Enhancement Act of 2014\(^2\) (CEA) updated the role of the National Institute of Standards and Technology (NIST) to “facilitate and support the development of” cybersecurity risk frameworks. Through CEA, NIST must identify “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.” This formalized NIST’s previous work developing Framework Version 1.0 under Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” issued in February 2013\(^3\), and provided guidance for future Framework evolution.

Critical infrastructure\(^4\) is defined in the U.S. Patriot Act of 2001\(^5\) as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization’s size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation’s infrastructure. Members of each critical infrastructure sector perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). This reliance on technology, communication, and interconnectivity has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as technology and the data it produces and processes are increasingly used to deliver critical services and support business/mission decisions, the potential impacts of a cybersecurity incident on an

---


organization, the health and safety of individuals, the environment, communities, and the broader economy and society should be considered.

To manage cybersecurity risks, a clear understanding of the organization’s business drivers and security considerations specific to its use of technology is required. Because each organization’s risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization’s approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

The Framework remains effective and supports technical innovation because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks — different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.
To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework’s five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about “compliance” with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization’s own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like “compliance with the Framework” can be confusing and mean something very different to various stakeholders.

The Framework complements, and does not replace, an organization’s risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

While the Framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. The common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- The **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- **Framework Implementation Tiers** ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the
characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

- A Framework Profile (“Profile”) represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization’s risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO)
31000:2009\textsuperscript{6}, ISO/International Electrotechnical Commission (IEC) 27005:2011\textsuperscript{7}, NIST Special Publication (SP) 800-39\textsuperscript{8}, and the \textit{Electricity Subsector Cybersecurity Risk Management Process} (RMP) guideline\textsuperscript{9}.

1.3 \textbf{Document Overview}

The remainder of this document contains the following sections and appendices:

- \textbf{Section 2} describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- \textbf{Section 3} presents examples of how the Framework can be used.
- \textbf{Section 4} describes how to use the Framework for self-assessing and demonstrating cybersecurity through measurements.
- \textbf{Appendix A} presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- \textbf{Appendix B} contains a glossary of selected terms.
- \textbf{Appendix C} lists acronyms used in this document.


2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

2.1 Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in Figure 1:

![Figure 1: Framework Core Structure](image)

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018
• **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”

• **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

• **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See [Appendix A](#) for the complete Framework Core listing.

• **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

• **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

• **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
• **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

• **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

### 2.2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization’s overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization’s management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization’s current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.
Successful implementation of the Framework is based upon achieving the outcomes described in the organization’s Target Profile(s) and not upon Tier determination. Still, Tier selection and designation naturally affect Framework Profiles. The Tier recommendation by Business/Process Level managers, as approved by the Senior Executive Level, will help set the overall tone for how cybersecurity risk will be managed within the organization, and should influence prioritization within a Target Profile and assessments of progress in addressing gaps.

The Tier definitions are as follows:

**Tier 1: Partial**

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.

- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

**Tier 2: Risk Informed**

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.

- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.
Tier 3: Repeatable

- **Risk Management Process** – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

- **Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.

- **External Participation** - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community’s broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

Tier 4: Adaptive

- **Risk Management Process** – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.

- **Integrated Risk Management Program** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.
- **External Participation** - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

### 2.3 Framework Profile

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations. This Framework does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory can contribute to the roadmap described above. Prioritizing the mitigation of gaps is driven by the organization’s business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. Furthermore, the Framework is a risk-based approach where the applicability and fulfillment of a given Subcategory is subject to the Profile’s scope.
2.4 Coordination of Framework Implementation

**Figure 2** describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization’s overall risk management process and to the implementation/operations level for awareness of business impact.

*Figure 2: Notional Information and Decision Flows within an Organization*
3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization’s cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The Framework can be applied throughout the life cycle phases of plan, design, build/buy, deploy, operate, and decommission. The plan phase begins the cycle of any system and lays the groundwork for everything that follows. Overarching cybersecurity considerations should be declared and described as clearly as possible. The plan should recognize that those considerations and requirements are likely to evolve during the remainder of the life cycle. The design phase should account for cybersecurity requirements as a part of a larger multidisciplinary systems engineering process. A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as captured in a Framework Profile. The desired cybersecurity outcomes prioritized in a Target Profile should be incorporated when a) developing the system during the build phase and b) purchasing or outsourcing the system during the buy phase. That same Target Profile serves as a list of system cybersecurity features that should be assessed when deploying the system to verify all features are implemented. The cybersecurity outcomes determined by using the Framework then should serve as a basis for ongoing operation of the system. This includes occasional reassessment, capturing results in a Current Profile, to verify that cybersecurity requirements are still fulfilled. Typically, a complex web of dependencies (e.g., compensating and common controls) among systems means the outcomes documented in Target Profiles of related systems should be carefully considered as systems are decommissioned.

The following sections present different ways in which organizations can use the Framework.

3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization’s current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired

---

outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including “How are we doing?” Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create aCurrent Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization’s overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization’s desired cybersecurity outcomes. Organizations also may develop their own additional Categories and
Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

**Step 6: Determine, Analyze, and Prioritize Gaps.** The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

**Step 7: Implement Action Plan.** The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

### 3.3 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services. Examples include:

- An organization may use a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.
- An organization can better manage cybersecurity risk among stakeholders by assessing their position in the critical infrastructure and the broader digital economy using Implementation Tiers.

Communication is especially important among stakeholders up and down supply chains. Supply chains are complex, globally distributed, and interconnected sets of resources and processes.
between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.11

Cyber SCRM is the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization.

A primary objective of cyber SCRM is to identify, assess, and mitigate “products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain.” Cyber SCRM activities may include:

- Determining cybersecurity requirements for suppliers,
- Enacting cybersecurity requirements through formal agreement (e.g., contracts),
- Communicating to suppliers how those cybersecurity requirements will be verified and validated,
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies, and
- Governing and managing the above activities.

As depicted in Figure 3, cyber SCRM encompasses technology suppliers and buyers, as well as non-technology suppliers and buyers, where technology is minimally composed of information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). Figure 3 depicts an organization at a single point in time. However, through the normal course of business operations, most organizations will be both an upstream supplier and downstream buyer in relation to other organizations or end users.

11 Communicating Cybersecurity Requirements (Section 3.3) and Buying Decisions (Section 3.4) address only two uses of the Framework for cyber SCRM and are not intended to address cyber SCRM comprehensively.


This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018
Figure 3: Cyber Supply Chain Relationships

The parties described in Figure 3 comprise an organization’s cybersecurity ecosystem. These relationships highlight the crucial role of cyber SCRM in addressing cybersecurity risk in critical infrastructure and the broader digital economy. These relationships, the products and services they provide, and the risks they present should be identified and factored into the protective and detective capabilities of organizations, as well as their response and recovery protocols.

In the figure above, “Buyer” refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations. “Supplier” encompasses upstream product and service providers that are used for an organization’s internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

Whether considering individual Subcategories of the Core or the comprehensive considerations of a Profile, the Framework offers organizations and their partners a method to help ensure the new product or service meets critical security outcomes. By first selecting outcomes that are relevant to the context (e.g., transmission of Personally Identifiable Information (PII), mission critical service delivery, data verification services, product or service integrity) the organization then can evaluate partners against those criteria. For example, if a system is being purchased that will monitor Operational Technology (OT) for anomalous network communication, availability may be a particularly important cybersecurity objective to achieve and should drive a Technology Supplier evaluation against applicable Subcategories (e.g., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).
3.4 Buying Decisions

Since a Framework Target Profile is a prioritized list of organizational cybersecurity requirements, Target Profiles can be used to inform decisions about buying products and services. This transaction varies from Communicating Cybersecurity Requirements with Stakeholders (addressed in Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier. The objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements. Often, this means some degree of trade-off, comparing multiple products or services with known gaps to the Target Profile.

Once a product or service is purchased, the Profile also can be used to track and address residual cybersecurity risk. For example, if the service or product purchased did not meet all the objectives described in the Target Profile, the organization can address the residual risk through other management actions. The Profile also provides the organization a method for assessing if the product meets cybersecurity outcomes through periodic review and testing mechanisms.

3.5 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

3.6 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology to address individual privacy and civil liberties implications that may result from cybersecurity. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program engender privacy and civil liberties considerations. Technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and cybersecurity have a strong connection. An organization’s cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed. Some examples include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; and cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including some types of incident detection or monitoring that may inhibit freedom of expression or association.

The government and its agents have a responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or its agents that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.
To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in Appendix A, the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

**Governance of cybersecurity risk**

- An organization’s assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program.
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained.
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.
- Process is in place to assess implementation of the above organizational measures and controls.

**Approaches to identifying, authenticating, and authorizing individuals to access organizational assets and systems**

- Steps are taken to identify and address the privacy implications of identity management and access control measures to the extent that they involve collection, disclosure, or use of personal information.

**Awareness and training measures**

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities.
- Service providers that provide cybersecurity-related services for the organization are informed about the organization’s applicable privacy policies.

**Anomalous activity detection and system and assets monitoring**

- Process is in place to conduct a privacy review of an organization’s anomalous activity detection and cybersecurity monitoring.

**Response activities, including information sharing or other mitigation efforts**

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities.
- Process is in place to conduct a privacy review of an organization’s cybersecurity mitigation efforts.
4.0 Self-Assessing Cybersecurity Risk with the Framework

The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives. Ideally, organizations using the Framework will be able to measure and assign values to their risk along with the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be.

Over time, self-assessment and measurement should improve decision making about investment priorities. For example, measuring – or at least robustly characterizing – aspects of an organization’s cybersecurity state and trends over time can enable that organization to understand and convey meaningful risk information to dependents, suppliers, buyers, and other parties. An organization can accomplish this internally or by seeking a third-party assessment. If done properly and with an appreciation of limitations, these measurements can provide a basis for strong trusted relationships, both inside and outside of an organization.

To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are implemented and managed. While measurements of all those items is beyond the scope of the Framework, the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities in the following ways:

- Making choices about how different portions of the cybersecurity operation should influence the selection of Target Implementation Tiers,
- Evaluating the organization’s approach to cybersecurity risk management by determining Current Implementation Tiers,
- Prioritizing cybersecurity outcomes by developing Target Profiles,
- Determining the degree to which specific cybersecurity steps achieve desired cybersecurity outcomes by assessing Current Profiles, and
- Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References.

The development of cybersecurity performance metrics is evolving. Organizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use, while avoiding reliance on artificial indicators of current state and progress in improving cybersecurity risk management. Judging cyber risk requires discipline and should be revisited periodically. Any time measurements are employed as part of the Framework process, organizations are encouraged to clearly identify and know why these measurements are important and how they will contribute to the overall management of cybersecurity risk. They also should be clear about the limitations of measurements that are used.

For example, tracking security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. Verifying achievement of some organizational objectives requires analyzing the data only after that objective was to have been achieved. This type of lagging measure is more
absolute. However, it is often more valuable to predict whether a cybersecurity risk *may* occur, and the impact it *might* have, using a leading measure.

Organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations.
Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization’s risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material, including Informative References, relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.
### Table 1: Function and Category Unique Identifiers

