



Information Technology Services Standards



 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 1 of 16				

Table of Contents

- 1 Purpose2
- 2 Entities Affected by this Standard.....2
- 3 Definitions2
- 4 Standards5
 - 4.1 Information Classification.....5
 - 4.2 Information Handling.....10
 - 4.3 Information Disposal12
- 5 Contacts.....13
- 6 Applicable Federal and State Laws and Regulations.....13
- 7 Related Documents14

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 2 of 16				

1 Purpose

CSULA must protect the information it owns based on the nature of the information and the risk exposure to the University from inappropriate or undesired access, disclosure, or destruction. The degree of protection provided correlates directly with the risk exposure regardless of the information's media. The degree of protection afforded information is consistent from creation to destruction, including handling and disposal.

Unauthorized access to protected data could introduce fraud, identity theft, loss of reputation, or other risks to the organization. Since protected data is stored, processed and shared in both electronic and paper form, safeguards are required to address information classification, handling and disposal.

CSULA must ensure that information on all media is classified, handled and disposed of in a secure manner. CSULA encourages minimal use and storage of its restricted data to reduce the risk of data compromise.

2 Entities Affected by this Standard


This standard applies to all CSULA users, Third-party Service Providers and any other person accessing CSULA information or information systems.

3 Definitions


- a) **Confidential Information:** In addition to the personal information listed below, examples of confidential information include the following: financial records, student educational records, physical description, home address, home phone number, grades, ethnicity, gender, employment history, performance evaluations, disciplinary action plans, or NCAA standings. Confidential information must be interpreted in combination with all information contained on the computer to determine whether a violation has occurred.

A student may exercise the option to consider directory information, which is normally considered public information, as confidential per the Family Educational Records Privacy Act (FERPA). Directory information includes the student's name, address, phone, dates of attendance, degrees received, major program, height and weight (if an athlete), e-mail address, enrollment status, campus, school, college, division, class standing and awards.


- b) **Data Sanitization:** The process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device. A device that has been sanitized has no usable residual data and even advanced forensic tools should not be able to recover sanitized data.
- c) **Data Steward:** Individual(s) who have management responsibilities (e.g., planning, policy, etc.) for defined segments of the University data as it relates to their functional operations. Individual(s) with operational responsibility for the physical and electronic security of the data.

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 3 of 16				

- d) **Disposition:** A range of processes associated with implementing records/information retention, destruction, or transfer decisions that are documented in the records/information retention and disposition schedule or other authority.
- e) **DVD:** Electronic storage media similar in physical appearance to CDs, but that use a different laser (one that allows for more data to be stored on the disk) to read information. DVDs require a special DVD drive. DVD-R is a write-once format. DVD-RW is similar to DVD-R, but has a re-writable format.
- f) **Electronic Storage Media:** Electronic or optical data storage media or devices that include, but are not limited to, the following: computer hard drives, magnetic disks, CDs, DVDs, flash drives, memory sticks, tapes and Personal Digital Assistants (PDAs – e.g., Palm Pilots, Pocket PCs and smart phones). Also called memory devices.
- g) **Health Insurance Information:** An individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.
- h) **Information Security Officer (ISO):** The CSULA Information Security Officer is the Director for IT Security and Compliance.
- i) **Level 1 Confidential Data:** Confidential data is 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. Confidential data is 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 if data is lost, stolen, unlawfully shared, or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a “business need-to-know.” Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.
- j) **Level 2 Internal Use Data:** Internal use data is information that must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information at this level could cause financial loss, damage to the CSU’s reputation, violate an individual’s privacy rights, or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.
- k) **Level 3 Public Data:** This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard. Knowledge of this information does not expose the CSU to financial loss or jeopardize the security of the CSU’s information assets. Publicly available data may still be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 4 of 16				

