Data Classification and Protection Standards

Effective Date: July 28, 2015

1.0 INTRODUCTION

This document provides an operational standard for the management of protected data/data elements. Data classification is the process of assigning value to data in order to organize it according to its risk to loss or harm from disclosure.

The California State University, Chico data classification and protection standards establish a baseline derived from federal laws, state laws, regulations, CSU Executive Orders, CSU ICSUAM and campus policies that govern the privacy and confidentiality of data.

The CSU, Chico data classification and protection standards apply to all data collected, generated, maintained, and entrusted to the CSU (e.g. student, research, financial, employee data, etc.) except where superseded by grant, contract, or federal copyright law. These standards apply to information in electronic or hard copy form.

Implements: CSU Policy ICSUAM 8065 Information Asset Management
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8065.0.shtml

2.0 CLASSIFICATION DESCRIPTION: LEVEL 1 - CONFIDENTAL

From CSU 8065.S02 Information Security Data Classification Standard

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:

- 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.
- 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.
- Limited use - Information intended solely for use within the CSU and limited to those with a "business need-to know."
- 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 includes, but is 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
- EMEDC records
- Prospective donor profiles
- Retention Tenure & Promotion Documents (RTP)

3.0 CLASSIFICATION DESCRIPTION: LEVEL 2 - INTERNAL USE

From CSU 8065.S02 Information Security Data Classification Standard

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:

- Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.
- 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 includes but is 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
- 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

- 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

- Mother's maiden name
- Race and ethnicity
- Parents' and other family members' names
- Birthplace (City, State, Country)
- Gender
- Marital Status
- Physical description
- Other

4.0 CLASSIFICATION DESCRIPTION: LEVEL 3 - GENERAL

From CSU 8065.S02 Information Security Data Classification Standard

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

Examples of Level 3 – General information includes but is not limited to:

Campus Identification Keys

- Chico State ID (EmplID)
- 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)

5.0 SECURITY CONTROLS

Implements CSU 8065.S001 Information Security Asset Management Standard

Appropriate technical and organizational controls must be put in place to prevent the unauthorized or unlawful processing or disclosure of data. Departments must ensure that the security controls in terms of physical security (e.g. control access to buildings or rooms, correctly handle and dispose of printed material containing personal data), administrative controls (e.g. restrict password, restrict access on the basis of role or authority), and technical controls (e.g. store personal data on a secure server, make use of privacy enhancing technologies) are appropriate for the data being processed and maintained.

- Data security controls must be implemented commensurate with data value, sensitivity, and risk. Data in each classification will require varying security measures appropriate to the degree in which the loss or corruption of the data would be harmful to individuals, impair the business or academic functions of the University, result in financial loss, or violate law, policy or CSU contracts.
- Security controls implemented will be dictated by the data classification level. Controls will include, but not be limited to, an appropriate combination of the following:
    - Physical Access Controls
    - Administrative Access Controls
    - Technical Access Controls

6.0 Handling Guidelines

Implements CSU 8065.S001 Information Security Asset Management Standard

- Protected Level 1 information should not be stored within shadow systems (e.g. files, home-grown databases, spreadsheets, documents, tables, etc.)
    - If there is a compelling reason to store this information within a shadow system, the system must be identified and appropriate controls must be in place commensurate with the primary source of the confidential information.
- Protected Level 1 information should not be sent, transmitted, or disseminated in an unsecured manner. The medium used to send, transmit, or disseminate protected level 1 information should be appropriately protected from modification or disclosure.

The table below describes how information should be handled according to its classification and as it relates to systems development. For example, if a report is printed and automatically distributed, labeling information and distribution standards would be required.

	Level 1	Level 2	Level 3
Labeling	"CSU, Chico, Level 1 - Confidential", must appear on the bottom of each page. Control statements which clarify a label must be added directly under the "Level 1 - Confidential" label on each page. "Level 1 - Confidential" must also appear on removable media labels.	"CSU, Chico, Level 2 -Internal Use" should appear on the bottom of each page and on removable media labels. Control statements which clarify a label, should be added directly under the "Level 2 - Internal Use" label on the first page; they may be added on each subsequent page as necessary.	No Labeling is required. Control Statements, which classify a label, may be added at the bottom of the first page or screen, or on removable media labels.