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Identity Management and Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| IDENTIFY (ID) | Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | ID.AM-1: Physical devices and systems within the organization are inventoried | CIS CSC 1  
COBIT 5 BAI09.01, BAI09.02  
ISA 62443-2-1:2009 4.2.3.4  
ISA 62443-3-3:2013 SR 7.8  
ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
NIST SP 800-53 Rev. 4 CM-8, PM-5 |
| | | ID.AM-2: Software platforms and applications within the organization are inventoried | CIS CSC 2  
COBIT 5 BAI09.01, BAI09.02, BAI09.05  
ISA 62443-2-1:2009 4.2.3.4  
ISA 62443-3-3:2013 SR 7.8  
ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1  
NIST SP 800-53 Rev. 4 CM-8, PM-5 |
| | | ID.AM-3: Organizational communication and data flows are mapped | CIS CSC 12  
COBIT 5 DSS05.02  
ISA 62443-2-1:2009 4.2.3.4  
ISO/IEC 27001:2013 A.13.2.1, A.13.2.2  
NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 |
| | | ID.AM-4: External information systems are catalogued | CIS CSC 12  
COBIT 5 APO02.02, APO10.04, DSS01.02  
ISO/IEC 27001:2013 A.11.2.6  
NIST SP 800-53 Rev. 4 AC-20, SA-9 |
| | | ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | CIS CSC 13, 14  
COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02  
ISA 62443-2-1:2009 4.2.3.6  
ISO/IEC 27001:2013 A.8.2.1  
NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 |
| | | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and | CIS CSC 17, 19  
COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Environment (ID.BE):</strong></td>
<td></td>
<td>The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</td>
<td></td>
</tr>
<tr>
<td>ID.BE-1</td>
<td></td>
<td>The organization's role in the supply chain is identified and communicated</td>
<td>COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.2.1, A.15.2.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11</td>
</tr>
<tr>
<td>ID.BE-2</td>
<td></td>
<td>The organization's place in critical infrastructure and its industry sector is identified and communicated</td>
<td>COBIT 5 APO02.06, APO03.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 Clause 4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 PM-8</td>
</tr>
<tr>
<td>ID.BE-3</td>
<td></td>
<td>Priorities for organizational mission, objectives, and activities are established and communicated</td>
<td>COBIT 5 APO02.01, APO02.06, APO03.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 PM-11, SA-14</td>
</tr>
<tr>
<td>ID.BE-4</td>
<td></td>
<td>Dependencies and critical functions for delivery of critical services are established</td>
<td>COBIT 5 APO10.01, BAI04.02, BAI09.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14</td>
</tr>
<tr>
<td>ID.BE-5</td>
<td></td>
<td>Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)</td>
<td>COBIT 5 BAI03.02, DSS04.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.2.1, A.17.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14</td>
</tr>
<tr>
<td><strong>Governance (ID.GV):</strong></td>
<td></td>
<td>The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the</td>
<td></td>
</tr>
<tr>
<td>ID.GV-1</td>
<td></td>
<td>Organizational cybersecurity policy is established and communicated</td>
<td>CIS CSC 19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO10.03, APO13.01, EDM01.01, EDM01.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.2.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.5.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                      | management of cybersecurity     | ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned | CIS CSC 19  
COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04  
ISA 62443-2-1:2009 4.3.2.3.3  
ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1  
NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2 |
|                      | risk                             | with internal roles and external partners                                   |                             |
|                      | Management of regulatory         | ID.GV-3: Legal and regulatory requirements regarding cybersecurity,           | CIS CSC 19  
COBIT 5 BA02.01, MEA03.01, MEA03.04  
ISA 62443-2-1:2009 4.4.3.7  
NIST SP 800-53 Rev. 4 -1 controls from all security control families |
|                      | processes addressing cybersecurity risks | including privacy and civil liberties obligations, are understood and managed |                             |
|                      | Management of governance         | ID.GV-4: Governance and risk management processes address cybersecurity risks | COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02  
ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3  
ISO/IEC 27001:2013 Clause 6  
NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 |
|                      | and risk management               |                                                                             |                             |
|                      | Assessment (ID.RA)               | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. |                             |
|                      |                                  | ID.RA-1: Asset vulnerabilities are identified and documented                 | CIS CSC 4  
COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02  
ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12  
ISO/IEC 27001:2013 A.12.6.1, A.18.2.3  
NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 |
|                      |                                  | ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources | CIS CSC 4  
COBIT 5 BA108.01  
ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12  
ISO/IEC 27001:2013 A.6.1.4  
NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.RA-3:</td>
<td></td>
<td>Threats, both internal and external, are identified and documented</td>
<td>CIS CSC 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 Clause 6.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16</td>
</tr>
<tr>
<td>ID.RA-4:</td>
<td></td>
<td>Potential business impacts and likelihoods are identified</td>
<td>CIS CSC 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS04.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 Clause 6.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11</td>
</tr>
<tr>
<td>ID.RA-5:</td>
<td></td>
<td>Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</td>
<td>CIS CSC 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO12.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.12.6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16</td>
</tr>
<tr>
<td>ID.RA-6:</td>
<td></td>
<td>Risk responses are identified and prioritized</td>
<td>CIS CSC 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO12.05, APO13.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 Clause 6.1.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11</td>
</tr>
<tr>
<td>Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID.RM-1:</td>
<td></td>
<td>Risk management processes are established, managed, and agreed to by</td>
<td>CIS CSC 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>organizational stakeholders</td>
<td>COBIT 5 APO12.04, APO12.05, APO13.02, BA102.03, BA104.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 PM-4, PM-9</td>
</tr>
<tr>
<td>ID.RM-2:</td>
<td></td>
<td>Organizational risk tolerance is determined and clearly expressed</td>
<td>COBIT 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>APO12.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.2.6.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 PM-9</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>ID.RM-3</td>
<td></td>
<td><strong>Supply Chain Risk Management (ID.SC):</strong>&lt;br&gt;The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</td>
<td>COBIT 5 APO12.02&lt;br&gt;ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3&lt;br&gt;NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-1</td>
<td>CIS CSC 4&lt;br&gt;COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BA101.03, BA102.03, BA104.02&lt;br&gt;ISA 62443-2-1:2009 4.3.4.2&lt;br&gt;ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2&lt;br&gt;NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-2</td>
<td>COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BA102.03&lt;br&gt;ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.7, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14&lt;br&gt;ISO/IEC 27001:2013 A.15.2.1, A.15.2.2&lt;br&gt;NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-3</td>
<td>COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05&lt;br&gt;ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7&lt;br&gt;ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15 1.3&lt;br&gt;NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-4</td>
<td>COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05&lt;br&gt;ISA 62443-2-1:2009 4.3.2.6.7&lt;br&gt;ISA 62443-3-3:2013 SR 6.1&lt;br&gt;ISO/IEC 27001:2013 A.15.2.1, A.15.2.2</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| PROTECT (PR) | Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | CIS CSC 1, 5, 15, 16  
COBIT 5 DSS05.04, DSS06.03  
ISA 62443-2-1:2009 4.3.3.5.1  
ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9  
NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 |
| | PR.AC-2: Physical access to assets is managed and protected | COBIT 5 DSS01.04, DSS05.05  
ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.3.8  
NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 |
| | PR.AC-3: Remote access is managed | CIS CSC 12  
COBIT 5 APO13.01, DSS01.04, DSS05.03  
ISA 62443-2-1:2009 4.3.3.6.6  
ISA 62443-3-3:2013 SR 1.13, SR 2.6  
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties</td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15</td>
<td></td>
</tr>
<tr>
<td>PR.AC-5: Network integrity is protected (e.g., network segmentation)</td>
<td></td>
<td>CIS CSC 3, 5, 12, 14, 15, 16, 18</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COBIT 5 DSS05.04</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.7.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 2.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24</td>
<td></td>
</tr>
<tr>
<td>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions</td>
<td></td>
<td>CIS CSC 9, 14, 15, 18</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COBIT 5 DSS01.05, DSS05.02</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 3.1, SR 3.8</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7</td>
<td></td>
</tr>
<tr>
<td>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)</td>
<td></td>
<td>CIS CSC 1, 12, 15, 16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COBIT 5 DSS05.04, DSS05.10, DSS06.10</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| Awareness and Training (PR.AT) | All users are informed and trained | | CIS CSC 17, 18  
COBIT 5 APO07.03, BAI05.07  
ISA 62443-2-1:2009 A.3.2.4.2  
ISO/IEC 27001:2013 A.7.2.2, A.12.2.1  
NIST SP 800-53 Rev. 4 AT-2, PM-13 |
| PR.AT-2: Privileged users understand their roles and responsibilities | | CIS CSC 5, 17, 18  
COBIT 5 APO07.02, DSS05.04, DSS06.03  
ISA 62443-2-1:2009 A.3.2.4.2, A.3.2.4.3  
ISO/IEC 27001:2013 A.6.1.1, A.7.2.2  
NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities | | CIS CSC 17  
COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05  
ISA 62443-2-1:2009 A.3.2.4.2  
ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2  
NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16 |
| PR.AT-4: Senior executives understand their roles and responsibilities | | CIS CSC 17, 19  
COBIT 5 EDM01.01, APO01.02, APO07.03  
ISA 62443-2-1:2009 A.3.2.4.2  
ISO/IEC 27001:2013 A.6.1.1, A.7.2.2  
NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities | | CIS CSC 17  
COBIT 5 APO07.03  
ISA 62443-2-1:2009 A.3.2.4.2  
ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security (PR.DS)</td>
<td></td>
<td>PR.DS-1: Data-at-rest is protected</td>
<td>CIS CSC 13, 14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 3.4, SR 4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.8.2.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS-2: Data-in-transit is protected</td>
<td>CIS CSC 13, 14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO01.06, DSS05.02, DSS06.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS-3: Assets are formally managed throughout removal, transfers, and</td>
<td>CIS CSC 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 BAI09.03</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS-4: Adequate capacity to ensure availability is maintained</td>
<td>CIS CSC 1, 2, 13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO13.01, BAI04.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 7.1, SR 7.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.12.1.3, A.17.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS-5: Protections against data leaks are implemented</td>
<td>CIS CSC 13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 5.2</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>PR.DS-6:</td>
<td>Integrity checking mechanisms are used to verify software, firmware, and information integrity.</td>
<td>CIS CSC 2.3, COBIT 5 AP0106.01, A11.21, A13.1.3.1, A13.2.1, A13.2.2, A13.2.4, A14.1.2, A14.1.3, A14.1.4, SC-8, SC-13, SC-31, SL-4</td>
<td>NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-3, PS-3, SC-7, SC-8, SC-13, SC-31, SL-4</td>
</tr>
<tr>
<td>PR.DS-7:</td>
<td>The development and testing environments are separate from the production environment.</td>
<td>CIS CSC 18, 20, COBIT 5 BA03.08, BA07.04</td>
<td>NIST SP 800-53 Rev. 4 SC-16, SI-7</td>
</tr>
<tr>
<td>PR.DS-8:</td>
<td>Integrity checking mechanisms are used to verify hardware integrity.</td>
<td>CIS CSC 2.3, A14.1.3, A14.2.4</td>
<td>NIST SP 800-53 Rev. 4 SC-16, SI-7</td>
</tr>
<tr>
<td>PR.IP-1:</td>
<td>A baseline configuration of information technology/industrial control systems is created and maintained.</td>
<td>CIS CSC 3.9, 11, COBIT 5 BA03.01, BA03.02, BA10.03, BA10.05</td>
<td>ISO/IEC 27001:2013 A12.2.1, A12.2.2, A14.2.3, A14.2.4, ISO/IEC 27001:2013 A11.2.4, ISO/IEC 27001:2013 A12.2.1, A12.2.2, A14.2.3, A14.2.4, CM-5, CM-6, CM-7, CM-9, SA-10, SI-7</td>
</tr>
<tr>
<td>PR.IP-2:</td>
<td>Cycle to manage systems is implemented.</td>
<td>CIS CSC 18, COBIT 5 AP013.01, BA03.01, BA10.02, BA10.03, BA10.05</td>
<td>ISO/IEC 27001:2013 A12.2.1, A12.2.2, A14.2.3, A14.2.4, CM-5, CM-6, CM-7, CM-9, SA-10</td>
</tr>
</tbody>
</table>

**Information Protection Processes and Procedures**

- **PR.IP-1:** Security policies that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, are maintained and used to manage information systems and assets.

- **PR.IP-2:** A System Development Life Cycle to manage systems is implemented.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| **PR.IP-3:** Configuration change control processes are in place | | | ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5  
NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 |
| **PR.IP-4:** Backups of information are conducted, maintained, and tested | | | CIS CSC 3, 11  
COBIT 5 BA101.06, BA106.01  
ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3  
ISA 62443-3-3:2013 SR 7.6  
NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 |
| **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met | | | CIS CSC 10  
COBIT 5 APO13.01, DSS01.01, DSS04.07  
ISA 62443-2-1:2009 4.3.4.3.9  
ISA 62443-3-3:2013 SR 7.3, SR 7.4  
NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 |
| **PR.IP-6:** Data is destroyed according to policy | | | COBIT 5 DSS01.04, DSS05.05  
ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6  
NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 |

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.IP-7</td>
<td></td>
<td>Protection processes are improved</td>
<td>COBIT 5 APO11.06, APO12.06, DSS04.05&lt;br&gt;ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8&lt;br&gt;ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10&lt;br&gt;NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6</td>
</tr>
<tr>
<td>PR.IP-8</td>
<td></td>
<td>Effectiveness of protection technologies is shared</td>
<td>COBIT 5 BAI08.04, DSS03.04&lt;br&gt;ISO/IEC 27001:2013 A.16.1.6&lt;br&gt;NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4</td>
</tr>
<tr>
<td>PR.IP-9</td>
<td></td>
<td>Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</td>
<td>CIS CSC 19&lt;br&gt;COBIT 5 APO12.06, DSS04.03&lt;br&gt;ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1&lt;br&gt;ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3&lt;br&gt;NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17</td>
</tr>
<tr>
<td>PR.IP-10</td>
<td></td>
<td>Response and recovery plans are tested</td>
<td>CIS CSC 19, 20&lt;br&gt;COBIT 5 DSS04.04&lt;br&gt;ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11&lt;br&gt;ISA 62443-3-3:2013 SR 3.3&lt;br&gt;ISO/IEC 27001:2013 A.17.1.3&lt;br&gt;NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14</td>
</tr>
<tr>
<td>PR.IP-11</td>
<td></td>
<td>Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)</td>
<td>CIS CSC 5, 16&lt;br&gt;COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05&lt;br&gt;ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3&lt;br&gt;ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4&lt;br&gt;NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PR.PT-3:</strong> The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</td>
<td></td>
<td>NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8</td>
<td></td>
</tr>
<tr>
<td><strong>PR.PT-4:</strong> Communications and control networks are protected</td>
<td></td>
<td>CIS CSC 3, 11, 14, COBIT 5 DSS05.02, DSS05.05, DSS06.06, ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4, ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7, ISO/IEC 27001:2013 A.9.1.2, NIST SP 800-53 Rev. 4 AC-3, CM-7</td>
<td></td>
</tr>
<tr>
<td><strong>DETECT (DE): Anomalies and Events (DE.AE):</strong> Anomalous activity is detected</td>
<td><strong>DE.AE-1:</strong> A baseline of network operations and expected data flows for</td>
<td>CIS CSC 1, 4, 6, 12, 13, 15, 16, COBIT 5 DSS03.01, ISA 62443-2-1:2009 4.4.3.3</td>
<td></td>
</tr>
</tbody>
</table>
### Function and the potential impact of events is understood.

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4</td>
</tr>
<tr>
<td>DE.AE-2: Detected events are analyzed to understand attack targets and methods</td>
<td>CIS CSC 3, 6, 13, 15</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 DSS05.07</td>
</tr>
<tr>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8</td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2</td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4</td>
</tr>
<tr>
<td>DE.AE-3: Event data are collected and correlated from multiple sources and sensors</td>
<td>CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 BA108.02</td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 6.1</td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4</td>
</tr>
<tr>
<td>DE.AE-4: Impact of events is determined</td>
<td>CIS CSC 4, 6</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 APO12.06, DSS03.01</td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 27001:2013 A.16.1.4</td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4</td>
</tr>
<tr>
<td>DE.AE-5: Incident alert thresholds are established</td>
<td>CIS CSC 6, 19</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 APO12.06, DSS03.01</td>
</tr>
<tr>
<td></td>
<td>ISA 62443-2-1:2009 4.2.3.10</td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 27001:2013 A.16.1.4</td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8</td>
</tr>
</tbody>
</table>

### Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify

<table>
<thead>
<tr>
<th>DE.CM-1: The network is monitored to detect potential cybersecurity events</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CIS CSC 1, 7, 8, 12, 13, 15, 16</td>
</tr>
<tr>
<td></td>
<td>COBIT 5 DSS01.03, DSS03.05, DSS05.07</td>
</tr>
<tr>
<td></td>
<td>ISA 62443-3-3:2013 SR 6.2</td>
</tr>
<tr>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| DE.CM-2: | The physical environment is monitored to detect potential cybersecurity events | | COBIT 5 DSS01.04, DSS01.05  
ISA 62443-2-1:2009 A.3.3.3.8  
NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 |
| DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events | | COBIT 5 DSS05.07  
ISA 62443-3-3:2013 SR 6.2  
ISO/IEC 27001:2013 A.12.4.1, A.12.4.3  
NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 |
| DE.CM-4: Malicious code is detected | | COBIT 5 DSS05.01  
ISA 62443-2-1:2009 A.3.4.3.8  
ISA 62443-3-3:2013 SR 3.2  
ISO/IEC 27001:2013 A.12.2.1  
NIST SP 800-53 Rev. 4 SI-3, SI-8 |
| DE.CM-5: Unauthorized mobile code is detected | | COBIT 5 DSS05.01  
ISA 62443-3-3:2013 SR 2.4  
ISO/IEC 27001:2013 A.12.5.1, A.12.6.2  
NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44 |
| DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events | | COBIT 5 APO07.06, APO10.05  
ISO/IEC 27001:2013 A.14.2.7, A.15.2.1  
NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 |
| DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed | | COBIT 5 DSS05.02, DSS05.05  
ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1  
NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 |
| DE.CM-8: Vulnerability scans are performed | | COBIT 5 DSS05.02, DSS05.05  
ISO/IEC 27001:2013 A.14.2.7, A.15.2.1  
NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 |