- l) **Personal Information:** California Civil Code 1798.29 defines personal information as: An individual's first name or first initial and last name in combination with any one or more of the following data elements:
- Social Security Number
 - Driver's license or California Identification Card number
 - Account number, or 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
 - Health insurance information
- m) **Portable Electronic Storage Media:** Includes, but is not limited to, the following: CDs, CDRWs, DVDs, Zip disks, flash drives, floppy disks, I-pods, digital media players and portable hard drives.
- n) **Proprietary Information:** Information that an individual or entity possesses, owns, or for which there are exclusive rights. Examples include: faculty research, copyrighted materials, white papers, research papers, business continuity and other business operating plans, e-mail messages, vitae, letters, confidential business documents, organization charts or rosters, detailed building drawings and network architecture diagrams. Proprietary information, if lost or stolen, could compromise, disclose, or interrupt operations or embarrass the individual or the University.
- o) **Protected Data:** An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance, or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.
- p) **Record:** "Authentic official copy of a document deposited with a legally designated officer..." (Merriam-Webster Online: <http://www.merriam-webster.com/>). Records can be in any format (handwritten, printed, digital, etc.) and can be stored on paper, computer media, e-mail, hand-held peripherals, CDs, DVDs, wireless devices, video or audio tapes, films, microfilm, microfiche, or any other media.
- q) **Retention Period:** The period of time that a record/information shall/should be kept.
- r) **Shred Bin:** A device that captures discarded paper documents in a locked container. The container is periodically retrieved by an approved vendor, who takes the contents offsite for destruction.
- s) **Shredder:** A device that renders documents completely unreadable by slicing/mincing paper into fine pieces. Approved shredders should be NSA Level 5 compatible.
- t) **State Records Center:** The Center provides storage and retrieval of those records covered by approved Records Disposition Schedules that are not active enough to justify continued retention in the office, but which must be available on a reference basis for a specified period of time or be retained to satisfy legal requirements.

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 5 of 16				

4 Standards

Administrative officials (i.e., vice presidents, deans, directors and other Management Personnel Plan (MPP) employees) are responsible for enforcing the following standards of classifying, handling and disposing of University information for their areas:


4.1 Information Classification

Document classification is critical to maintain staff and student privacy as well as protect valuable information assets of the organization. CSULA has adopted the CSU Data Classification Standard as a minimum information classification standard. The CSU Data Classification Standard is based on federal laws, state laws, regulations, CSU Executive Orders and University policies that govern the privacy and confidentiality of information.


This standard outlines three levels of classification to which information must be secured. The CSU Data Classification Standard applies to all information generated and/or maintained by the University (such as student, research, financial and employee information) except when superseded by grant, contract, or federal copyright law.

The Data Steward of an information asset (both paper and electronic) is responsible for making the determination as to how an asset must be classified (e.g., Level 1, Level 2, or Level 3). The Data Steward is also responsible for ensuring that those with access to the data understand their responsibilities for collecting, using and disposing of the data only in appropriate ways.


Classification	Description	Examples
Level 1 Confidential Data	Confidential data is 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. Confidential information is 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.	<ul style="list-style-type: none"> ○ Passwords or credentials ○ PINs (Personal Identification Numbers) ○ Birth date combined with the last four digits of SSN and name ○ Credit card numbers with cardholder name or expiration date and/or card verification code ○ 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

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 6 of 16				

	<p>Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information.</p> <p>Level 1 and Level 2 access will be granted on a strict "need-to-know" basis only and will be restricted to authorized staff and other participants who have executed an approved Non-Disclosure Agreement (NDA). This information includes organization contact lists, internal processing procedures, employee schedules and other information required to function within the organization but too sensitive to release to the public.</p>	<ul style="list-style-type: none"> ○ Social Security number and name ○ Health insurance information with name ○ 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 ○ Electronic or digitized signatures ○ Private key (digital certificate) ○ Vulnerability/security information related to a campus or system ○ Attorney/client communications ○ Legal investigations conducted by the University ○ Third-party propriety information per contractual agreement ○ Sealed bids ○ Employee name with personally identifiable employee information <ul style="list-style-type: none"> ○ Biometric information ○ Electronic or digitized signatures ○ Personal characteristics
--	--	--

