

California State University, Fresno
Data Handling Standard (Revision M)

(Approved by Information Security Committee on 01/25/2010)

1. Introduction

The level of control of institutional data depends on its classification and the level of risk associated with loss or compromise of the information. Information (data) can exist in many forms. It can be printed or written on a piece of paper, stored electronically, transmitted by post or by electronic means, shown on films, or spoken in conversation¹. Whatever form the information takes, or means by which it shared, stored or transmitted, it should always be appropriately protected.

Three classification categories (Confidential, Restricted, Unrestricted) have been defined to maintain appropriate protection of institutional data. The standard facilitates the identification, management and access requirements to promote stewardship of university data.

All institutional data possessed by or used by a particular organizational unit within the university must have a designated Information (Data) Owner. Information (Data) Owners are designated members of university management who act as stewards of the data.

2. Information (Data) Owner

Executive Order 1031 provides for the implementation of California State University (CSU) Systemwide Records/Information Retention and Disposition Schedules. A record or information means a recording upon any tangible thing in any form of communication or representation, including letters, words, pictures, sounds, or symbols, any combination of these or other means to engage in business, regardless of media².

The executive order also requires that each campus, for retention and disposition, designate official campus custodian(s) for each type of record. "Custodian of Record" is the term for the campus-designated department head that maintains the official/original copy of the records/information at Fresno State.

The "Custodian of Record" identified from the records and retention schedule posted at <http://www.csufresno.edu/adminserv/records> is the designated Information (Data) Owner for each respective type of data.

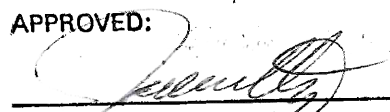
If a "Custodian of Record" is not identified for an area in the records and retention schedule, then the highest-ranking management personnel (MPP) of that respective area shall be designated as the Information (Data) Owner.

The Information (Data) Owner is responsible for providing proper protection of information and coordinating the implementation of this standard for a functional area of the University.

¹ ISO/IEC 27002:2005, page viii

² <http://www.calstate.edu/eo/EO-1031.html>

APPROVED:



JOHN D. WELTY
PRESIDENT

DATE 2/24/10

3. Examples

An Information Owner can use the following criteria to determine which data classification is appropriate for the respective institutional data or information system. A positive response to the highest category in any row is sufficient to place that data or system into that classification.

	CATEGORY I (Confidential Data)
Legal Requirements	Required by law, regulations, Executive Order or other obligations.
Reputation Risk	High
Other Institutional Risks	Information that provides access to critical resources, physical or virtual.
Examples (List is not All-inclusive)	<ul style="list-style-type: none"> • California State Law “notice triggering information” (Formerly SB1386/AB1298 data) <ul style="list-style-type: none"> ○ Individual’s first name or first initial and last name in combination with one or more of the following: <ul style="list-style-type: none"> ▪ Social security number, ▪ Or driver's license number, ▪ Or California identification number, ▪ Or financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account • Medical information (HIPPA) ¹ • Health insurance information • Student records (FERPA) ² • Personally Identifiable Information (PII) ³ • Credit card data ⁴ • Criminal investigations • Information specifically designated as confidential

¹ Health Insurance Portability and Accountability Act (HIPPA) provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

⁴ Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student educational records.

⁵ Personally Identifiable Information (PII)—information that can be used to locate or identify an individual, such as names, date of birth, aliases, Social Security numbers, drivers license number, biometric records, and other personal information that is linked or linkable to an individual. No single law governs all uses of personally identifiable information.

⁶ This includes credit card data regulated by the Payment Card Industry (PCI).