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. | DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability | COBIT 5 BA03.10, DSS05.01  
ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7  
ISO/IEC 27001:2013 A.12.6.1  
NIST SP 800-53 Rev. 4 RA-5 | CIS CSC 19  
COBIT 5 APO01.02, DSS05.01, DSS06.03  
ISA 62443-2-1:2009 4.4.3.1  
ISO/IEC 27001:2013 A.6.1.1, A.7.2.2  
NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 |
| DE.DP-2: Detection activities comply with all applicable requirements | COBIT 5 DSS06.01, MEA03.03, MEA03.04  
ISA 62443-2-1:2009 4.4.3.2  
NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14 | |
| DE.DP-3: Detection processes are tested | COBIT 5 APO13.02, DSS05.02  
ISA 62443-2-1:2009 4.4.3.2  
ISA 62443-3-3:2013 SR 3.3  
ISO/IEC 27001:2013 A.14.2.8  
NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 | |
| DE.DP-4: Event detection information is communicated | CIS CSC 19  
COBIT 5 APO08.04, APO12.06, DSS02.05  
ISA 62443-2-1:2009 4.3.4.5.9  
ISA 62443-3-3:2013 SR 6.1  
NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 | |
| DE.DP-5: Detection processes are continuously improved | COBIT 5 APO11.06, APO12.06, DSS04.05  
ISA 62443-2-1:2009 4.4.3.4  
ISO/IEC 27001:2013 A.16.1.6  
NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 | |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESPOND (RS)</td>
<td>Response Planning (RS.RP):</td>
<td>RS.RP-1: Response plan is executed during or after an incident</td>
<td>CIS CSC 19</td>
</tr>
<tr>
<td></td>
<td>- Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</td>
<td></td>
<td>COBIT 5 APO12.06, BAI01.10</td>
</tr>
<tr>
<td></td>
<td>Communications (RS.CO):</td>
<td>RS.CO-1: Personnel know their roles and order of operations when a response is needed</td>
<td>CIS CSC 19</td>
</tr>
<tr>
<td></td>
<td>- Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</td>
<td></td>
<td>COBIT 5 EDM03.02, APO01.02, APO12.03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO-2: Incidents are reported consistent with established criteria</td>
<td>CIS CSC 19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS03.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2:1:2009 4.3.4.5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SI-5, PM-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SI-5, PM-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SI-5, PM-15</td>
</tr>
</tbody>
</table>

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis (RS.AN)</td>
<td>Analysis is conducted to ensure effective response and support recovery activities.</td>
<td>RS.AN-1: Notifications from detection systems are investigated</td>
<td>CIS CSC 4, 6, 8, 19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS02.04, DSS02.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS02.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO12.06, DSS03.02, DSS05.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-7, IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RS.AN-2: The impact of the incident is understood</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RS.AN-3: Forensics are performed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS02.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO12.06, DSS03.02, DSS05.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-7, IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IS.C CSC 4, 19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS02.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.5.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.16.1.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 EDM03.02, DSS05.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SI-5, PM-15</td>
</tr>
<tr>
<td>Mitigation (RS.MI)</td>
<td>Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</td>
<td>RS.MI-1: Incidents are contained</td>
<td>COBIT 5 DSS02.04, DSS02.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.5.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4</td>
</tr>
</tbody>
</table>

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>RS.MI-2:</strong> Incidents are mitigated</td>
<td>NIST SP 800-53 Rev. 4 IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RS.MI-3:</strong> Newly identified vulnerabilities are mitigated or documented as accepted risks</td>
<td>CIS CSC 4, 19, COBIT 5 APO12.06, ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10, ISO/IEC 27001:2013 A.12.2.1, A.16.1.5, NIST SP 800-53 Rev. 4 IR-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Improvements (RS.IM):</strong> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</td>
<td>COBIT 5 APO12.06, ISO/IEC 27001:2013 A.12.6.1, NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RS.IM-1:</strong> Response plans incorporate lessons learned</td>
<td>COBIT 5 BAI01.13, ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4, ISO/IEC 27001:2013 A.16.1.6, Clause 10, NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RS.IM-2:</strong> Response strategies are updated</td>
<td>COBIT 5 BAI01.13, DSS04.08, ISO/IEC 27001:2013 A.16.1.6, Clause 10, NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RECOVER (RC) Recovery Planning (RC.RP):</strong> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</td>
<td>CIS CSC 10, COBIT 5 APO12.06, DSS02.05, DSS03.04, ISO/IEC 27001:2013 A.16.1.5, NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RC.RP-1:</strong> Recovery plan is executed during or after a cybersecurity incident</td>
<td>COBIT 5 APO12.06, BAI05.07, DSS04.08, ISA 62443-2-1:2009 4.4.3.4, ISO/IEC 27001:2013 A.16.1.6, Clause 10, NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Improvements (RC.IM):</strong> Recovery planning and processes are improved by incorporating lessons learned into future activities.</td>
<td>COBIT 5 APO12.06, BAI07.08, ISO/IEC 27001:2013 A.16.1.6, Clause 10, NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RC.IM-1:</strong> Recovery plans incorporate lessons learned</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>RC.IM-2:</strong> Recovery strategies are updated</td>
<td></td>
</tr>
</tbody>
</table>
### Function

<table>
<thead>
<tr>
<th>Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC.CO-1: Public relations are managed</td>
</tr>
<tr>
<td>RC.CO-2: Reputation is repaired after an incident</td>
</tr>
<tr>
<td>RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams</td>
</tr>
</tbody>
</table>

### Informative References

<table>
<thead>
<tr>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT 5 EDM03.02</td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 A.6.1.4, Clause 7.4</td>
</tr>
<tr>
<td>COBIT 5 MEA03.02</td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 Clause 7.4</td>
</tr>
<tr>
<td>COBIT 5 APO12.06</td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 Clause 7.4</td>
</tr>
<tr>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4</td>
</tr>
</tbody>
</table>

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): [http://www.isaca.org/COBIT/Pages/default.aspx](http://www.isaca.org/COBIT/Pages/default.aspx)
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): [https://www.cisecurity.org](https://www.cisecurity.org)

Informative References are only mapped to the control level, though any control enhancement might be found useful in achieving a subcategory outcome.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

Informative References are not exhaustive, in that not every element (e.g., control, requirement) of a given Informative Reference is mapped to Framework Core Subcategories.
Appendix B: Glossary

This appendix defines selected terms used in the publication.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buyer</td>
<td>The people or organizations that consume a given product or service.</td>
</tr>
<tr>
<td>Category</td>
<td>The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”</td>
</tr>
<tr>
<td>Critical Infrastructure</td>
<td>Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>The process of protecting information by preventing, detecting, and responding to attacks.</td>
</tr>
<tr>
<td>Cybersecurity Event</td>
<td>A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).</td>
</tr>
<tr>
<td>Cybersecurity Incident</td>
<td>A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.</td>
</tr>
<tr>
<td>Detect (function)</td>
<td>Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.</td>
</tr>
<tr>
<td>Framework</td>
<td>A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”</td>
</tr>
<tr>
<td>Framework Core</td>
<td>A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.</td>
</tr>
<tr>
<td>Framework Implementation Tier</td>
<td>A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.</td>
</tr>
<tr>
<td><strong>Framework Profile</strong></td>
<td>A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Function</strong></td>
<td>One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.</td>
</tr>
<tr>
<td><strong>Identify (function)</strong></td>
<td>Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.</td>
</tr>
<tr>
<td><strong>Informative Reference</strong></td>
<td>A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the “Data-in-transit is protected” Subcategory of the “Data Security” Category in the “Protect” function.</td>
</tr>
<tr>
<td><strong>Mobile Code</strong></td>
<td>A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.</td>
</tr>
<tr>
<td><strong>Protect (function)</strong></td>
<td>Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.</td>
</tr>
<tr>
<td><strong>Privileged User</strong></td>
<td>A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.</td>
</tr>
<tr>
<td><strong>Recover (function)</strong></td>
<td>Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.</td>
</tr>
<tr>
<td><strong>Respond (function)</strong></td>
<td>Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>The process of identifying, assessing, and responding to risk.</td>
</tr>
<tr>
<td><strong>Subcategory</strong></td>
<td>The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”</td>
</tr>
<tr>
<td><strong>Supplier</strong></td>
<td>Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.</td>
</tr>
<tr>
<td><strong>Taxonomy</strong></td>
<td>A scheme of classification.</td>
</tr>
</tbody>
</table>
Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

ANSI  American National Standards Institute
CEA   Cybersecurity Enhancement Act of 2014
CIS   Center for Internet Security
COBIT Control Objectives for Information and Related Technology
CPS   Cyber-Physical Systems
CSC   Critical Security Control
DHS   Department of Homeland Security
EO    Executive Order
ICS   Industrial Control Systems
IEC   International Electrotechnical Commission
IoT   Internet of Things
IR    Interagency Report
ISA   International Society of Automation
ISAC  Information Sharing and Analysis Center
ISAO  Information Sharing and Analysis Organization
ISO   International Organization for Standardization
IT    Information Technology
NIST  National Institute of Standards and Technology
OT    Operational Technology
PII   Personally Identifiable Information
RFI   Request for Information
RMP   Risk Management Process
SCRM  Supply Chain Risk Management
SP    Special Publication
Institute Cybersecurity and Risk Governance Practices to Improve Information Security

**FOUNDAIONAL**  
*Refreshed: 4 May 2018 | Published: 26 January 2017  | ID: G00317760*

Analyst(s): Tom Scholtz, Rob McMillan

Effective governance should be a cornerstone of security programs, and ineffective governance is the most common cause of failure. Security and risk management leaders need to implement governance capabilities that support accountability, authority, risk management and assurance.

**FOUNDATIONAL DOCUMENT**  
This research is reviewed periodically for accuracy. Last reviewed on 4 May 2018.

**Key Challenges**

- In many organizations, security and security risk governance practices are still immature, and they often lack executive support and business participation.
- Many organizations struggle to establish clear accountability and authority, which are key prerequisites for effective, risk-based security decision making.
- The increasing adoption of digital business strategies has resulted in citizen IT initiatives that challenge conventional security and security risk governance practices.

**Recommendations**

Security and risk management leaders responsible for information security management programs should:

- Implement governance processes and activities that support accountability, authority, risk management and assurance.
- Institute governance roles and forums that will support decision making and oversight.
- Ensure that the right people, with appropriate authority to make governance decisions, are involved in the governance processes and forums.
Table of Contents

Introduction.......................................................................................................................... 2
Analysis................................................................................................................................. 3
Implement Governance Processes and Activities That Support Accountability, Authority, Risk
Management and Assurance............................................................................................ 3
Set and Manage Accountability and Decision Rights......................................................... 4
Decide Acceptable Risk........................................................................................................ 5
Enable Risk Control............................................................................................................ 6
Assure Control Effectiveness.............................................................................................. 6
Institute Appropriate Governance Roles and Forums..................................................... 6
The Executive Sponsor....................................................................................................... 8
The Cybersecurity Steering Committee............................................................................ 9
Midlevel Forums................................................................................................................ 9
Cyber/Information Security Teams.................................................................................. 9
Ensure That the Right People Are Involved in Governance Activities......................... 10
Gartner Recommended Reading....................................................................................... 10

List of Tables

Table 1. Governance Roles and Forums............................................................................. 8

List of Figures

Figure 1. Macro Security and Risk Governance Process................................................. 3
Figure 2. Security and Risk Governance Processes and Activities................................. 4
Figure 3. Simplified Example RACI Chart for Application Risk....................................... 7

Introduction

This document was revised on 1 May 2018. For more information, see the Corrections page.

Gartner research indicates that many organizations are struggling to implement effective
cybersecurity and security risk governance practices.¹ This immaturity results in a lack of clarity on
risk ownership in the enterprise, inhibiting its ability to effectively and safely exploit the business
benefits of the digital transformation.²
Security and risk governance is defined as the processes and capabilities that ensure that reasonable and appropriate actions are taken to protect the organization's information resources, in the most effective and efficient manner, in pursuit of its business objectives. There are four primary goals:

- To set and manage accountability and decision rights
- To decide what is acceptable risk
- To enable risk control
- To provide assurance to executives and stakeholders that information risk is being managed appropriately

Security and risk governance is a continuous process (see Figure 1) that provides risk and assurance capability against a backdrop of continuous change in the business, technology and threat environments.

Figure 1. Macro Security and Risk Governance Process

Analysis

Implement Governance Processes and Activities That Support Accountability, Authority, Risk Management and Assurance

The single most important goal of the governance function is to establish and manage clear accountability and decision rights for the protection of the enterprise's information resources (see Figure 2). Without this, security policies will be ineffective, security processes will fail, moral hazards (see Note 1) will prevail and risks will not be controlled.
Figure 2. Security and Risk Governance Processes and Activities

Set and Manage Accountability and Decision Rights

- Enterprise Security Charter
- Policy Framework
- Organization

Decide Acceptable Risk
- Assessment
- Policies
- Arbitration

Enable Risk Control
- Program
- Strategy
- Resource Allocation

Assure Control Effectiveness
- Assessments
- Metrics

Source: Gartner (January 2017)

Set and Manage Accountability and Decision Rights

The principle of owner accountability must be documented in an enterprise security charter (ESC; see "Best Practices for Creating an Enterprise Information Security Charter"), which is signed and clearly supported by the chief executive and the board. It must clearly state that the ultimate accountability for protecting the enterprise’s information resources and, by implication, its business processes and outcomes, rests with the business owners of the information resources. The biggest security weaknesses are often inherent in weak business processes, and these present major risks to the information and to business outcomes. The ESC must establish that the resource owners have the authority to make the risk-based decisions required to fulfill their accountability. Resource owners are typically business process, application and data owners (i.e., the roles that own the security risk).

When clear business resource ownership cannot be identified (e.g., in cases of shared information and infrastructure), the accountability, risk ownership and associated authority must be vested with the CIO, or another central function, such as the COO.