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 7 of 16				

		<ul style="list-style-type: none"> ○ Donor name and giving amount
<p>Level 2 Internal Use Data</p>	<p>Internal Use Information is information that must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information at this level could cause financial loss, damage to cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary.</p> <p>Non-directory student information may not be released except under certain prescribed conditions.</p> <p>Level 1 and Level 2 access will be granted on a strict "need-to-know" basis only and will be restricted to authorized staff and other participants who have executed an approved Non-Disclosure Agreement (NDA). This information includes organization contact lists, internal processing procedures, employee schedules and other information required to function within the organization but too sensitive to release to the public.</p>	<ul style="list-style-type: none"> ○ Identity Validation Keys (name with) <ul style="list-style-type: none"> ○ Birth date (full: mm-dd-yy) ○ Birth date (partial: mm-dd only) ○ Student name with personally identifiable education records <ul style="list-style-type: none"> ○ Grades ○ Courses taken ○ Schedule ○ Test scores ○ Advising records ○ Educational services received ○ Disciplinary actions ○ Employee Information <ul style="list-style-type: none"> ○ Employee net salary ○ Employment history ○ Home address ○ Personal telephone numbers (including emergency contacts) ○ Personal e-mail address ○ Payment History ○ Employee evaluations ○ Disciplinary actions ○ Background investigations ○ Mother's maiden name ○ Race and ethnicity ○ Parents and other family members names

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 8 of 16				


		<ul style="list-style-type: none"> o Birthplace (city, state, country) o Gender o Marital Status o Physical description o Photograph (voluntary for public display) o Other <ul style="list-style-type: none"> o Library circulation information o Trade secrets or intellectual property such as research activities o Location of critical or protected assets o Licensed software
<p>Level 3 Public</p>	<p>This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard.</p> <p>Knowledge of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets. Level 3 information may be subject to appropriate campus review or disclosure procedures to mitigate potentials risks of inappropriate disclosure.</p> <p>Publicly available data may still be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.</p>	<ul style="list-style-type: none"> o Campus Identification Keys <ul style="list-style-type: none"> o Campus identification number o User ID (do not list in a public or a large aggregate list where it is not the same as the student e-mail address) o E-mail o Student Information¹ <ul style="list-style-type: none"> <u>Educational directory information</u> (FERPA) includes: <ul style="list-style-type: none"> o Name o Address o Telephone number o E-mail address o Photograph o Date and place of birth



Information Classification, Handling and Disposal

Standard No:	ITS-2006-S	Rev:	--
Owner:	IT Security and Compliance		
Approved by:	Sheryl Okuno, Director IT Security and Compliance		
Interim Issue:	9-2-10	Effective:	9-2-10

		<ul style="list-style-type: none"> ○ Major field of study ○ Participation in officially recognized activities and sports ○ Height and weight of members of athletic teams ○ Dates of attendance ○ Grade level ○ Enrollment status ○ Degrees, honors and awards received ○ Most recent previous educational agency or institution attended by the student <u>Bargaining unit student employee directory information</u> ○ Name of the department employing the student ○ The student employee's telephone number within the department ○ The student employee's e-mail address within the department ○ The student employee's job classification ○ Employee Information (including student employees) <ul style="list-style-type: none"> ○ Employee title ○ Status as student employee (such as TA, GA, ISA)
--	--	--

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 10 of 16				

		<ul style="list-style-type: none"> ○ Employee campus e-mail address ○ Employee work location and telephone number ○ Employing department ○ Employee classification ○ Employee gross salary ○ Name (first, middle, last) (except when associated with protected data) ○ Signature (non-electronic)
--	--	--

¹CSULA may disclose “Directory Information” without prior written consent of the student. However, at any time the student may exercise the option to consider this information confidential by completing the *Releasing Student “Directory Information” to Outside Agencies* form available each quarter in the CSULA Schedule of Classes and submitting it to the Office of Enrollment Services, ADM 146. All requests for student directory information must be directed to the Office of Enrollment Services, ADM 146 or the Records Office, ADM 409.

Aggregates of data must be classified based upon the most secure classification level. That is, when data of mixed classification exist in the same file, document, report or memorandum, the classification of that file, document, report or memorandum must be of the highest applicable level of classification. If additional guidance is needed, then the campus ISO must be consulted.


Each department/division will maintain an inventory of areas where CSULA Level 1 and 2 Information is stored.

4.2 Information Handling

All paper and electronic media that contains protected data must be secured. Employees, when possible, must secure documents containing protected data by maintaining a clean desk and/or locking documents in secure, designated areas when out of the office. Document security may be achieved through locking the door to a private office, or locking documents in a cabinet or drawer. If no locking storage areas are available documents must still be stored away from plain sight.