State Property: Computers, laptops, workstations, and servers	Level 1 data may not be stored on computers, laptops, workstations and servers unless authorized in writing by appropriate administrator and data owner. Systems and electronic storage devices used to store Level 1 Confidential information must meet minimum CSU Chico, desktop security standards.	Systems and electronic storage devices used to store Level 2 Internal Use information must meet minimum CSU Chico, desktop security standards.	No restrictions.
State Property: Computers, laptops, workstations, and servers	Level 1 data may not be stored on non-state owned computers, laptops, and servers.	Level 2 Internal Use data for students enrolled in the current semester may be stored on University and non-university owned computers during the current term only. At the end of the term It is recommended that Level 2 data stored on non-university owned computers be, removed to an appropriate, secure archive medium and location or encrypted.	No restrictions.
Mobile devices, smart phones, tablets	Protected Level 1 data may not be stored on a mobile device unless authorized in writing by appropriate administrator and Data Owner(s). Encrypted via campus-approved method.	Mobile devices, smart phones, and tablets should utilize screen locks and remote wipe support. Mobile devices that use cloud storage for content storage should is discouraged.	No restrictions.
Reproduction	Reproduction is discouraged, however, if done, must be done with permission from the owner.	Reproduction is authorized if not prohibited by the control statement.	No restrictions.
Distribution	Information distributed outside of CSU, Chico must have valid, current, and properly executed Non-Disclosure Agreement in place and approved by the data/information authority.	Distribution must be only to those who have a business need to know and are either CSU, Chico employees or someone who has signed a confidentiality statement.	May be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.
Public Cloud Storage (Dropbox, Google Drive, MS O365)	Storage of Level 1 data prohibited. Currently-available cloud storage solutions do not provide the level of protection required for Level 1 data. CSU, Chico recommends storing University data on Bay or in the system of record.	Storage of Level 2 data discouraged. Currently-available cloud storage solutions do not provide the level of protection required for Level 2 data. CSU, Chico recommends storing University data on Bay or in the system of record.	No restrictions.

Computer Printing	Remove printouts immediately if using a public printer or as appropriate for internal shared printers.	No restrictions.	No restrictions.
Mail (Hard Copies)	May be sent through interoffice or U.S. Mail but must be sealed in a plain envelope having no classification marking and clearly marked on the outside "To be Opened by Addressee Only."	May be sent through interoffice of U.S. Mail with no special handling. If being sent to another building, it must be placed in an interoffice envelope with no special marking.	No restrictions.
Electronic Mail (e-mail)	Must be encrypted with an approved CSU, Chico Information Security Office sanctioned encryption package or algorithm.	May be sent to other CSU, Chico employees and over a public network with appropriate authorization – Email is not secure and consideration of content should be considered.	No restrictions.
Data Transmission	Must be encrypted with an approved CSU, Chico Information Security Office sanctioned encryption package or algorithm.	May be sent to other CSU, Chico employees and over a public network with appropriate authorization.	No restrictions.
Fax	Authorized only from and to CSU, Chico controlled fax machines. Must be attended at each end. Level 1 information should not be sent to public fax machines.	May be sent to other CSU, Chico employees as long as the receiving and send fax are CSU, Chico controlled. Fax to a public location is not allowed.	No restrictions.
Telephone	Authorized, but only to CSU, Chico employees and or individuals covered by non-disclosure agreement. Phone message system must have password protection capability.	No restrictions, but conversations must be limited to other CSU, Chico employees or individuals covered by non-disclosure agreement.	No restrictions.
Visual Disclosure	Ensure that documents and screens are positioned to prevent inadvertent disclosure. Do not leave documents and screens unattended and unsecured in a location. Erase all white boards at the end of meetings.	Whenever possible, do not leave documents and screen unattended and unsecured in public locations.	No restrictions.