The detailed accountability and decision rights for the security and risk processes should be documented and communicated through the use of responsible, accountable, consulted and informed (RACI) charts. The ESC must also provide a clear mandate for establishing and managing an information/cybersecurity program, including determining its scope (see "CISOs Need to Understand the Components of Their Information Security Programs"). This mandate typically vests the chief information security officer (CISO) with the responsibility and authority to run the program.
Digital business transformation provides new challenges to security and risk governance (see "Managing Risk and Security at the Speed of Digital Business"), and it is imperative that the six principles of trust and resilience in digital business are also captured in the ESC (see "Use Six Principles of Resilience to Address Digital Business Risk and Security").

One practical manifestation of the accountability and decision rights for security risk is the policy management process and framework that the resource owners, CIOs and CISOs must use to implement their risk control decisions. The CISO is responsible for defining a security policy hierarchy and process that will make this as easy and effective as possible (see "Five Golden Rules for Creating Effective Security Policy" and "Ten Security Policy Writing Mistakes You Cannot Afford to Make").

Another practical manifestation of accountability is the structure of the security organization. There is no single best-practice template for the security organization; however, from a governance perspective, it is important to optimally balance the assurance, strategic and operational processes and tasks in a practical organizational model (see "Security Governance, Management and Operations Are Not the Same"). In the context of digital business, the onus is on senior leadership to invest in developing and recruiting the new skills required for such processes as agile and Mode 2 development, which increasingly integrate operational technology and the Internet of Things.

Decide Acceptable Risk

The second major goal of the governance function is to decide levels of acceptable risk. This entails empowering the resource owners, the CIO and the CISO with the context, skills and resources to perform appropriate risk assessments. Based on the results of these assessments, the resource owners must decide how much risk is acceptable, as well as how to deal with the unacceptable risk at a defined cost. The risk treatment plan must then be approved by the relevant governance body and formalized in policies and appropriate controls.

In a digital business environment, this implies that all the relevant parties understand and can deal with the potentially conflicting risk appetites inherent in both agile and Mode 2 projects (see "The Four Steps to Manage Risk and Security in Bimodal IT").

An important element of managing risk is to understand that individual resource owners might have different risk appetites, and that these could conflict with the formal corporate risk appetite or with the risk appetites of other resource owners. Hence, a key governance function is to implement and manage a process to arbitrate among conflicting risk appetites. Typical conflicts that require arbitrations include situations in which:

- A resource owner believes he or she has a valid business reason for requesting exemption from existing policy or control requirements for an application or system.
- Different resource owners have different risk appetites — hence, different security control requirements — for their systems, even though these systems will share infrastructure. The prevalence of this type of conflict increases in organizations embracing digital business development strategies.
A business owner may be willing to accept a risk, but the risk exceeds the enterprise's risk appetite.

Enable Risk Control

The third governance goal is to enable effective risk control within a context of limited financial and human resources. The key enabler for effective risk control is to establish:

- A formal security program (see "CISOs Need to Understand the Components of Their Information Security Programs") that implements and operates the security controls. In too many organizations, these security programs look to implement controls for the sake of having controls (often guided by some arbitrarily selected control framework), rather than understanding the real risk context. Although the security team is typically responsible for the practical implementation and operation of most security controls, the governance function must ensure the proper prioritization of security investments, based on the criteria of expected risk reduction, the resource requirements and the expected time to value of the respective projects in the roadmap.

- A strategic planning capability that enables the organization to develop and refine a roadmap of investments that recognizes continuous change in the business, technology and threat environments (see "Security Management Strategy Planning Best Practices").

The increased velocity associated with digital business means that organizations are increasing the frequency (and decreasing the planning horizons) of their strategic planning activities. In the past, enterprises commonly developed security strategy plans with three- to five-year horizons every three years; however, most now have an annual plan with a two- to three-year planning horizon. More-mature organizations are formalizing a quarterly review of their security strategies to make timely adjustments, based on changes in the business, technology and threat environments.

Assure Control Effectiveness

The fourth governance goal is to assure control effectiveness. This typically entails periodic policy and control compliance assessments, including evaluating the retained risk and deciding whether additional remedial investment is required. This function also includes ensuring that prescribed security controls are integrated into new applications or infrastructure projects, before they are accepted into production.

Finally, this entails collecting appropriate metrics operational and assurance metrics. They should be reported regularly to the security governance bodies and to executive leadership (see "Sharpen Your Security Metrics to Make Them Relevant and Effective").

Institute Appropriate Governance Roles and Forums

Security accountability is often neglected or misunderstood. Organizations often view the CISO as the single, accountable role for the security posture of an organization. However, mature organizations understand that the accountability for the security and risk position of the organization rests with the senior executives who are ultimately responsible for the resources and business
processes that support the organization’s business outcomes (see "Achieve Level 4 Maturity in Gartner’s ITScore for Information Security").

The CISO is accountable for identifying security risks and for implementing security controls; however, the governance function, as typically represented by an enterprise security steering committee, is ultimately accountable for setting the security and risk direction of the organization and ensuring that the CISO has the required resources. The CISO is also responsible for ensuring that the responsible executives make prudent decisions, but the executives themselves are accountable for those decisions. Although leading organizations understand this and have accountability models that implement a chain of responsibility that aligns with this approach, Gartner speaks with many organizations that have more-traditional approaches in which the CISO bears a large, if not complete, degree of responsibility and accountability, often without the necessary resources and authority. Setting such an accountability model in written form in the ESC and via a RACI chart can clarify the requirements expected from the role players (see Figure 3).

Figure 3. Simplified Example RACI Chart for Application Risk

<table>
<thead>
<tr>
<th>Role</th>
<th>Assess Risk</th>
<th>Manage Risk</th>
<th>Fund Resources</th>
<th>Implement</th>
<th>Assure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Owner</td>
<td>I</td>
<td>R, A</td>
<td>R, A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>IT</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>R, A</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Security</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>R</td>
</tr>
</tbody>
</table>

**Responsible:** Person or function responsible for executing the activity  
**Accountable:** Person or function that owns the activity, approves work and is held accountable for it  
**Consulted:** Person or function with information relevant to the activity  
**Informed:** Person or function to be informed of progress and results

Source: Gartner (January 2017)

Gartner research indicates that it is a best practice to use a multilayer governance structure (see Table 1). This supports scalable governance around different scopes of control, functions and outcomes (see "Security Governance, Management and Operations Are Not the Same").
### Table 1. Governance Roles and Forums

<table>
<thead>
<tr>
<th>Forums/Roles</th>
<th>Functions</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Sponsor</td>
<td>• Set accountability and authority</td>
<td>• Policy legitimacy and awareness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authority of the information security program</td>
</tr>
<tr>
<td>Cybersecurity Steering Committee</td>
<td>• Risk assurance</td>
<td>• Policies and strategies</td>
</tr>
<tr>
<td></td>
<td>• Policy and strategy endorsement</td>
<td>• Control decisions</td>
</tr>
<tr>
<td></td>
<td>• Program oversight</td>
<td>• Budgets</td>
</tr>
<tr>
<td></td>
<td>• Conciliation/arbitration</td>
<td>• Priorities</td>
</tr>
<tr>
<td></td>
<td>• Budget allocation</td>
<td>• Arbitration decisions</td>
</tr>
<tr>
<td></td>
<td>• Approvals and exemptions</td>
<td></td>
</tr>
<tr>
<td>Midlevel Councils</td>
<td>• Project oversight</td>
<td>• Local policies</td>
</tr>
<tr>
<td></td>
<td>• Local policy definition</td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td>• Reporting</td>
<td></td>
</tr>
<tr>
<td>Cyber/Information Security Teams</td>
<td>• Risk assessment</td>
<td>• Compliance certifications and exceptions</td>
</tr>
<tr>
<td></td>
<td>• Project oversight</td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td>• Operations oversight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policy compliance monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reporting</td>
<td></td>
</tr>
</tbody>
</table>

Source: Gartner (January 2017)

**The Executive Sponsor**

The top-level governance entity sets the accountability for protecting information resources and the associated level of authority required throughout all of the governance, management and operations layers. It could consist of a single role (e.g., the CEO or CRO), or a small committee of two or three roles (e.g., CEO, CRO and COO). Such committees typically meet once or twice a year, but they can meet more frequently, as needs dictate.

The additional responsibilities of this function are to establish top-down support for security policy, to institute the relevant governance bodies and to act as the main champion of the information security program. It should ensure that the relevant steering committee has the authority to arbitrate conflicting security and risk requirements.
The Cybersecurity Steering Committee
The main functions of this committee are to:

- Set, communicate and ensure the respective accountabilities for information security and risk
- Oversee risk and control decisions
- Formally endorse and authorize security policies
- Approve and allocate the budget of the security and risk management program
- Guide the security and risk program and the architecture strategy
- Oversee the program execution and assess the value of security investments, processes and activities
- Review requests for policy and risk exemptions
- Monitor the accumulated risk represented by the existing policy and control exceptions
- Conciliate or arbitrate among conflicting security requirements

This committee typically consists of business unit managers; C-level executives from HR, financial, legal, risk and governance; the CISO; and the CIO. Members should be sufficiently senior to make binding trade-off decisions, and to positively recommend enterprise-wide security spending decisions. These forums typically meet quarterly, or sometimes monthly (see "Best Practices for Establishing an Information Security Steering Committee").

Midlevel Forums
Large organizations often attempt to achieve scalability in their governance processes by instituting midlevel counsels or committees. Typically, the primary focus of such forums is to provide local governance in decentralized or federated enterprises. In organizations that have experienced issues with participation and support for information security, such additional layers of governance can contribute to greater levels of buy-in. The main activities are to agree on local security policies and standards, to monitor localized security projects, to act as local representatives of the executive sponsor and the corporate steering committee, and to report back to these functions on general policy compliance and emerging issues.

Inasmuch as the adoption of digital business strategies is driven from within the business units, rather than from central IT, regional forums can play an effective role in governing citizen IT projects. Membership typically consists of the CISO, regional and midlevel business managers, and local IT management. These forums generally meet monthly.

Cyber/Information Security Teams
Although security teams typically have management and operational responsibilities, a sizable part of the functions of these teams is oversight (i.e., they "ensure," rather than manage or execute). Such functions include the development of security policy, the oversight of IT projects (including risk
assessments), and policy compliance scanning and monitoring. The team also acts as an initiator and consolidator of governance reporting functions.

Ensure That the Right People Are Involved in Governance Activities

Common governance mistakes include:

- Populating the governance forum with IT and/or security staff, leading to security and risk decisions that do not reflect the organization's business needs
- Allowing senior staff to send delegates to attend meetings, which leads to moribund committees that are either unwilling or unable to set direction and make difficult, unpopular or expensive decisions.

The effectiveness of information security and risk governance depends heavily on the profiles and attitudes of the people involved in the governance bodies and processes. Participants must have the authority to make decisions, commensurate with the scope of the relevant forum or function, on behalf of the constituencies that they represent. Although participants might occasionally have to defer to their line management on major decisions, they should be able to decide on most issues without resorting to this.

One pitfall to avoid is having appointed members of committees regularly (or permanently) delegate attendance at these forums to their juniors. One way to avert this is to have a rule that absence or delegation to a junior implies agreement with all tabled decisions — in other words, there is no right of veto in absentia or by a delegate, unless the member is on approved leave or travel.

Furthermore, committee members must fully "buy into" the objectives of the respective committees (making committee membership a formal job specification requirement might help). Without the right profiles and attitudes of members, governance forums have the tendency to develop into ineffective debating societies.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Best Practices for Creating an Enterprise Information Security Charter"

"CISOs Need to Understand the Components of Their Information Security Programs"

"Five Golden Rules for Creating Effective Security Policy"

"Security Governance, Management and Operations Are Not the Same"

"Measure, Report and Improve Enterprise Risk-Engaged Culture"

"CIOs Should Manage Technology Risk and Cybersecurity Through the Lens of Business Value"

"Develop a Pragmatic Vision and Strategy for Digital Business Security"
Evidence

1 Primary research conducted by Gartner (see "Survey Analysis: Information Security Governance, 2015-16") indicates that security governance processes are still immature:

- Only 14% of respondents indicated that business unit managers constitute primary membership of governance bodies (n = 407).
- Only 30% of respondents indicated that business units are involved in developing the policies that will affect their business (n = 419).

2 More than 65 Gartner client inquiries on the topic of security governance in 2016

3 More than 260 Gartner client inquiries on the topic of security and risk management strategy in 2016

Note 1 Moral Hazard

A moral hazard is a situation in which a person or role takes more risk, because he or she believes that he or she will only benefit from the positive results of the risky activity, while another person or role will be accountable for the negative consequences (costs) of the risks.
Gartner Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations, visit http://www.gartner.com/technology/about.jsp
Security Management Strategy Planning Best Practices

Analyst(s): Tom Scholz

This research outlines a process for effective strategic planning for the information security program, emphasizing the techniques that are unique to the security discipline. Additionally, it highlights some common pitfalls that planners should avoid.

Key Findings

- Strategic security planning is a waste of time unless it is aligned with business strategy and accommodates environmental trends.
- A usefully comprehensive picture of the current state of a security program can only be generated through the use of multiple different assessment methods.
- Generic benchmarking and survey data (such as security spending as a percent of IT spending) are overrated as sources of security program planning guidance.

Recommendations

- Define an achievable, realistic vision for your organization's security program.
- Use a combination of methods for assessing the current state of your program.
- Maintain clear links between objectives, gaps, and specific projects and actions.
- Report at least quarterly on progress against the strategic plan.

Table of Contents
Analysis

Introduction..............................................................................................................2

The Strategic Planning Process..................................................................................3
    Vision Statement......................................................................................................3
    Business Strategy.....................................................................................................6
    Environmental Trends..............................................................................................6
    Current-State Assessment.......................................................................................7
    Gap Analysis............................................................................................................7
    Prioritization............................................................................................................8
    Approval..................................................................................................................8
    Reporting..................................................................................................................9
    Some Common Pitfalls to Avoid................................................................................9
    Conclusions.............................................................................................................10

Gartner Recommended Reading..................................................................................10

List of Tables

Table 1. Illustrative Linkage of Projects to Current State and Objectives......................8

List of Figures

Figure 1. The Strategic Planning Process....................................................................3
Figure 2. Sample Basic Conceptual Security Program Vision.......................................4
Figure 3. Example: Expanded Security Program Vision...............................................5

Analysis

Introduction

Strategy planning is a key component of an effective information security program (see "The Structure and Scope of an Effective Information Security Program"). While the basic elements of strategic security planning are similar to that of any strategic planning process, there are specific best-practice techniques that are unique to the security discipline. Security managers are often swamped by tactical challenges, impeding their ability to do effective strategic planning. This research outlines a consistent approach and proven techniques that information security leaders should use at least once per year to formalize a strategic plan for their programs.1
The Strategic Planning Process

Figure 1 outlines the basic steps of a strategic planning process that should form the basis of any strategic planning activity.