	CATEGORY II (Restricted Data)
Legal Requirements	Administrative, contractual or other obligations.
Reputation Risk	Medium
Other Institutional Risks	Smaller subsets of protected data.
Examples (List is not All-inclusive)	<ul style="list-style-type: none"> • Information resources <ul style="list-style-type: none"> ○ Electronic signatures ○ Location of assets ○ Private keys (digital certificates) • Donor information • Non-confidential research activities • Telephone billing • Sealed bids • Non-directory employee information

	CATEGORY III (Unrestricted Data)
Legal Requirements	Protection of data is at the discretion of the Information Owner.
Reputation Risk	Low
Other Institutional Risks	General university information.
Examples (List is not All-inclusive)	<ul style="list-style-type: none"> • Campus maps • Directory information

4. Requirements

Each organizational unit handling university data shall develop, maintain and execute a data protection plan describing how the respective area manages the handling, access and protection of university data. An annual review of data classification is required. Every plan to safeguard university data shall include the following components from the protection matrix.

A) Data in any form (paper, electronic, digital, etc.) (Minimum handling procedures)

ACTION	CATEGORY I (Confidential)	CATEGORY II (Restricted)	CATEGORY III (Unrestricted)
Data Access	University employees, auxiliaries, and those with university business requirements that have authorization and signed confidentiality agreements. Access must be noted in the position description of university and auxiliary employees.	University employees, auxiliaries and those with university business requirements that have authorization. Access should be noted in the position description of university and auxiliary employees.	University affiliates, auxiliaries and the public.
Data Disposal	All data, computer systems, electronic devices and digital media must be properly, permanently, irreversibly removed, cleaned or destroyed beyond the ability to recover the information.	All data in any form (paper, electronic, etc.), computer systems, electronic devices and digital media must be properly, permanently, irreversibly removed, cleaned or destroyed beyond the ability to recover the information.	No special requirements.
Data Retention	The designated custodian of records will adhere to the retention and disposal schedules located at http://www.csufresno.edu/adminserv/records .	The designated custodian of records will adhere to the retention and disposal schedules located at http://www.csufresno.edu/adminserv/records .	No special requirements.
Data Viewing (including duplication)	Read/view access is restricted using various access control methods and is based on roles, classifications, entitlements, or affiliations defined by respective Information Owner or their designee.	Read access is restricted using various access control methods and is based on roles, classifications, entitlements, or affiliations defined by respective Information Owner or their designee.	No special requirements.

B) Paper Records (Minimum handling procedures)

ACTION	CATEGORY I (Confidential)	CATEGORY II (Restricted)	CATEGORY III (Unrestricted)
Labeling documents	Category I documents must be labeled as “Confidential” regardless of internal or external use. Documents approved for distribution should be labeled accordingly.	Category II documents must be labeled as “Restricted” regardless of internal or external use. Documents approved for distribution should be labeled accordingly.	No special requirements.
Duplicating documents	Receiver of document containing Category I information must not further distribute without permission of respective Information Owner or designee.	Duplication of documents is at the discretion of the Information Owner or designee.	No special requirements.
Mailing documents via campus mail	The outer envelope is labeled as “Confidential”. Handling procedures include using an envelope inside a second envelope, stamping "Confidential" on the inner and outer envelope.	The outer envelope is labeled as “Restricted”. No other special requirements.	No special requirements.
Mail delivery via campus mail	Documents are kept in a secure environment upon delivery and distributed to the addressed individual.	No special requirements.	No special requirements.
Mailing documents via external mail carriers	No classification marking on external envelope required; Confirmation of receipt is required as legally or contractually mandated.	No special requirement, unless contractually obligated.	No special requirements.
Storing of documents	Stored in a locked drawer or in a locked room or in another approved secure location and must be out of sight at all times not in use.	Stored in a secure environment (locked office) and out of sight when not in use.	No special requirements.

C) Data Storage (Minimum handling procedures)