Information Technology Services Standards

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 11 of 16				

Any information classified as protected data is not intended for public consumption. As such, special steps must be taken when sharing these documents with external entities. All documents and information not classified as “Public” will require formal approval from the Data Steward before they are communicated externally.

Protected data storage will be kept to a minimum. Individuals must not store protected data on non-University computer systems, personal storage media, or otherwise make copies of protected data without prior written authorization of an appropriate administrator.

Data stored must be appropriately labeled and protected according to its classification. When a file folder contains information of various levels of classification, the file folder must be labeled with the classification of the most sensitive information contained in the file folder. All “confidential” documents should carry labeling in the document footer attesting to its classification level. All electronic media must be labeled prior to storage or transmission outside the organization. All unlabeled documents will be treated as public documents and may be handled accordingly.

All electronic documents containing protected data must be stored in protected areas of the network (group drives, private drives, etc.). Media back-ups must be stored in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility. Backup media must be stored in a physically secure, fireproof location.

Protected data must not be used for testing or development purposes, except when unavoidable. If protected data must be used in a non-production environment, then security controls in the non-production environment must be as strong as the security controls in the production environment.


When Level 1 data is electronically sent, it must be sent via a method that uses strong encryption. When Level 2 Information is electronically sent, it must be protected using encryption measures strong enough to minimize the risk of the information’s exposure if intercepted or misrouted. Campus protected data must be transported via a delivery mechanism that can be tracked, and provided to users only after being authorized by appropriate campus personnel.

All protected data stored on portable electronic storage media must be encrypted. For further information regarding portable electronic storage media, see *ITS-1005-G User Guidelines for Portable Electronic Storage Media*.

The physical transportation of media containing protected data, whether in hardcopy or electronic form, must be secured through use of a secured courier or a delivery mechanism that can be accurately tracked. Protected data must only be transmitted to parties approved for access.

The transfer of essential, but inactive, records can be transferred to the State Records Center (a lower-cost central storage) following the instructions outlined in CSULA Administrative Procedure 707, *Records Retention, Management and Disposition*.

Data Stewards are responsible for determining any special security precautions that must be followed to ensure the integrity, security and appropriate level of confidentiality of their information.

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 12 of 16				

4.3 Information Disposal

Documents and media must be destroyed according to the CSU Systemwide Records/ Information Retention and Disposition Schedule (CSU Executive Order No. 1031) and CSULA Administrative Procedure 707 *Records Retention, Management and Disposition* .


All records should be reviewed at least annually and those identified as eligible for disposition should be approved for destruction unless there is a legitimate business reason to postpone that destruction. Information that has been identified as or is reasonably believed to be relevant to an existing or potential legal proceeding, government investigation, or audit must be retained while the matter is ongoing even when permitted by the CSU Systemwide Records/Information Retention and Disposition Schedule. The appropriate campus management must notify the individuals and/or IT organizations holding the information as to its eligibility for retention or disposition.

The official version of a record should be maintained for the longest approved retention period subscribed in the Records/Information Retention and Disposition Schedule. Any unofficial copy of a record may be destroyed once it has met the business need for which it is kept. Under no circumstance should duplicates or drafts (unofficial records) be retained longer than the official version of the record. When records are approved for destruction, all copies in the possession of employees in all media and formats must also be discarded.

Protected data must be discarded through shredding either by a local confetti or pulp shredder or by placing them in a paper and hard copy media collection point (shred bin). The shred bin must be secure to protect documents prior to final disposal. At least once per month, a document disposal service will shred all documents and dispose of them according to handling requirements in their disposal agreements. Hardcopy materials must be crosscut shred, incinerated, or pulped. Any third-party service providers used for disposal of systems must demonstrate compliance to this standard.

CSULA will maintain paper and hard copy media collection points (shred bins) or local shredders at each facility to collect and protect protected data until it can be properly destroyed. If employees are unsure of the sensitivity of information on a document, the document must be shredded immediately.