**Figure 1. The Strategic Planning Process**

![Diagram of the strategic planning process]

Source: Gartner (January 2012)

The following paragraphs outline these process steps in more detail.

**Vision Statement**

The starting point for any strategic plan is to define the desired state, that is, the vision of what the strategy aims to achieve during a defined period. A typical objective of an information security program is to establish a continuous, iteratively improving regimen of planning, building and running
security solutions that are aligned to business requirements. Most organizations will develop an initial vision of such an information security management system (ISMS) from existing standards and frameworks, such as International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, ITIL and COBIT. Figure 2 provides an example that is derived from ISO/IEC 27001 and ITIL.

Figure 2. Sample Basic Conceptual Security Program Vision

OLA = operational-level agreement; SLA = service-level agreement; ITIL = Information Technology Infrastructure Library

Source: Gartner (January 2012)

The vision model outlined in Figure 2, while a good starting point, is too generic for any given organization. Hence, its vision should be expanded and customized so that it provides a meaningful target against which the rest of the planning process can be mapped.

In the first instance, this means adopting and expanding on the basic vision model to ensure it represents the planning and process models used elsewhere in the organization. Figure 3 is an example of a security program vision that retains the process-centric principles outlined in Figure 2, while expanding on the high-level processes and functions that will underpin the ISMS. It also demonstrates how an organization can adopt the "Plan-Do-Check-Act" continuous improvement model from ISO/IEC 27001 to, for example, a "plan-build-run-govern" model that is aligned with process framework in use within that organization (see "Activity Cycle Overview: Security and Risk Management Professionals").
These vision models need to be supplemented by a set of specific objectives that need to be achieved during the planning period. These objectives could, for example, include:

- An overall maturity level for the program
- Target maturity levels for specific processes and functions
- New capabilities to deal with changing technology realities, such as newly emerging threats or disruptive technologies
- A change in the approach to security management — see "No More Dr. No: Developing a Strategy for Business-Aligned Information Security" and "Seven Techniques for More Proactive Risk and Security Management"
- Changes in the security management governance culture and approach in the organization — see "Information Security and Risk Governance: Functions and Processes"
- Effective integration of security reporting into overall risk reporting strategies — see "Introducing Risk-Adjusted Value Management"
- Certification against an industry standard for parts of the enterprise — see "How to Make the Most of ISO/IEC 27001"
Major architectural changes, such as migrating from a perimeter-focused security infrastructure to a more application and data-centric infrastructure

- An ability to support the growth strategy of the enterprise — for example, developing a framework for integrating acquired organizations into the corporate security program

Tagging these objectives with a numbering system (such as O1, O2, and so on) will support consistency throughout the planning process.

Developing these objectives requires an understanding of the business strategy and environmental trends (see the below) and how these influence the practice of information security in the enterprise.

The combined vision models and objectives represent the vision statement for the planning period.

**Business Strategy**

The business strategy should have a major influence on the security strategy. Most commercial organizations have a core strategy based on price, service, quality leadership, or a combination of two of these. This core strategy will directly influence the IT and security strategies. For example, a core business strategy based on price leadership might well be based on the ability to exploit new Internet-based technologies requiring IT and security strategies based on quality leadership.

In addition to the core strategy, the enterprise will typically have a number of ancillary strategies. For example, it might have a market share growth target that can be achieved via acquisition; organic growth; or geographic, vertical or product expansion. It might also have specific strategic objectives regarding the value and position of the brand of the enterprise. All of these strategies can potentially have direct or indirect impact on the security strategy.

Sources of information about the business strategy could include the corporate annual report, “town hall” meetings, interviews with relevant executives and the common requirements vision of the enterprise architecture (see “Advancing the Common Requirements Vision Deliverable”). For example, the security officer of a large power company used corporate initiatives and statements of direction to directly link risk and security efforts to business context. The executives had already created a five-year strategic plan that was rich with guidance and specific terminology. This, in turn, had been used by the CIO to create the IT strategic plan, and echoed many of the important business themes from an IT perspective. It was a relatively straightforward exercise to extend those themes and specific initiatives through the risk and security team’s five-year strategic plan and budgeting requests.

**Environmental Trends**

Trends in the economic, business, market, regulatory, political and technology environments can have a profound impact on the security risk facing the enterprise. Any changes in these environments need to be assessed and, if appropriate, dealt with in the security strategy. Currently, cloud computing, mobile device management and consumerization should feature in most security strategies. For example, organizations exposed to the Eurozone crisis in 2011 through 2012 would include appropriate steps in their security strategy — see "Assessing the Impact of the Euro Crisis on Information Security."
Current-State Assessment

There is no single method for assessing the overall effectiveness and efficiency of security in the enterprise. Most organizations use a combination of different assessment types in order to paint an overall picture:

- Vulnerability assessments and penetration tests to assess the technical infrastructure.
- Risk assessments to balance the investment on controls appropriate to the actual risks (see "Toolkit: Applying the Gartner Risk Assessment Methodology to Critical Enterprise Assets").
- Internal and external audit results to assess the effectiveness of policy and controls compliance.
- Maturity assessments to assess the maturity of the security program and its associated processes. Gartner provides an online security maturity assessment tool (see "ITScore Overview for Security and Risk Management").

The assessment activities often result in an iterative update of the vision statement as newly identified weaknesses dictate new objectives.

The results of the assessment activities must be summarized into a "current state" document or document section that becomes an integral part of the strategic plan document. Once again, numbering the respective current-state findings (for example, C1, C2 and so on) is useful for maintaining planning consistency.

Gap Analysis

Gap analysis consists of mapping the current state against the vision statement, identifying the gaps between the two states in order to derive the actions and projects required to close these gaps.

The diverse nature of the current-state assessments makes the task of identifying specific projects or activities potentially challenging. Some of the gaps will indicate comparatively specific actions — for example, identifying that a specific policy needs to be developed to cater for public cloud computing. But for many gap objectives (such as moving the security governance function from a maturity Level 2.5 to Level 3.5 over two years, or making the security program more business-aligned), it is not always readily obvious what the appropriate mitigation activities are.

Hence, the analysis will often require a certain amount subjective and qualitative decision making, predicated brainstorming and discussion workshops among the appropriate stakeholders.

As the list of potential projects and activities is compiled, it important to maintain the links between the projects/activities, the current-state realities and the objectives, as outlined in the vision statement (see Table 1). Such an approach not only ensures focus during the planning activities, but also, by providing line of sight between objectives, realities and proposed actions, it supports effective executive communication during the approval stage.
### Table 1. Illustrative Linkage of Projects to Current State and Objectives

<table>
<thead>
<tr>
<th>Project/Action</th>
<th>Current State</th>
<th>Objective</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institute a Security Steering Committee</td>
<td>C3, C5</td>
<td>01</td>
<td>Implement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement a Content-Aware Data Loss Prevention Solution</td>
<td>C7</td>
<td>Pilot</td>
<td>Phase 1</td>
<td>Phase 2</td>
<td></td>
</tr>
<tr>
<td>Implement a Balanced Scorecard for Security</td>
<td>O7, O9</td>
<td>Pilot</td>
<td>Deploy</td>
<td>Refine</td>
<td></td>
</tr>
<tr>
<td>Etc.</td>
<td>Etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Gartner (January 2012)

Consider breaking longer-term projects and initiatives up into smaller projects. And anything beyond the simplest of projects should be staged into phases and milestones.

**Prioritization**

Few, if any, organizations will have the resources required to execute on all of the identified projects and activities; hence, these will have to be prioritized against the following criteria:

- The level of risk reduction potentially achieved by a given project/activity
- The resources (skills, staff and systems) required
- The financial cost
- The "time to value," that is, the period between the initial investment and the point at which the project will start accruing value to the organization

It is a good idea to have a mix of longer and shorter time-to-value projects within the strategic plan. This enables the security program to demonstrate meaningful progress on a quarterly time scale, making it easier to maintain long-term executive support for the security program.

**Approval**

The final step in the planning process is to obtain executive approval and budget. The strategy will typically be communicated using a written report and an executive presentation. The report and the presentation should clearly describe the current state, the desired state, and how the projects with their respective phases and milestones will help to achieve the desired state (see "Use a Structured Approach to Communicate Your Security Strategy").

It is also important to express how the proposed projects will contribute to business value. While this facet is implicitly included in the planning process through linking it to the business strategy, ensure your audience is aware of this by explicitly highlighting it in the executive communications material. "Articulating the Business Value of Information Security" provides one approach for achieving this.
Sponsorship, funding and budget allocation for the security program are key functions of the security governance function (see "Information Security and Risk Governance: Functions and Processes").

Reporting
A key part of maintaining support for the security program is effective and continuous reporting on the progress of the program. A balanced scorecard approach is imminently suitable for this purpose (see "Toolkit: Developing a Balanced Scorecard for Security").

In order to maintain the credibility of the security leadership team, it is important to keep this reporting as honest as possible. Be clear about:

- Which expected benefits were realized fully or partially
- Which expected benefits were not realized
- Which unexpected benefits materialized
- Which unexpected issues/disadvantages materialized
- On which projects the jury is still out

Progress should be reported on a quarterly basis. The reporting activity in itself will often highlight problems or changing circumstances that will necessitate changes or refinements in the overall strategy.

Gartner predicts that, by 2014, 70% (double 2011 levels) of IT risk and security officers in G2000 organizations will be required to report at least annually to the board of directors on the state of security (see "Eight Practical Tips to Link Risk and Security to Corporate Performance").

Some Common Pitfalls to Avoid

- Placing too much emphasis on generic benchmarking data (such as, security spending as a percentage of IT spending), rather than ensuring that the strategy maps to the unique cultural context and business needs of the organization. While benchmarking and survey data provide valuable guidance information, it is, by nature, averaged and generalized. Any given security program strategy should primarily be based on the business context of the enterprise (see "Two Simple Techniques to Facilitate Business Alignment").
- Executing the planning process as a unilateral exercise, giving little or no cognizance to other business or IT strategies. Other strategic planning initiatives (such as enterprise architecture) can provide meaningful context.
- Developing a vision that is too ambitious, impractical and unattainable from a technology or cultural perspective. While it is laudable to have aspirations within the strategy, all the objectives should be readily obtainable within the planning horizon.
Not being firm enough during the prioritization phase, resulting in too many high-priority projects being included in the short-term planning scope, with predictable results when it comes to progress reporting. The planned activities must be mapped to realistic resource availability.

Failing to segment large-scale initiatives into smaller, more-achievable projects, or into clearly delineated project phases. More-granular initiatives improve control and make it easier to deliver value in a shorter time frame.

Focusing too aggressively on your peers to the exclusion of other information sources. In many industries, poor security practices have flourished because the companies focused only on each other and not best practices. In some cases, like the pharmaceutical industry, this has led to immature programs at many companies that are in multiyear correction processes at the demand of their boards of directors.

Conclusions

Strategic planning for information security should be based on general planning principles, taking into account the unique requirements of the security discipline.

The plan, extending three to five years into the future, must map out intended activities that will take place across specific time frames, working toward the desired endpoint. It should be reassessed at least annually, if not more often, to make course corrections based on changing conditions, goals or success (or failure).

Strategic planning is not a perfect science — security leaders improve their planning capabilities through practice and experience.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Toolkit: Security Strategy Template"

"ITScore for Information Security"

"Toolkit: Board-Ready Slides for Cybersecurity and Technology Risk"

Evidence

1 This research is based on 38 client meetings and inquiry calls during 3Q11 and 4Q11 on the topic of strategic planning for information security. It includes at least nine client strategy document reviews and an on-site planning workshop with a major multinational bank.
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations, visit http://www.gartner.com/technology/about.jsp
MEMORANDUM

Date: January 29, 2013
To: Presidents
Provis Officers of Academic Affairs
From: Ephraim P. Smith
Executive Vice Chancellor and Chief Academic Officer
Subject: Accessible Technology Initiative

Background

The Americans with Disabilities Act of 1990 (ADA) and Section 504 of the Rehabilitation Act of 1973 (504) require that qualified individuals be provided equal access to programs, services, and activities. California Government Code 11135 applies Section 508 of the 1973 Rehabilitation Act, as amended in 1998, to State entities and to the California State University (CSU). Section 508 of the Rehabilitation Act was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities and to encourage development of technologies that will help achieve these goals.

The CSU policy statement on accessibility is articulated in Executive Order 926. Implementation of this policy is guided by the Accessible Technology Initiative (ATI) as established in Coded Memo AA-2006-41 and revised in the following coded memos: AA-2007-04, AA-2007-13, AA-2008-21, AA-2009-19, AA-2010-13, and AA-2011-21. This coded memo supersedes all previous coded memos.

Vision

All CSU programs, services, and activities should be accessible to all students, staff, faculty, and the general public. This encompasses all technology products used to deliver academic programs and services, student services, information technology services, and auxiliary programs and services.

The CSU’s Accessible Technology Initiative (ATI) implementation approach is driven by the following principles:

- Technology accessibility is an institution-wide responsibility that requires commitment and involvement from leadership across the enterprise.
- Technology access for individuals with disabilities must provide comparable functionality, affordability, and timeliness and should be delivered in a seamless manner as possible.
- The implementation of Universal Design principles should reduce the need for, and costs associated with, individual accommodations for inaccessible technology products.

Key Strategies

The CSU Accessible Technology Initiative targets the elimination of accessibility barriers across the university. The CSU is using a "Capabilities maturity" strategy to achieve its vision for accessibility. This strategy focuses campus and system efforts on continuously improving and institutionalizing its business and academic programs that will reliably, sustainably, and successfully deliver accessible educational, administrative, and community services for all. The implementation of the ATI is based on the following key components:

- Establish strong administrative/executive support. The CSU codified its commitment to technology accessibility in Executive Order 926. Pursuant to EO 926, campus presidents are charged with establishing a campus committee and overseeing campus ATI activities.
- Ensure continuous quality improvement. Some ATI goals require investments and changes to business procedures that will require time to deploy to our large, diverse CSU community. Just as accessibility barriers often develop over a period of years, remediation activities will sometimes require years to fully implement. During this extended remediation period, the CSU should work to achieve incremental improvements in barrier removal each year.
- Prioritize projects/activities. The ATI covers a broad range of technology accessibility goals involving technology products in use across all university programs and services. Given that there are finite resources (e.g. staffing, time, and tools) available each year to work on these goals, campuses should select ATI implementation activities that target accessibility barriers with the greatest impact.
- Identify specific Goals/Success Indicators. In order to ensure that meaningful progress is made over time, the CSU has collectively established specific ATI goals and success indicators. The broad ATI goals are articulated in the ‘Goals’ subsection below. The Success Indicators are published and available on the ATI website.
- Document progress. It is critical that the CSU document the substantive steps that have been taken over time to remove technology accessibility barriers. This approach (1) establishes a credible institutional commitment to equal access for persons with disabilities and facilitates reporting during campus audits. The CSU ATI implementation therefore utilizes annual campus reports to document progress (discussed further in the ‘Annual Reports’ subsection below).
- Drive vendor improvements to product accessibility support. The CSU seeks to improve product accessibility through partnerships and by leveraging the procurement process.