ACTION	CATEGORY I (Confidential)	CATEGORY II (Restricted)	CATEGORY III (Unrestricted)
Storing data on university servers	Policy on Minimum Security Baseline For Connected Devices at http://www.csufresno.edu/its/policies and the protective measures in appendix A.	Policy on Minimum Security Baseline For Connected Devices at http://www.csufresno.edu/its/policies and the protective measures in appendix A.	Policy on Minimum Security Baseline For Connected Devices at http://www.csufresno.edu/its/policies .
Storing data on university end user computer systems	If Category I data must be stored, it must be encrypted. Original Category I data not active and on retention schedules must be stored on university servers.	If Category II data must be stored, it must be encrypted. Original Category II data not active and on retention schedules must be stored on university servers.	No special requirements.
Storing data on university removable media or portable devices	Category I data must be encrypted when stored on such media or devices. Such media or devices must be stored in a secured location when not in use.	It is recommended that Category II be encrypted when stored on such media or devices. Such media or devices must be stored in secured location when not in use.	No special requirements.
Storing data on non-university electronic media	Category I data must be encrypted and included in department confidentiality plans. Devices must comply with Policy on Minimum Security Baseline For Connected Devices at http://www.csufresno.edu/its/policies .	Category II data must be encrypted and included in department confidentiality plans. Devices must comply with Policy on Minimum Security Baseline For Connected Devices at http://www.csufresno.edu/its/policies .	No special requirements.
Granting permission to create or modify data	Create / Modify access is restricted using various access control methods and is based on roles, classifications, entitlements, or affiliations defined by respective Information Owner or their designee.	Create / Modify access is restricted using various access control methods and is based on roles, classifications, entitlements, or affiliations defined by respective Information Owner or their designee.	No special requirements.
Granting permission to delete data	Deletions are restricted using various access control methods and are based on roles, classifications, entitlements, or affiliations defined by respective Information Owner or their designee. Also, adhere to records management requirements for deleting data.	Deletions are restricted using various access control methods and are based on roles, classifications, entitlements, or affiliations defined by respective Information Owner or their designee.	No special requirements.
Preventing data disclosure to unauthorized requestors	Do not disclose any information. Consider what is being requested and who is requesting it. Refer suitable requests to the Information Owner and questionable requests to Information Security Office.	If the requestor's credentials or authenticity cannot be completely assured, do not disclose any information. Refer suitable requests to the Information Owner and questionable requests to Information Security Office.	No special requirements.

Preventing unauthorized viewing or eavesdropping of data	Prevent data access or viewing on unattended electronic media (computers, flash drives, etc.). Implement procedures and measures to protect the privacy of Category I data while working with such information.	Prevent data access or viewing on unattended electronic media (computers, flash drives, etc.). Implement procedures and measures to protect the privacy of Category II data while working with such information.	No special requirements.
Printing hard copy report of data	Unattended printing to public printers is not allowed. Unattended printing to department printers requires a cover page and must be picked up as soon as possible. All printing is subject to the paper labeling requirements in section B.	Unattended printing to public printers is not allowed. Unattended printing to department printers must be picked up as soon as possible. All printing is subject to the paper labeling requirements in section B.	No special requirements.
Logon Banner /Application Alert	All computer systems that are capable must display a banner concerning the confidentiality and appropriate use of Category I data.	All computer systems that are capable must display a banner concerning the confidentiality and appropriate use of Category II data.	No special requirements.
Auditing access activity	Log all logon attempts and access of Category I data as defined by policy or business requirements. Review all audit trails and notify Information Owner and/or Information Security Office of any suspicious or abnormal activity.	Log all unsuccessful logon attempts. Review access attempts and notify Information Owner and/or Information Security Office of any suspicious or abnormal activity.	No special requirements.
Audit logs	Retain audit logs for a minimum of 90 days or as required by retention schedules.	Retain audit logs for a minimum of 90 days or as required by retention schedules.	No special requirements.

D) Data Transmission (Minimum handling procedures)

ACTION	CATEGORY I (Confidential)	CATEGORY II (Restricted)	CATEGORY III (Unrestricted)
Transmitting information via fax	Faxed documents must be appropriately labeled to state the confidential nature of the communications and include instructions should the fax be misdirected. If possible, arrangements should be made at both ends of the transmission to monitor the fax machine until the entire fax has been sent and received. Do not leave a fax machine unattended when sending or receiving Category I documents.	Faxed documents must be appropriately labeled to state the restricted nature of the communications and include instructions should the fax be misdirected. If possible, inform recipient about the incoming fax. Do not leave a fax machine unattended when sending or receiving Category II documents.	No special requirements.
Transmitting information via voice mail	Do not leave voice mail messages containing Category I information unless it is a business requirement or at the request of the recipient. Do not forward Category I data to another voice mail.	Do not leave voice mail messages containing Category II information unless it is a business requirement or at the request of the recipient.	No special requirements.
Transmitting information via wired, wireless, or cellular networks (e.g. e-mail, instant messaging, file transfers, telnet sessions, web applications)	All Category I data transmissions and authentication must utilize an encryption mechanism between the sender and receiver; or the file, document, e-mail, or folder must be encrypted before transmission. All transmissions containing Category I data should include only the minimum amount of information necessary.	All Category II data transmissions and authentication must utilize an encryption mechanism between the sender and receiver; or the file, document, e-mail or folder must be encrypted before transmission. All transmissions containing Category II data should include only the minimum amount of information necessary	No special requirements.

