

California State University, Fresno Data Classification Policy

Introduction

California State University, Fresno owned information (data) must be protected in accordance with legal, regulatory, contractual and administrative requirements. Data in their many forms are one of the University's most important assets. This policy describes the proper management, use and protection of university data.

Scope

Each employee, student, volunteer, agent, contractor or affiliate of the University with access to or who handles university data is a steward of that data and responsible for the proper handling of such information.

Data Classification

The overall sensitivity of institutional data encompasses its confidentiality, privacy, integrity and availability. Data with the highest risk needs the greatest amount of protection; data at lower risk can be given appropriate levels of protection. This approach allows the university to apply appropriate levels of resources to the protection of the institutional data based upon requirements.

Three categories (Confidential, Restricted, Unrestricted) of classification have been defined to maintain appropriate protection of university data. Confidential is the highest category (requires the highest level of protection); Unrestricted is the lowest category defined.

For each classification, several data handling requirements are defined in the “*Data Handling Standard*”, to appropriately safeguard the information. This standard also identifies how a combination of lower category data can lead to a higher classification category.

Category I: (Confidential Data):

Category I data is highly sensitive and may have personal privacy considerations or may be restricted by federal or state law and regulations¹. In addition, the negative impact on the university should this data be incorrect, improperly disclosed, or not available when needed is typically very high.

¹ California Civil Code 1798-1798.78 places specific requirements on State agencies in the collection, use, maintenance and dissemination of information relating to individuals; California Code of Regulations, Title 5, Education, Sections 42396-42396.5 identifies principles of personal information management that shall be implemented within The California State University System (CSU). Other examples include the Health Insurance Portability and Accountability Act (HIPPA), Sarbanes-Oxley and Gramm-Leach-Bliley.

Category I institutional data must be controlled from creation to destruction, and access will be granted only to those persons affiliated with the university who require such access in order to perform their job, or to those individuals permitted by law. Access to confidential data must be individually requested and then authorized by the Information Owner who is responsible for the data.

Category II: (Restricted Data):

University data not otherwise identified as Category-I data, but which is releasable (e.g., contents of specific e-mail, date of birth, salary, etc.) must be appropriately protected to ensure a controlled and lawful release.

University records (data) releasable under public access to government records laws² is categorized as restricted data and authorized for release by the designated university custodian of records.

Restricted data is moderately sensitive in nature. The risk for negative impact on the institution should this information not be available when needed is typically moderate.

Category II institutional data access must be requested from and authorized by, the Information Owner who is responsible for the restricted data. Access to restricted data may be authorized to groups of persons by their job classification or responsibilities, and may also be limited by one's employing unit or affiliation.

Category III: (Unrestricted Data)

University data not otherwise identified as Category-I or Category-II data is generally regarded as publicly available data. Such Category III institutional data is defined as public information and published with no restrictions.

Publicly available data is information that can be used, analyzed and obtained without requesting permission from the information owner.

Data Protection

All institutional data possessed by or used by a particular organization unit within the university must have a designated Information Owner. Information Owners do not legally own the information entrusted to their care. They are instead designated members of university management who act as stewards, and who supervise the ways in which certain types of information are used and protected.

Information Owners, assisted by Information Security, will assess risks and threats to data for which they are responsible, and accordingly classify and oversee appropriate protection of institutional data.

² California Public Records Act, Federal Freedom of Information Act

Information owners must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law, regulations, and with university policies and procedures.

Information owners must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.

Institutional data must be protected from unauthorized modification, destruction or disclosure. Permission to access institutional data, as needed, will be granted to all eligible university employees for legitimate university purposes.

Authorization for access to Category I (Confidential) and Category II (Restricted) institutional data comes from the Information Owner, and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other authority.

Where access to Category I and Category II institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was granted.

University employees must report instances in which institutional data is at risk of unauthorized modification, disclosure or destruction.

Users must respect the confidentiality and privacy of individuals whose confidential or restricted records (data) they access, observe restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Compliance

This policy exists in addition to all other university policies and federal and state regulations governing the protection of the university's data. Compliance with this policy will ensure that uniform safeguards are applied to protect university data, reducing the risk of disclosure, unauthorized modification and unavailability.