Implementation Goals

Campuses are required to accomplish the ATI goals listed below. Each ATI goal is supported by a set of success indicators that describe the processes, procedures, and activities that need to be accomplished in order to meet the goal. As changes in technology occur, the success indicators may be modified following consultation with campus executive leadership.

Web Accessibility Goals

- Web Accessibility Evaluation Process: Identify and repair or replace inaccessible websites, web applications, and digital content.

https://www.calsstate.edu/acadaff/codedmemos/AA-2013-03.html
**New Website/Web Application and Digital Content Design and Development Process:** New website/web application and digital content development complies with all Section 508 accessibility guidelines.

**Ongoing Monitoring Process:** Updating and maintenance of websites/web applications and digital content comply with Section 508 Accessibility Standards.

**Exemptions and Alternatives Process:** Documented non-compliant websites, web applications and digital content must be delivered in an equally effective alternate format and granted an exemption.

**Training Process:** Professional development training has incorporated Section 508 accessibility guidelines into website and web applications development and digital content preparation.

**Communication Process:** The campus community is aware of Section 508 guidelines to make web based information available to everyone (students, staff, faculty & the general public) regardless of disability.

**Administrative Process:** Campus governance entities are aware of and kept informed about web accessibility.

### Procurement Accessibility Goals

- **Procurement Procedures:** An ATI Electronic and Information Technology (E&IT) Procurement Plan, documents, forms, and other materials to support 508 procurements at the campus are created and published.
- **Staffing or Role Definition:** ATI procurement team is fully staffed with clearly defined roles for processing E&IT procurements.
- **Exemption Process:** A well-documented process has been established and is used for exemptions to E&IT procurements.
- **Equally Effective Access Plans:** Equally Effective Access Plans are created for E&IT products that are not fully 508 compliant.
- **Training:** All parties involved in E&IT procurement have been trained, and a continual training program is in place.
- **Outreach (Communications):** All individuals on campus involved in the purchasing of goods are knowledgeable about Section 508 in the context of E&IT procurement.
- **Evaluation & Monitoring:** Campus has established a continual evaluation process with standard forms and procedures. Feedback from the process along with direction is provided to training, outreach, and other groups involved in E&IT procurements.
- **Experience/Implementation:** Campuses have sufficient experience and expertise in completing E&IT procurements.

### Instructional Materials Accessibility Goals

- **Timely Adoption:** The campus has implemented a comprehensive plan to ensure the timely adoption of textbooks and other instructional materials.
- **Identification of Instructional Materials for Late-Hire Faculty:** The campus has implemented a comprehensive plan to ensure that textbooks have been identified for courses with late-hire faculty.
- **Early Identification of Students with Disabilities:** The campus has implemented a comprehensive plan to ensure that students with disabilities are identified and able to request alternate media materials in a timely manner.
- **Facility Use of Learning Management Systems (or non-Learning Management System) Course Websites:** The campus has implemented policies and procedures to promote the posting of all required curricular and instructional resources (including print-based and multimedia materials) in a central, accessible electronic location.
- **Accessibility Requirements for Multimedia:** The campus has implemented policies and procedures to ensure that accessibility requirements have been incorporated into the adoption process for all multimedia-based instructional resources.
- **Accessibility Requirements for Curricular Review and Approval:** The campus has implemented policies and procedures to ensure that accessibility requirements have been incorporated into the curricular review process.
- **Supporting Faculty Creation of Accessible Instructional Materials:** The campus has implemented policies and procedures to support faculty in selecting, authoring, and delivering accessible instructional materials.
- **Communication Process and Training Plan:** The campus has implemented a broad-based ATI awareness campaign, supported by a comprehensive training infrastructure to increase technological accessibility across the campus.
- **Process Indicators:** Campus Instructional Materials Accessibility Plan (IMAP) committee has sufficient breadth, resources, and authority to effectively implement a comprehensive IMAP initiative.

### Implementation Approach

The ATI recognizes that each CSU campus faces unique challenges with implementing the ATI. The implementation approach outlined below was therefore developed in collaboration with the Executive Sponsors Steering Committee (ESSC), the ATI Leadership Council and the ATI Priority Area Communities of Practice to ensure that campuses have adequate flexibility to manage their ATI implementation.

Each year, the CSU will make progress toward accomplishing the ATI goals by using a combination of systemwide and campus-based activities. Campuses will assess their capacity, select specific success indicators to work on, engage in a variety of projects and activities that address these success indicators, and report on their progress in the ATI Annual Reports. In addition, the ATI, in consultation with campus leaders, will select success indicators to work on collaboratively at the systemwide level.

### Chancellor’s Office ATI Responsibilities

The ATI department is part of systemwide Academic Technology Services (ATS) within the Academic Affairs division. ATS will continue supporting the ATI by providing staffing and resources. The ATI is committed to helping campuses accomplish the ATI goals by engaging in the following activities:

- Supporting campus ATI planning and implementation efforts by: developing guidance, providing training resources, sharing significant accomplishments and exemplary practices, and researching promising tools and techniques.
- Coordinating systemwide ATI activities that reduce costs, leverage CSU resources, and increase capacity.
- Collaborating with campus leadership through the ATI Leadership Council and Executive Sponsors Steering Committee to implement systemwide accessible technology policy, projects, and planning.
- Maintaining effective ongoing communication with key stakeholder groups and consulting with systemwide affinity groups.
- Coordinating the annual report process including analyzing ATI Annual Reports and distributing systemwide aggregated report results.
- Providing systemwide support to drive improvements to product accessibility support by vendors and publishers.

### Campus ATI Responsibilities

https://www.calstate.edu/acadaff/codedmemos/AA-2013-03.html
The ATI Steering Committee on each campus and at the Chancellor's Office will oversee the ATI implementation including reviewing and revising the ATI Campus Plan, implementing project and activities to meet ATI goals, and documenting progress toward these goals using the ATI Annual Report process. Each of these responsibilities is described in more detail below.

**Participation by Key Stakeholder Groups on Campus**

- **Campus Administration including Presidents, Provosts, CIO's, Vice-Presidents:** Provide regular communication and ensure adequate resources in support of the ATI campus implementation.
- **Academic and Faculty Senates:** The Senate Chair or their designee is strongly encouraged to serve on the campus ATI Steering Committee and participate in ATI instructional materials activities. The Senate at large is strongly encouraged to pass and facilitate the implementation of policies or resolutions that support the adoption of accessible technology.
- **Centers for Faculty Development:** Participate in relevant campus ATI committees and systemwide activities; Coordinate or actively participate in providing faculty training on ATI-related subjects.
- **Disability Services Offices:** Participate in the campus ATI Steering Committee; Participate in the development of Equally Effective Alternate Access Plans.
- **ADA Compliance Office:** Participate in the campus ATI Steering Committee; actively support the campus ATI implementation.

**Reviewing/Revising the ATI Campus Plan**

Each year, the campus Executive Sponsor, working with the campus ATI Steering Committee, will review and update the ATI Campus Plan to guide their implementation. The Plan will indicate the specific success indicators on which the campus will focus its efforts across the 3 priority areas. Campuses may adopt the ATI Campus Plan Template provided by the ATI or develop their own plan format. The Campus Plan Template is available on the ATI website.

When developing the Plan, campuses should consider the following information:

- Current campus progress as described in the Annual Report with particular attention to success indicators with a status level of Not Started or Initiated.
- Select ATI implementation activities across all 3 priority areas that will result in the greatest reduction of technology accessibility barriers.
- Use the ATI Prioritization Framework or a comparable campus process to consider factors such as impact, probability, and campus capacity when prioritizing ATI implementation activities.
- Deliverables associated with systemwide ATI activities that would advance campus progress if adopted.
- Campus collaborations that may accelerate or improve the quality of ATI activities.

**Implementing the ATI Campus Plan**

Ensuring the accessibility of information technology and resources is a shared responsibility of the entire campus and requires a coordinated, ongoing effort to ensure its success. Campus executive sponsors should lead the implementation effort on their campus through the following activities:

- Conduct regular ATI Steering Committee meetings no less than twice per year.
- Ensure that the Committee membership is comprised of all key stakeholder groups and includes members with appropriate experience and expertise to inform decision-making.
- Engage in a periodic administrative review process with the Committee regarding challenges, milestones, resources, and documenting ongoing progress.
- Monitor, leverage, and implement deliverables from systemwide ATI activities that will advance campus efforts.
- Ensure that Committee members monitor, participate in, and contribute to Community of Practice activities.
- Channel communications from the Chancellor’s Office to appropriate parties on campus.

**Documenting Progress Using the Annual ATI Report**

Campuses will submit an ATI Annual Report to the Chancellor’s Office each year which details campus progress towards accomplishing the ATI Goals. The Chancellor’s Office ATI department will provide the framework and methodology for submitting ATI annual reports to campuses.

When completing the Annual Report each year, campuses will:

- Affirm that the campus has reviewed and revised its ATI Campus Plan.
- Report on the status of all goals and success indicators since campus progress may result from systemwide and campus-level activities.
- Document the campus commitment to work on specific success indicators.

**Implementation Timeline**

The timeline associated with ATI implementation tasks is provided below.

- **July-October:** Review/revise the ATI Campus Plan.
- **November:** Submit the ATI Campus Annual Report and affirm that the ATI Campus Plan has been reviewed and revised.
- **April:** Review the systemwide aggregate reports that describe progress across the system.

The Chancellor’s Office ATI department will support the implementation timeline through the following activities:

- **July:** Distribute the Campus Annual Report.
- **December-March:** Review the Campus Annual Report submissions and prepare systemwide aggregate reports.
- **April:** Distribute the systemwide aggregate reports that describe progress across the system.
California State University, Chico

Information Security Plan

Version 6.0
April 05, 2018
<table>
<thead>
<tr>
<th>Table of Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Scope</td>
<td>3</td>
</tr>
<tr>
<td>Information Security Organization</td>
<td>4</td>
</tr>
<tr>
<td>Roles and Responsibilities</td>
<td>4</td>
</tr>
<tr>
<td>Policy and Standards Management</td>
<td>7</td>
</tr>
<tr>
<td>Risk Management</td>
<td>8</td>
</tr>
<tr>
<td>Incident Response</td>
<td>9</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>10</td>
</tr>
<tr>
<td>Evaluation and Revision of the Information Security Plan</td>
<td>10</td>
</tr>
<tr>
<td>Appendix A - Definitions</td>
<td>11</td>
</tr>
<tr>
<td>Appendix B - Additional Roles and Responsibilities</td>
<td>12</td>
</tr>
<tr>
<td>Appendix C - References</td>
<td>15</td>
</tr>
</tbody>
</table>
Introduction

Information security is essential to the mission of the University and is a campus-wide responsibility. CSU, Chico recognizes the need for a comprehensive information security plan which outlines a risk-based layered approach to the implementation of security controls.

The purpose of the Information Security Plan is to:

- Assign development and management responsibilities for information security
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held (e.g. paper, electronic, oral, etc.)
- Develop risk management strategies to identify and mitigate threats and vulnerabilities to information assets
- Establish and maintain an incident response plan
- Maintain ongoing security awareness and training programs
- Comply with applicable laws, regulations, and CSU policies

Scope

CSU, Chico is responsible for protecting the confidentiality, integrity and availability of University information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the integrity of the mission of CSU, Chico, violate individual privacy rights, and possibly constitute a criminal act. It is the collective responsibility of all users to ensure:

- Confidentiality of personally identifiable information
- Integrity of data stored on or processed by CSU, Chico information systems
- Availability of information stored on or processed by CSU, Chico information systems
- Security of CSU, Chico information systems
- Compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection

This plan for the protection of systems and information applies to the following:

- All campus departments, including auxiliary units, and external business or organizations that provide goods or services to CSU, Chico
- Central and departmentally-managed information assets
- All students, faculty, staff, and consultants employed by CSU, Chico or any other person having access to CSU, Chico information assets
- All categories of information, regardless of the medium in which the information asset is held (e.g. paper, electronic, oral, etc)
- Information technology facilities, software, and equipment (including personal computer systems) owned or leased by CSU, Chico.
Information Security Organization

Information security is an increasingly complex legal and technical challenge requiring an enterprise-wide management organization. At CSU, Chico, the management structure for information security is illustrated below.

Information Security Roles and Responsibilities

Roles and Responsibilities

The responsibilities of the Chief Information Security Officer, Information Security Officer, Student Records Data Custodians and CSIRT are detailed below. Additional roles and responsibilities related to information security are outlined in Appendix B.