Removable Media (Flash Drives/External Hard Drives)	Level 1 data may only be stored on removable media and external hard drives if the entire media device is encrypted using campus approved encryption methods.	Files containing Level 2 data should be encrypted using campus supported encryption.	No restrictions.
Storage and Backup	Backups must be encrypted. Strongly recommended that paper or removable media be stored in a locked enclosure when not in use. Media should not be left unattended on a desk. Electronic storage requires access controls and file protection mechanisms. If these are not found in the operating system in use, then additional security packages are required. Backups require the same care as originals to maintain confidentiality.	When on CSU, Chico property, no special requirements. If transported outside, appropriate care must be taken to prevent disclosure or theft.	No restrictions.
Record Retention	Records of any type of medium, such as paper, microfiche, magnetic, or optical, must be retained as required by the campus record retention and disposal schedule for the record type.	Records of any type of medium, such as paper, microfiche, magnetic, or optical, must be retained as required by the campus record retention and disposal schedule for the record type.	Records of any type of medium, such as paper, microfiche, magnetic, or optical, must be retained as required by the campus record retention and disposal schedule for the record type.
Disposal	Hard copy requires a secure disposal container or shredder. Electronic storage media must be irretrievably erased or disposed of in a secure fashion.	Hard copy should use a secure disposal container or shredder. Normal deletion commands or utilities within operating systems are sufficient for files. Reformatting of media is also valid.	Normal waste disposal.
Inventory	Must be locked securely. All paper and electronic repositories must be identified. Security measures and access controls should be reassessed annually.	No requirements.	No requirements.

Access control	Employee must have signed a confidentiality statement before access is granted. Vendors must have an authorizing non-disclosure agreement and/or confidentiality agreement before access is granted. The appropriate data owner must approve all access to level 1 data.	Employee must have signed a confidentiality statement before access is granted. Vendors must have an authorizing non-disclosure agreement and/or confidentiality agreement before access is granted.	No specific requirements.
Reclassify or declassify	Campus data classification standards for level 1 data must meet or exceed CSU data classification standards published in section 8000 of the system-wide policy. The campus can elect to move information up to level 1, but never from level 1 to a classification level with lower protection requirements.	Only the data owner can reclassify or declassify.	No requirements.

7.0 REFERENCES AND LEGISLATIVE RESOURCES

Related Federal Laws and Regulations

- Gramm-Leach Bliley Act of 1999
- HIPAA – Health Information Portability and Accountability Act
- Family Education Rights and Privacy Act of 1974 (FERPA)
- Federal Trade Commission Regulations (16 CFR, Part 314) Standards for Safeguarding Customer Information; Final Rule, May 23, 2002
- Federal Trade Commission Regulations (16 CFG, Part 313) Privacy of Consumer Financial Information
- Payment Card Industry (PCI) Data Security Standard

Related CA State Laws and Regulations

- California Information Practices Act of 1977 (California Civil Code Section 1798.85)
- California Education Code, Section 89546, Employee Access to Information Pertaining to Themselves
- California Code of Regulations, Title 5, Sections 42396-42396.5
- Comprehensive Computer Data Access and Fraud Act (California Penal Code, Section 502)
- California: SB 1386: Disclosure of Security Breach of Confidential Information
- California: SB 2246: Customer Records: Act to add to Title 1.81, Part 4 of Division 3 of the Civil Code

Related CSU Policies

- CSU Executive Order 796 (req. compliance with FERPA)
- Records Access Manual: Office of General Counsel: The California State University, March 2005 (Records exempted from disclosure)
- Chancellor's Office Memorandum of March 26, 2003: Increased Security Measures for CMS
- California State University HR: 2005-07: New Legislation Regarding the Use of Social Security Numbers (CO)
- California State University HR: 2005-16: Requirements for Protecting Confidential Personal Data Information

8.0 DOCUMENTION REVIEW AND APPROVAL

Review/Approval History

Date	Audience	Action	Version
2/2/2009	System Security Meeting	Presented	v1.0
2/27/2009	CIO	Reviewed	v1.0
2/27/2009	CIO	Approved	v1.0
3/2/2009	Cabinet	Reviewed	v1.0
4/27/2009	Cabinet	Approved	v1.0
5/11/2015	Policies and Standards Group	Reviewed / Recommended	v2.0
7/21/2015	Information Technology Executive Committee (ITEC)	Approved	v2.0