

Data Classification and Protection Standard

**California State University, Sacramento
Data Classification and Protection Standard**

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, Sacramento data classification standard establishes a baseline derived from Federal laws, state laws, regulations, CSU Executive Orders, and campus policies that govern the privacy and confidentiality of data. The CSU, Sacramento data classification standard applies to all data collected, generated, maintained, and entrusted to the CSU (e.g. student, research, financial, employee data) except where superseded by grant, contract, or federal copyright law. This data classification standard applies to information in electronic or hard copy form.

Protected data classification levels

California State University, Sacramento has identified three classification levels that are referred to as level 1, level 2, and level 3 data. Although all the enumerated data values require some level of protection, particular data values are considered more sensitive and correspondingly tighter controls are required for these values. The most critical level of sensitivity begins with Level 1. Levels 1 and level 2 are considered protected levels.

Classification	Description	Examples
Level 1 Confidential	This information can cause the most serious harm to individuals and to the campus as a result of unauthorized access. Much of this information is protected by statutes, regulation, other legal obligation or mandate. The CSU has identified specific guidelines regarding the disclosure of much of this information to parties outside of the university and controls are needed to protect the unauthorized access, modification, transmission, storage, or other use.	<ul style="list-style-type: none"> • 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 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 the campus or a system
Level 2 Business Use	This information must be guarded due to proprietary, ethical or privacy considerations. Campus guidelines will indicate the controls needed to protect the unauthorized access, modification, transmission, storage or other use.	<p>Identity validation keys</p> <ul style="list-style-type: none"> • Birth date (full: mm-dd-yy) • Birth date (partial: mm-dd only) • Mother’s maiden name <p>Student information</p> <ul style="list-style-type: none"> • Educational records (Excludes directory information) <ul style="list-style-type: none"> o Grades o Courses taken o Schedule o Test Scores o Advising records o Educational services received o Disciplinary actions <p>Non-directory student information may not be released except under certain prescribed conditions</p>

Classification	Description	Examples
		<p>Employee Information</p> <ul style="list-style-type: none"> • Employee net salary • Employment history • Home address • Personal telephone numbers • Personal email address • Parents and other family members names • Payment History • Employee evaluations • 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 <p>Other</p> <ul style="list-style-type: none"> • Legal investigations conducted by the University • Sealed bids • Trade secrets or intellectual property such as research activities • Location of assets • Linking a person with the specific subject about which the library user has requested information or materials.
<p>Level 3 Public</p>	<p>This information is regarded as publicly available. These data values are either explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both on- and off- campus (e.g., an employee’s work e-mail addresses), or not specifically classified elsewhere in the protected data classification standard. Publicly available data may still subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.</p>	<p>Campus Identification Keys</p> <ul style="list-style-type: none"> • Sacramento 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) <p>Student Information</p> <ul style="list-style-type: none"> • Educational directory information (FERPA) <p>Employee Information</p> <ul style="list-style-type: none"> • 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)

Security Measures

Appropriate technical and organizational measures must be put in place to prevent the unauthorized or unlawful processing or disclosure of data. Departments must ensure that the security measures 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 measures 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 measures implemented for data will be dictated by the data classification level. Measures will include, but not be limited to, an appropriate combination of the following:
 - Physical Access Control
 - Administrative Access Control
 - Technical Access Control

Handling Guidelines

- Protected Level 1 information should not be stored within shadow systems (e.g. files, home-grown databases, spreadsheets, documents, and tables)
 - If there is a compelling reason to store this information within a shadow system, the system needs to be identified and appropriate controls need to 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.
- Procedures regarding the archival and destruction of, at a minimum, Level 1 data should be implemented.

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.

Data Disposal

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 on complete pass across the entire media.
- Campus back-up (i.e., tape, optical) media must be physically destroyed or degaussed.

Disposing of any and all confidential data should have a disposal log. 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

Appendix A: 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 CFR, 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