Chief Information Security Officer

At CSU, Chico, the Vice Provost of Information Resources and Chief Information Officer (CIO) is responsible for establishing and coordinating the campus-wide information security strategy and is designated the Chief Information Security Officer (CIO). The CIO is responsible for the development, maintenance, and yearly review of the Information Security Plan in collaboration with units under the supervision of the following administrators:

- Provost and VP, Academic Affairs
- VP, Business and Finance
- VP, Student Affairs
- VP, University Advancement
- Deans
- Information Security Officer
- All record management custodians
- All managers and employees of computing units
- Others affected by security management and response
Information Security Plan

Information Security Officer

The Information Security Officer (ISO) reports to the CIO and is responsible for assuring information security efforts across campus are coordinated and reduce overall risk. The ISO is also responsible for security planning, analysis, policies, standards and incident handling, as well as establishing and maintaining a framework to assure that information security strategies are aligned with University objectives and consistent with applicable laws and regulations. This individual’s responsibilities include but are not limited to:

- Providing oversight of confidential information in the custody of the University
- Providing oversight of security of the equipment or repository where the information is processed and/or maintained
- Promoting and encouraging campus standards, best practices and procedures
- Evaluating the effectiveness of the current safeguards for controlling these risks
- Developing and providing oversight of plans and procedures to preserve confidential information in the event of natural or man-made disasters

Data Owners Information Security Group

Data Owners are responsible for records retention schedule series custodian responsibilities as defined in CSU EO 1031 and data governance responsibilities as defined by the CSU Information Security Policy, ICSUAM 8000. In their governance role, data owners are responsible for classifying, defining controls, authorizing access, monitoring compliance with CSU/campus security policies and standards, and identifying the level of acceptable risk for the information assets assigned to them. A data owner is usually a member of management in charge of a specific business unit and is ultimately responsible for the protection and use of information within that unit. The group is composed of key managers from all four vice presidential areas as follows:

<table>
<thead>
<tr>
<th>Schedule Series</th>
<th>Record Schedule Series Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Personnel/Payroll</td>
<td>AVP for Staff Human Resources</td>
</tr>
<tr>
<td>2.0 Fiscal</td>
<td>AVP of Financial Services</td>
</tr>
<tr>
<td>3.0 Environmental Health &amp; Safety</td>
<td>Director, Environmental Health &amp; Safety</td>
</tr>
<tr>
<td>4.0 Student Records</td>
<td>University Registrar</td>
</tr>
<tr>
<td>5.0 Facilities</td>
<td>Director, Facilities Management and Services</td>
</tr>
<tr>
<td>6.0 University Police</td>
<td>Chief of Police</td>
</tr>
<tr>
<td>7.0 University Advancement</td>
<td>Director of Advancement Services and Annual Fund</td>
</tr>
<tr>
<td>8.0 Academic Personnel</td>
<td>Associate Vice President for Faculty Affairs</td>
</tr>
<tr>
<td>9.0 Curriculum &amp; Accreditation</td>
<td>AVP for Academic Programs</td>
</tr>
<tr>
<td>10.0 Grants &amp; Sponsored Programs</td>
<td>Vice Provost for Research</td>
</tr>
<tr>
<td>11.0 Institutional Records</td>
<td>Chief of Staff</td>
</tr>
</tbody>
</table>
Computer Security Incident Response Team (CSIRT)

The Computer Security Incident Response Team assesses, responds, and resolves information security incidents in partnership with campus technical staff, University Police, Dispute Resolution, Public Affairs, etc. Their tasks include but are not limited to:

- Notifying appropriate units of possible security infringements
- Reporting any security breach as outlined in the Plan
- Disseminating guidelines related to security to departmental data managers

Members include:

- Brooke Banks, Chief of Staff and Executive Assistant to the President
- John Feeney, Chief of Police
- Mike Thorpe, Risk Manager
- Sheryl Woodward, AVP, Staff Human Resources
- Joe Wills, Director of Public Affairs and Publications
- Mark Hendricks, Information Security Officer

Information Security Roles and Responsibilities

![Diagram of Information Security Roles and Responsibilities]

May 2014
Policy and Standards Management

The CSU Responsible Use Policy as well as Executive Memorandum 97-18, Policy on the Use of Computing and Communications Technology (Revised Policy for Faculty EM 07-01) outline user responsibilities and acceptable use of computing and communications systems, services, and facilities, and serves as the foundation for the campus information security program. To complement the policy, CSU, Chico continues to develop a body of information security standards, guidelines and procedures for the protection of the business infrastructure and environment, the computing infrastructure and environment, and confidential information in its custody.

All CSU, Chico standards, procedures and guidelines are vetted according to the Documentation Review and Approval Procedure.

CSU and CSU, Chico Policies, Standards, and Procedures

CSU policies and standards are published in the Integrated CSU Administrative Manual (ICSUAM). ICSUAM login page: https://esyou.calstate.edu/Policies/ICSUAM/Pages/default.aspx

All CSU policies and standards, as well as campus supplemental policies, standards, and procedures are published on the Information Security web page: http://www.csuchico.edu/isee/policies_standards/index.shtml
Risk Management
Risks to information assets must be actively managed in order to prioritize resources and remediation efforts. Risk management involves the identification and evaluation of risks to information security assets (risk assessment) and the development of strategies to reduce the risk to acceptable levels (risk mitigation).

CSU, Chico has developed a series of risk management processes that identify and assess risks to its information assets and reduce such risks to acceptable levels.

Risk Assessment
Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of security controls. The Information Security Office works with data authorities and system owners to conduct periodic risk assessments of campus information assets. The results of the risk assessment are documented.

Risk Mitigation
Risk mitigation involves prioritizing, evaluating, and implementing appropriate risk-reducing activities recommended as a result of the risk assessment process. Since the elimination of all risk is impossible, campus leadership balances the cost and effectiveness of the proposed risk-reducing activities against the risk being addressed. Controls selected to mitigate risks include administrative, operational, technical, physical, and environmental measures as appropriate.

Mitigation strategies ensure the confidentiality, integrity, and availability of information assets and are commensurate with risks identified by risk assessments. For those risks where the risk mitigation strategy involves the use of controls, these controls must ensure that risks are reduced to an acceptable level, taking into account:
- Legal and regulatory requirements and compliance
- University operation and policy requirements and constraints
- Cost of implementation, maintenance, and operation

Reporting Information Security Risks
The ISO completes a risk assessment of all critical and protected assets at least every two years. The risk assessment report includes a description of the methodology used to conduct the risk assessment, the results of the risk assessment, and the campus mitigation strategies for addressing each identified risk.
Incident Response

CSU, Chico has a documented incident response plan that includes processes for investigating, responding to, reporting, and recovering from incidents involving loss, damage, misuse of information assets, or improper dissemination of critical or protected information, regardless of the medium in which the breached information is held (e.g. paper, electronic, oral).

All suspected security incidents must be reported to the Information Security Officer. In the event of a security incident, the following actions may be taken:

- Blocking access to the affected computing system
- Notifying the appropriate Data Authorities, Administrator/College Dean, or Department Chair
- Assessing the nature of the breach, including a description of the incident, the response process, the notification process, and the actions taken to prevent further breaches of security
- Consulting with University Counsel as appropriate

The University is required to disclose any breach of system security to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In determining the need for notification, the Incident Handling Team will follow the guidelines established by the California Office of Privacy Protection. The notification process is subject to the University policy on official communications (EM 05-05).

Records Retention and Disposition

CSU Executive Order 1031 establishes records retention and disposition schedules and requirements for the CSU. The campus has implemented EO 1031 through the CSU, Chico Records Retention Plan. The CSU, Chico Records Retention Plan identifies roles and responsibilities for records retention and a schedule for annual certification of records by schedule series custodians. Schedule Series custodians are also referred to as data owners. The data owner is the campus-designated department head who maintains the official/original copy of the record/information series for retention purposes in compliance with EO 1031 Records Retention Policy. Some records fall out of the direct management of the data owner, administrators of these records are known as records custodians. Formal delegation of specific responsibilities to records custodians should be documented.

Data Owner/Schedule Series Custodian Responsibilities

- Completing the Annual Records Retention Certification for assigned records/information schedule series
- Ensuring that Records Retention responsibilities for records custodians are established and communicated to all records custodians for the assigned schedule series.
- Ensuring that Records Custodians are aware of their responsibilities to ensure that records retention and disposition activities are conducted in compliance with the CSU Records Retention Policy and schedules.
- Ensuring that records custodians are aware that records retention and disposition procedures must be developed and documented.
Security Awareness and Training

The University community needs to understand and support the information security objectives of availability, confidentiality and integrity, and the tradeoffs that may be necessary for effective control of risks. Security awareness programs are meant to promote CSU, Chico strategies for protecting information assets. Web-based security awareness training, updated yearly, is provided for all staff, faculty and student employees. In addition, the information security program and the Policy on Computing and Communications Technology (EM 97-18 & EM 07-01) are introduced at all new hire orientation sessions. The Chancellor’s Office has made available to all campuses training through CSU Skillport. This e-learning includes security awareness training which all employees will be required to take.

When appropriate, information security training is provided to individuals whose job functions require specialized skill or knowledge in information security. While the heads of relevant offices are ultimately responsible for ensuring compliance with information security practices, the Information Security Office will assist in the development of training and education programs for all employees who have access to confidential data. Federal, State, and University policies concerning confidential information are provided for review before access to protected/confidential information is allowed.

The information security program provides and coordinates training for individuals whose job functions require special knowledge of security threats, vulnerabilities, and safeguards. This training is focused on expanding knowledge, skills, and abilities for technical individuals responsible for securing systems and information.

Evaluation and Revision of the Information Security Plan

The Information Security Plan will be evaluated and adjusted to reflect changing circumstances, including changes in the University’s business practices, operations or arrangements, or as a result of testing and monitoring the safeguards.
Appendix A - Definitions

Access means a personal inspection, review, or communication of protected information. This includes records or data which are oral, written, or electronic.

Attacks are actions taken by an entity that exploit certain vulnerabilities.

Availability is a property that assures that the system has the capacity to meet service needs. It includes timeliness and usability. The property of availability protects against threats of denial of service.

Centralized computer systems means those computer hardware and software systems housed in and maintained in the data center by Information Resources.

Controls are mechanisms or procedures that mitigate threats. Among the goals of security controls are to ensure confidentiality, integrity, availability or privacy of information and systems.

Confidentiality is a property that assures information and systems are accessible only by authorized parties or entities. The property of confidentiality protects a system from the threat of disclosure. A disclosure threat is the possibility that data will be accessed by unauthorized entities.

Non-centralized computer systems means those computer hardware and software systems managed or housed in departments other than Information Resources or by individual employees.

Confidential Information means any information not exempted in specific legislation and identified as personal or confidential, such as personally-identifiable information, individually-identifiable health information, education records, and non-public information, as specified in federal or state law or CSU or CSU, Chico policy. Additional details regarding protected/confidential data can be found in the Data Classification and Protection Standard.

Data Authorities are the authorities of record of all protected data pertaining to individuals in their area including student, faculty and staff confidential data.

Disclosure means to permit access to or to release, transfer, disseminate, or otherwise communicate all or any part of confidential information by any means, orally, in writing, or electronic to any unauthorized person.

Handle means the access, collection, distribution, process, protection, storage, use, transmittal, or disposal of protected information.

Integrity is a property that assures that unauthorized changes in data cannot occur or can be detected if they do occur. The property of integrity protects against threats of modification and fabrication.

Privacy is a subset of confidentiality. It concerns information about an entity and assures that this information is not made public or accessible by unauthorized persons.

Threats are potential occurrences, malicious or otherwise, that can have undesirable effects on assets or resources associated with computer systems.

Vulnerabilities are characteristics of computer systems that make it possible for a threat to potentially occur. They are not necessarily weaknesses in a system and may be otherwise desirable qualities of a system.
Appendix B - Additional Roles and Responsibilities

Data Managers

These individuals include the Vice Provost for Human Resources, the Associate Vice President for Business and Finance, the Director of Financial Aid, the Vice Provost for Enrollment Management, and the University Registrar. Within their areas their responsibilities include but are not limited to:

- Implementing and administering the Plan in order to protect the privacy rights of faculty, staff, and students and to comply with legal and policy requirements
- Protecting confidentiality and security of electronic and paper information
- Defining business functions and staff authorized to access confidential information and approve authorization
- Ensuring that all employees receive employee/student confidentiality training as directed by the Vice Provost for Human Resources and the University Registrar
- Developing and implementing appropriate campus-wide mechanisms to ensure that all employees attend and comply with the required training
- Providing appropriate confidentiality training for employees with authorized access to confidential information as designated by the Vice Provost for Human Resources and/or the University Registrar
- Developing, implementing, and communicating the expectations and means for the safeguarding of confidential information to appropriate persons and organizations
- Ensuring that risk assessments are conducted when necessary
- Maintaining appropriate and timely documentation for employees with access to confidential data
- Reporting on the status of the Plan to the Information Security Officer (ISO)
- Providing recommendations for revisions to this Plan as appropriate

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Location</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeopleSoft Computerized Student Record (SIS+ legacy data converted to P/S fall 2005)</td>
<td>CMS Centralized Server Utah</td>
<td>University Registrar</td>
</tr>
<tr>
<td>Student Academic Permanent Record (paper-based source of the official student academic transcript)</td>
<td>Scanned images of paper records maintained on ENR server using ImageNow software. Paper files stored in Student Records and Registration Office, SSC (now called Office of the Registrar)</td>
<td>University Registrar</td>
</tr>
<tr>
<td>Student Advising, Graduation/Evaluation &amp; Academic Standing Records</td>
<td>Academic Advising Program</td>
<td>Director of Academic Advising Programs</td>
</tr>
<tr>
<td>Student Financial Aid Date</td>
<td>Student Financial Aid Office, SSC Scanned images of support documents stored on a server in Computing Services Butte Hall</td>
<td>Director of Financial Aid</td>
</tr>
<tr>
<td>Student Housing File</td>
<td>Student Housing Office</td>
<td>Director of Housing</td>
</tr>
<tr>
<td>Record Type</td>
<td>Location</td>
<td>Custodian</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Student Disciplinary and Conduct Records</td>
<td>Student Judicial Affairs Office</td>
<td>Coordinator of Judicial Affairs</td>
</tr>
<tr>
<td>Student Health Records</td>
<td>Student Health Center</td>
<td>Director of Student Health Services</td>
</tr>
<tr>
<td>Student Undergraduate Applicant Record</td>
<td>Office of Admissions</td>
<td>Director of Admissions</td>
</tr>
<tr>
<td>Student Graduate Applicant and Graduate Degree Records</td>
<td>Office of Graduate, International and Sponsored Programs (Graduate Studies)</td>
<td>Dean, School of Graduate, International and Sponsored Programs (Graduate Studies)</td>
</tr>
<tr>
<td>Student Counseling Files</td>
<td>Psychological Counseling and Wellness Center</td>
<td>Director of Psychological Counseling and Wellness Center</td>
</tr>
<tr>
<td>Student Learning Center Records</td>
<td>Student Learning Center</td>
<td>Associate Director for Disability Support Services</td>
</tr>
<tr>
<td>Student Testing Files</td>
<td>Office of Testing and Research</td>
<td>Director of Testing and Research</td>
</tr>
<tr>
<td>Student Career Placement Files</td>
<td>Career Planning and Placement Office</td>
<td>Director of Career Planning and Placement (now Career Center)</td>
</tr>
<tr>
<td>Student Employment Office</td>
<td>Student Employment Office</td>
<td>Director of Student Employment</td>
</tr>
<tr>
<td>Student-Athlete Eligibility/Advising Records</td>
<td>Compliance Office, Student Records and Registration Office</td>
<td>University Registrar</td>
</tr>
<tr>
<td>Student Billing and Financial Records</td>
<td>Data is stored in Cash Net Server and on SIS+, Kendall Hall and SIS+ Computer Services 4th floor Butte Hall</td>
<td>Director of Student Financial Services</td>
</tr>
<tr>
<td>Student Disability Records</td>
<td>Disability Support Services, (now Accessibility Resource Center)</td>
<td>Coordinator of Disability Support Services</td>
</tr>
<tr>
<td>University Advancement and Alumni Records</td>
<td>University Development and Advancement - Banner Database</td>
<td>VP for University Advancement</td>
</tr>
<tr>
<td>Veterans Records</td>
<td>Veterans Affairs, Student Records and Registration Office</td>
<td>University Registrar</td>
</tr>
<tr>
<td>Teacher Education Credentializing Records</td>
<td>Credential Specialist, Academic Advising Program</td>
<td>Director of Academic Advising Programs</td>
</tr>
<tr>
<td>College and Department Advising Records</td>
<td>College and Department Office</td>
<td>College deans and department chairs</td>
</tr>
<tr>
<td>Continuing Education Student Database</td>
<td>Office of Regional and Continuing Education</td>
<td>Dean of Regional and Continuing Education</td>
</tr>
</tbody>
</table>
Administrators/College Deans/CAD Tech Reps

