



California State University, Chico

Information Security Plan

Version 5.1
May 4, 2009



REVISION CONTROL

Document Title: Information Security Plan

Author: William E. Post, CISO, CIO

Date	By	Action	Pages
5/20/2004	Brooke Banks, Linda Post , Phyllis Weddington	Created Plan	All
6/14/2004	Linda Post	Edits	4,5,6,7,8, appendixes
11/3/2004	Brooke Banks	Removed references to Electronic Security Team	5
2/15/2005	Linda Post	Added link to interim E-mail policy	15
4/24/2009	Brooke Banks	Major revision	All
5/4/2009	Brooke Banks	Updated members of the CISC	6

Review/Approval History

Date	By	Action	Pages
6/15/2004	Provost Scott McNall	Reviewed	All
6/15/2004	Campus Information Security Committee	Reviewed	All
6/16/2004	B2000	Reviewed	All
6/25/2004	CIO	Approved	All
6/29/2004	CIO	Cabinet Notification	All
9/02/2004	President Zingg	Final Approval	All
4/27/2009	Cabinet	Reviewed	All
5/6/2009	Cabinet	Approved	All



Table of Contents

Introduction	4
Scope.....	4
Information Security Organization	5
Roles and Responsibilities.....	5
Policy and Standards Management.....	7
Risk Management.....	8
Incident Response	9
Security Awareness and Training.....	9
Evaluation and Revision of the Information Security Plan.....	10
Appendix A - Definitions.....	11
Appendix B - Additional Roles and Responsibilities.....	12
Appendix C - References.....	13



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

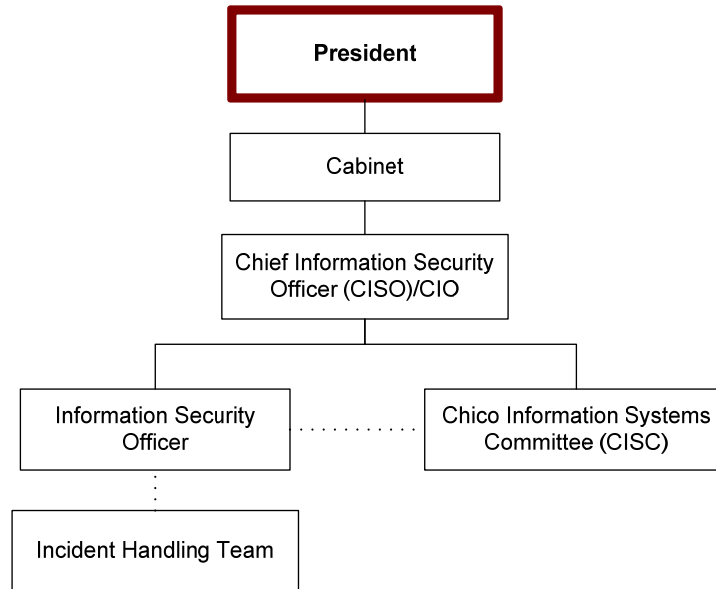
This plan for the protection of systems and information applies to the following:

- 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.



Roles and Responsibilities

The responsibilities of the Chief Information Security Officer, Information Security Officer, Chico Information Systems Committee and Incident Handling Team 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 (CISO). The CISO 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 Officer

The Information Security Officer (ISO) reports to the CISO 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

Chico Information Systems Committee (CISC)

The CISC's purpose is to coordinate implementation of enterprise technology projects. The committee reviews all new enterprise technology projects to assure they are effective and secure. The committee also reviews and discusses current security challenges and new security standards and guidelines. The CISC is composed of key managers from all four vice presidential areas as follows:

- Director of CMS (Chair)
- Vice Provost for Information Resources and CIO
- Senior Vice Provost
- Vice Provost of Enrollment Management
- Director of Payroll and Benefits (interim)
- Assistant Vice President of Financial Services
- Associate Vice President for Student Affairs
- Senior Associate Vice President for University Advancement
- Vice Provost for Faculty Affairs

Incident Handling Team (IHT)

The Incident Handling 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



Policy and Standards Management

Executive Memorandum 97-18, Policy on the Use of Computing and Communications Technology (Revised Policy for Faculty EM 07-01) outlines 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.