5. Definitions

Access Controls – Access controls are the means by which the ability to use, create, modify, view, etc., is explicitly enabled or restricted in some way (usually through physical and system-based controls).

Authentication – The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done using logon passwords.

Data (Information) – It can be printed or written on a piece of paper, stored electronically, transmitted by post or by electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it shared or stored, it should always be appropriately protected. (ISO/IEC 27002:2005, page viii)

Electronic Media – Any of the following: a) Electronic storage media including storage devices in computers (hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card.

Encryption – The translation of data, information or documents into a code that cannot be read without a "key". It is the conversion of data into a form that cannot be easily understood by unauthorized people.

Family Educational Rights and Privacy Act (FERPA) – A federal law that protects the privacy of student educational records.

Health Insurance Portability and Accountability Act (HIPPA) – Federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

Information Owner – The “Custodian of Record” identified from the records and retention schedule posted at <http://www.csufresno.edu/adminserv/records> is the designated Information (Data) Owner for each respective type of data. If a “Custodian of Record” is not identified for an area in the records and retention schedule, then the highest-ranking management personnel (MPP) of that respective area shall be designated as the Information (Data) Owner.

Personally Identifiable Information (PII) – Information that can be used to physically locate or identify an individual, such as names, date of birth, aliases, Social Security numbers, driver’s license number, biometric records, and other personal information that is linked or linkable to an individual. No single law governs all uses of personally identifiable information.

Portable Devices – Any transportable device that is capable of receiving and/or transmitting data. These include, but are not limited to, notebook computers, handheld computers, laptops, PDAs (personal digital assistants), pagers and cell phones.

Removable Media – Removable media devices permit data to be stored on media that is removable and interchangeable. CDs, DVDs, flash memory and floppy disks are examples of removable media.

Server – Any computer providing a service over the network. Services include, but are not limited to: Web site publishing, printing, wireless access and file sharing.

Appendix A
(Minimum Server Protective Measures)

Protective Measures	
1	All users with privileged access to the server must sign a Confidential Access Agreement and file the agreement with the appropriate manager.
2	Privileged (root, Administrator, super user, etc.) access to server must be used only when necessary to perform job duties and only for activities requiring privileged access.
3	The number of administrator accounts (privileged access) is to be kept to a minimum.
4	System events and privileged or elevated account activity must be audited on a per user basis.
5	Servers must be registered in a central database.
6	Access to audit logs must be restricted to users who require that access to perform their job duties.
7	Copies of all audit logs must be transferred via an encrypted connection to a secure machine for storage.
8	Where practical and appropriate, successful and failed attempts to access the information or service must be audited on a per user basis.
9	Where available, two-factor authentication must be required for privileged (root, Administrator, super-user, etc.) access to the server.
10	The server must be in a secure, dedicated server room with physical access controls.
11	A security incident response plan for the server must be developed, tested and communicated to all system administrators.
12	A designated security contact for the server must respond to all critical vulnerability and intrusion detection notifications within four hours.
13	User accounts must be managed in terms of password and username controls (password strings, password ageing, password expiration dates).
14	Backup requirements are documented and coordinated.
15	Services and applications that will not be used must be disabled where practical.
16	Servers must be routinely scanned for network vulnerabilities and firewalls must allow inbound scanner traffic on all ports.
17	Servers must meet all minimum security standards.