These individuals, including managers of campus auxiliary organizations, shall be responsible for oversight of employees authorized to handle confidential information in their areas of supervision. Their responsibilities include but are not limited to:

- Ensuring that the management and control of risks outlined in the Plan are adhered to by employees in their unit
- Granting permission to their employees to the appropriate level of access to confidential data
- Providing their employees with resources and methods to secure equipment and/or data repositories where confidential information is processed, stored, or handled

System Owners

These individuals are ultimately responsible for providing the system’s service/functionality to the campus. Often the system owner is a manager/director, department chair, or dean. Their responsibilities include but are not limited to;

- Make strategic decisions
- Approve security/risk management strategy
- Ultimately responsible for all system problems or security compromises

CSIRT

These individuals respond to serious incidents, perform top level review of campus information security policies, standards, guidelines and procedures. The committee is also responsible for periodic reporting by the ISO on significant incidents and overall institutional risks and vulnerabilities.
Appendix C - References

The CSU, Chico Information Security Plan complies with federal and state regulations and California State University policy specified in documents at the following links:

Federal and State Regulations

- Health Care Portability and Accountability Act of 1996 (HIPAA) [http://www.ihs.gov/Adminmngrresources/HIPAA/index.cfm](http://www.ihs.gov/Adminmngrresources/HIPAA/index.cfm)
- California Education Code, Section 89546, *Employee Access to Information Pertaining to Themselves* [http://www.loginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8499863841+0+0+0+0&WASaction=retrieve](http://www.loginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8499863841+0+0+0+0&WASaction=retrieve)
- California Penal Code, Section 502, *Comprehensive Computer Data Access and Fraud Act* [http://www.loginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8500924547+1+0+0+0&WASaction=retrieve](http://www.loginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8500924547+1+0+0+0&WASaction=retrieve)

California State University Policies and Procedures

CSU Records Retention & Disposition Schedules, [http://www.calstate.edu/recordsretention/](http://www.calstate.edu/recordsretention/)


**CSU, Chico Policies and Procedures**


- *Revised Policy on Use of Computing and Communications Technology for Faculty (EM 07-01), January 2007* [http://www.csuchico.edu/prs/EMs/EM07/em07_01.shtml](http://www.csuchico.edu/prs/EMs/EM07/em07_01.shtml)

- *CSU, Chico Student Privacy Rights and Student Records Administration Policies and Procedures Document (EM 06-34), June 2006* [http://www.csuchico.edu/prs/EMs/EM06/em06_34.htm](http://www.csuchico.edu/prs/EMs/EM06/em06_34.htm)

- *Shared Network Resource Password Policy (EM 01-04), February 2001* [http://www.csuchico.edu/prs/EMs/EM01/em01_04.htm](http://www.csuchico.edu/prs/EMs/EM01/em01_04.htm)


- *Policy for Official Communication via Electronic Mail (Interim) (EM 05-02), February 2005* [http://www.csuchico.edu/prs/EMs/EM05/em05_02.htm](http://www.csuchico.edu/prs/EMs/EM05/em05_02.htm)
California State University, Chico

Information Security
Incident Management Plan

Version 0.8
September 12, 2016
Introduction

Effective information security management involves a combination of prevention, detection, and reaction. In addition to deploying strong security protection, the university should be able to respond to incidents and invoke proper procedures if an information security incident occurs. Security event and incident management is vital to the information security management process.

The purpose of this document is to outline the procedures for management an information security event or incident. Such events or incidents may take the form of a virus, worm or Trojan attack, a denial of service (DoS) or other intrusion, or misuse of information resources by an individual, machine, or site.

Scope

These procedures and guidelines are for management, administration, and other technical and operational staff to prepare for, detect, and respond to information security incidents. Because security events and incidents involving different computer systems will lead to different consequences, departments should customize the security event and incident management procedures according to their specific needs.

Objectives

A well defined security event and incident management plan is vital to the effective operation of a computer system, in addition to the information security operation as a whole. The major objectives of security event and incident management include

- Ensure the required resources are available, including manpower, technology, etc.
- Ensure that all the responsible parties have a clear understanding of the tasks they should perform following predefined procedures
- Ensure that the response is systematic and efficient and that there is prompt recovery for the compromised system
- Ensure that the response activities are coordinated
- Minimize the possible impact of information leakage, corruption, and system disruption, etc.
- Share experience in incident response within and among departments
- Prevent further attacks and damages
- Coordinate related legal issues with the CO
Incident Management Procedures

All information security incident management procedures are located in the Information Security Knowledge Base on the wiki at https://wiki.csuchico.edu/confluence/display/i sec/Home.

Security Incident Response

The Security Incident Response Procedure defines the steps to be followed when an incident occurs. The procedure aims at minimizing damage, eradicating the cause of the incident, and restoring the system to normal operation etc., in accordance with predefined goals and priorities. The procedure is broadly categorized into five stages: identification, containment, eradication, recovery and follow-up.

Although the procedure is written generally with intrusions in mind, it is meant to serve as a guideline and as such the same basic steps apply to other types of incidents.

A system administrator or system manager may establish additional security incident response procedures, checklists, and best practices to guide teams. These procedures should be provided to all employees including management personnel for their reference and compliance. They should be clear, straightforward, and easily understood so all personnel understand what they need to do.

Notification

The Security Incident Notification Procedure defines the process to notify management and relevant parties of the incident to ensure that important decisions are promptly made. It sets out the points of contact (both internal and external) at various levels for notification based on the type and severity of the incident.

Notification procedures and contact lists may vary for different kinds of incidents and for different systems regarding contact points and follow-up actions.

Information about incidents should be disclosed only on a need-to-know basis, and only the Information Security Officer has the authority to share or authorize others to share information about security incidents with others not directly involved.

Reporting and Tracking

The Security Incident Reporting and Tracking Procedure defines the means of reporting and tracking suspicious activities so all parties involved are notified in a timely manner and all required information is documented. In addition, the procedure deals with how all parties involved will know to whom they should report, and in what way, and what they should not report.

A Post-incident Report is also prepared to maintain consistency and ensure completeness of the information collected during security incident reporting.

To facilitate an effective reporting and tracking procedure all involved staff should be familiar with the reporting procedure and capable of reporting security incidents quickly. In addition, a security incident reporting form should be created to standardize the information to be collected, and if necessary, draw up a separate procedure for non-office-hour reporting.
Roles and Responsibilities

Information Security Office
The Information Security Office (ISEC) is responsible for working with the campus community to secure systems and network resources, and protect the confidentiality of student, faculty and staff information. Related to incident management the Information Security Office is responsible to:

- Consult with campus users and departments to investigate security issues.
- Ensure incident response procedures are developed, implemented and followed
- Respond to and recover from disruptive and destructive information security events

Incident Management Team (IMT)
The Incident Management Team is responsible for implementation of the Incident Management Plan, including the facilitation of all incident management procedures (security incident response, notification and reporting and tracking). Their tasks include but are not limited to:

- Assessing, responding, and resolving information security incidents in partnership with campus technical staff, University Police, Public Affairs, etc.
- Notifying appropriate units of possible security infringements
- Reporting any security breach
- Disseminating guidelines related to security to departmental data managers and system administrators

System Administrators and Department/System Managers
All campus system administrators and department/system managers are responsible for following the incident management procedures outlined in the plan. A system administrator or department manager may establish additional security incident response procedures, checklists, and best practices, as well as system/department-specific contact lists.

Training and Implementation
Management, administration, and technical and operational staff need to have a thorough understanding of these procedures in order to work together to effectively respond to information security incidents. The Incident Management Team conduct a variety of training sessions to review and discuss the procedures so all parties are prepared in the event an incident occurs.

Once the detailed Security Incident Response procedure has been covered in training, it is not expected that technical and operational staff will refer to it at each stage during an incident. A checklist will also be available to speed response and ensure steps are not missed.

Department-and computer system-specific incident management procedures may not be covered in these training sessions yet need to be understood by appropriate staff.
Appendix A – Definitions

The term ‘incident’ refers to an adverse event in an information system and/or network, or the threat of such occurrence. Examples of incidents include unauthorized use of another user’s account, unauthorized use of system privileges, and execution of malicious code that destroys data. Incident implies harm or the attempt to harm.

An ‘event’ is any observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash, and packet flooding within a network. These observable events recorded on Incident Management Forms, along with the evidence collected, provide the bulk of your organization’s case if the perpetrator of an incident is caught and prosecuted.

The term ‘security incident’ refers to any incident related to information security. It refers to an adverse event in an information system and/or network which pose a threat to computer or network security in respect of availability, integrity, and confidentiality. Examples of security incidents include malicious code attacks, unauthorized access, unauthorized utilization of services, denial of resources, disruption of services, compromise of protected data/program/network system privileges, malicious destruction or modification of data/information, penetration and intrusion, misuse of system resources, viruses and hoaxes, and malformed codes or scripts affecting networked systems.
## Appendix B – Incident Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious code attacks</td>
<td>Malicious code attacks include attacks by programs such as viruses, Trojans, and worms used by hackers to gain privileges, capture passwords, and/or modify audit logs.</td>
</tr>
<tr>
<td>Denial of service (DoS)</td>
<td>Hackers and malicious code can disrupt/deny network and computing services in many ways, including erasing a critical program, “mail spamming” (flooding a user account or mail system), and altering system functionality by installing a Trojan.</td>
</tr>
<tr>
<td>Unauthorized access or utilization of services/hacks</td>
<td>Unauthorized access ranges from improperly logging into a user's account to unauthorized access to data stored on a system. Unauthorized access could also entail access to network data by installing a “sniffer” program or device to capture all packets traversing the network at a particular point. Examples of unauthorized utilization of services include using the network file system (NFS) to mount the file system of a remote server machine, the VMS file access listener to transfer files without authorization, or inter-domain access mechanisms in Windows NT to access files and directories in another organization's domain.</td>
</tr>
<tr>
<td>Misuse</td>
<td>Misuse occurs when someone uses a computing system for purposes prohibited by the Policy on the Use of Computing and Communications Services (EM 97-18).</td>
</tr>
<tr>
<td>Threats</td>
<td>Threats express the intention to inflict harm or indicate impending danger or harm. They are often received via e-mail, but could also be communicated via other electronic means.</td>
</tr>
</tbody>
</table>
Information Security Policies and Standards

CSU Systemwide Information Security Policies (http://www.calstate.edu/icsuam/sections/8000/) are published through the integrated California State University Administrative Manual (ICSUAM).

The table below is intended to provide links to campus and system wide policies, standards and other related documentation.

<table>
<thead>
<tr>
<th>Section</th>
<th>Policy Topic</th>
<th>Supplemental Policies</th>
<th>Standards</th>
<th>Procedures &amp; Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>7100.0</td>
<td>Identity and Access Management</td>
<td>![policy-7100.shtml]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8000.0</td>
<td>Introduction and Scope</td>
<td>![policy-8000.shtml]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8005.0</td>
<td>Policy Management</td>
<td>![policy-8005.shtml]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8010.0</td>
<td>Establishing an Information Security Program</td>
<td>![policy-8010.shtml]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8015.0</td>
<td>Organizing Information Security</td>
<td>![policy-8015.shtml]</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>8020.0</td>
<td>Information Security Risk Management</td>
<td>![policy-8020.shtml]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8025.0</td>
<td>Privacy of Personal Information</td>
<td>![policy-8025.shtml]</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>8030.0</td>
<td>Personnel Information Security</td>
<td>![policy-8030.shtml]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8035.0</td>
<td>Information Security Awareness and Training</td>
<td>![policy-8035.shtml]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8040.0</td>
<td>Managing Third Parties</td>
<td>![policy-8040.shtml]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8045.0</td>
<td>Information Technology Security</td>
<td>![policy-8045.shtml]</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Information Security and Identity Management (./index.shtml)

https://www.csuchico.edu/isec/policies/index.shtml
<table>
<thead>
<tr>
<th>Code</th>
<th>Policy Title</th>
<th>Valid</th>
<th>Active</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>8050.0</td>
<td>Configuration Management (policy-8050.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8055.0</td>
<td>Change Control (policy-8055.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8060.0</td>
<td>Access Control (policy-8060.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8065.0</td>
<td>Information Asset Management (policy-8065.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8070.0</td>
<td>Information Systems Acquisition, Development and Maintenance (policy-8070.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8075.0</td>
<td>Information Security Incident Management (policy-8075.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8080.0</td>
<td>Physical Security (policy-8080.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8085.0</td>
<td>Business Continuity and Disaster Recovery (policy-8085.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8090.0</td>
<td>Compliance (policy-8090.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8095.0</td>
<td>Policy Enforcement (policy-8095.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8100.0</td>
<td>Electronic and Digital Signatures (policy-8100.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8105.0</td>
<td>Responsible Use Policy (policy-8105.shtml)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### Plans and Reports
- Information Security Plan (PDF) [://assets/documents/information-security-plan-2016.pdf](#)
- State & Federal Information Security Laws & Regulations (policy-info.shtml)

### Applicable CSU Policies for Storage of Level I Data

Complete CSU Information Security Policy Documents [://www.calstate.edu/icsuam/sections/8000/](#)

---

**Information Resources**

Meriam Library, Room 338  
[www.csuchico.edu/ires](https://www.csuchico.edu/ires/)

Support Our College  
[https://www.csuchico.edu/giving/index.shtml](#)

**More in our division**

- Computing & Communication Services  
  [https://www.csuchico.edu/ccs](#)
- Creative Media & Technology  
  [https://www.csuchico.edu/cmt](#)
- Enterprise Applications & Data Services  
  [https://www.csuchico.edu/eads](#)
- Information Security  
  [https://www.csuchico.edu/isec](#)

---

[https://www.csuchico.edu/isec/policies/index.shtml](#)