Status of Current Policy and Standards Initiatives

The California State University system is developing information security policies and standards that the campus will implement upon their completion and approval. The following CSU, Chico standards, procedures and guidelines are available on the information security website.

Functional Standards

- Data Classification and Protection Standards
- Credit Card Security Handling Standards
- Credit Card Security Self-Assessment Questionnaire

Technical Standards

- Account Management Standards
- Application Code Development Standards
- Password Management Standards
- Remote Access Standards
- Server Security Baseline Standards
- Vulnerability Management Baseline Standards

Procedures

- Security Authority and Responsibility Procedure
- Documentation Review and Approval Procedure
- Privileged Accounts Procedure
- Reporting Lost or Stolen Computers Procedure
- Electronic Device Disposal Procedure
- Wildcard Certificate Requests and Handling Procedure

The following are some additional topics that will soon be addressed

- Physical Security
- 3rd Party Service Providers
- Legal Review Requirements
- E-discovery



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).

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.

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 Authorities

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

Administrators/College Deans

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



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

- Gramm-Leach-Bliley Act of 1999: Federal Trade Commission Regulations. The Act includes two regulations: *The Financial Privacy Rule* and *The Safeguards Rule*.
<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>
- Health Care Portability and Accountability Act of 1996 (HIPAA)
<http://www.ihs.gov/Adminmngrrsources/HIPAA/index.cfm>
- Family Education and Privacy Act of 1974 (FERPA),
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- California Information Practices Act of 1977
http://www.oispp.ca.gov/consumer_privacy/laws/code/ipa.asp
- California Code of Regulations, Title V, Sections 42396 through 42396.5
<http://ccr.oal.ca.gov/linkedslice/default.asp?SP=CCR-1000&Action=Welcome>
- California Education Code, Section 89546, *Employee Access to Information Pertaining to Themselves* <http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8499863841+0+0+0&WAIAction=retrieve>
- California Penal Code, Section 502, *Comprehensive Computer Data Access and Fraud Act*
<http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8500924547+1+0+0&WAIAction=retrieve>

California State University Policies and Procedures

- CSU Coded Memo: HR 2003-05, March 13, 2003, *Requirements for Protecting Confidential Employee Data: Updated to Reflect Confidentiality Agreement Requirement*,
<http://www.calstate.edu/HRAAdm/Policies/HR2003-05.pdf>
- CSU HR/PR 93-01 and Supplement #1, *Requirements for Protecting Confidential Employee Data*, <http://www.calstate.edu/HRAAdm/pdf2002/HR2002-27.pdf>
- CSU HR 2003-14, *HIPAA Regulations – Privacy Compliance*, July 15, 2003,
<http://www.calstate.edu/HRAAdm/pdf2003/HR2003-14.pdf>
- CSU *Information Security Policy*, August 2002,
http://its.calstate.edu/systemwide_it_advisory/ITAC_keydocuments/IT_Security_Policy_092002.doc
- CSU *Records Access Manual*, February 2003,
http://www.calstate.edu/GC/Docs/Records_Access_Manual.doc
- CSU Executive Order No. 1031, *System wide Records/Information Retention and Disposition Schedules Implementation*, <http://www.calstate.edu/EO/EO-1031.html>



- CSU Records Retention & Disposition Schedules, <http://www.calstate.edu/recordsretention/>
- CSU Memo, *Information Security Clarification*, March 28, 2003

CSU, Chico Policies and Procedures

- *Policy on Use of Computing and Communications Technology (EM 97-18)*, June 1997
http://www.csuchico.edu/prs/EMs/EM97/em97_18.htm
- *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
- *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
- *Shared Network Resource Password Policy (EM 01-04)*, February 2001
http://www.csuchico.edu/prs/EMs/EM01/em01_04.htm
- Information Resources Policies, Procedures and Guidelines
<http://www.csuchico.edu/ires/policies/index.html>
- Information Security <http://www.csuchico.edu/ires/security/index.html>
- *Policy for Official Communication via Electronic Mail (Interim) (EM 05-02)*, February 2005
http://www.csuchico.edu/prs/EMs/EM05/em05_02.htm