Prior to being redeployed, donated, surplus, recycled, destroyed, or otherwise disposed of, the information on computers, laptops, CDs, DVDs, memory drives (e.g., flash drives, memory sticks, thumb drives) and other electronic/optical equipment, devices and storage media must be permanently removed in a manner that prevents its recovery. Protected data stored on campus electronic media and hardware must be securely and thoroughly erased before such items can be re-used. Such data must be sanitized using campus-approved erasure tools or services. Data sanitation should be performed only by designated University personnel and not by an outside source or vendor. The procedures outlined in *ITS-1017-G User Guidelines for Safe Disposal of Electronic Storage Media* and *ITS-1021-G User Guidelines for Data Sanitization* should be followed. CSULA departments and units must certify that electronic and optical data storage devices and media have been properly sanitized (i.e., the data is permanently deleted) before Property Management will accept them for disposition or donation.

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 13 of 16				

5 Contacts

- a. For questions regarding specific department procedures related to document classification, handling and disposal, contact the department administrator.
- b. For assistance in reformatting hard drives and other electronic storage media, contact the ITS Help Desk at 3-6170. The ITS Help Desk will create a work order ticket to have the appropriately trained ITS staff assist the requestor.
- c. For assistance with file encryption or data sanitization, contact the department Information Technology Consultant (ITC).
 - o For a list of campus ITCs, visit <http://www.calstatela.edu/itc>
- d. Find a current list of recommended encryption tools at: <http://www.calstatela.edu/its/desktop/encryptiontools/>
- e. Find up-to-date instructions for WinZip encryption and Microsoft Office 2007 file encryption at: <http://www.calstatela.edu/encrypt>
- f. For questions regarding these guidelines or information security, contact IT Security and Compliance at itsecurity@calstatela.edu.
- g. Information about FERPA requirements is available online at <http://www.calstatela.edu/ferpa>.

6 Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	Family Educational Rights and Privacy Act (FERPA) http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
Gramm-Leach-Bliley Act 15 USC, Subchapter I, Sec. 6801-6809	Gramm-Leach-Bliley Act http://www.ftc.gov/privacy/glbact/glbsub1.htm A federal law on the disclosure of nonpublic personal information.
Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164	Standards for Privacy of Individually Identifiable Health Information http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000 all8parts.pdf A federal law that protects the privacy of health records.

Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 14 of 16				


The Donor Bill of Rights	The Donor Bill of Rights http://www.afpnet.org/Ethics/EnforcementDetail.cfm?ItemNumber=3359 The Donor Bill of Rights was created to ensure that philanthropy merits the respect and trust of the general public, and that donors and prospective donors can have full confidence in the nonprofit organizations and causes they are asked to support.
State	Title
Government Code Sections 14740-14769	State Records Management Act http://www.leginfo.ca.gov/.html/gov_table_of_contents.html Information on the administration of state records.
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85 http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that provides information on safeguarding personal information.
SB 1386	California Personal Information Privacy Act, SB 1386 http://www.info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals.

7 Related Documents


ID/Control #	Title
CSU Executive Order 1031	Systemwide Records/Information Retention and Disposition Schedules Implementation http://www.calstate.edu/eo/EO-1031.html This executive order provides for the implementation of the California State University (CSU) Systemwide Records/Information Retention Schedules.
CSU Information Security Policy	The California Status University Information Security Policy http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.



Information Technology Services Standards

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 15 of 16				

<p>CSULA Administrative Procedure 507</p>	<p>Property Control http://www.calstatela.edu/univ/admfin/procedures/507.pdf Establishes the policy and procedures governing the accountability, control, inventory, movement and other responsibilities for University property.</p>
<p>CSULA Administrative Procedure 707</p>	<p>Record Retention, Management and Disposition http://www.calstatela.edu/univ/admfin/procedures/707.pdf This document establishes procedures for the safe management of University records and the transfer of University records to the State Records Center, the retrieval of stored records and the destruction of obsolete records.</p>
<p>ITS-1000-G</p>	<p>User Guidelines for E-mail Communications http://www.calstatela.edu/its/policies/ This guideline helps students, faculty and staff maintain the University's accepted standard of e-mail use.</p>
<p>ITS-1005-G</p>	<p>User Guidelines for Portable Electronic Storage Media http://www.calstatela.edu/its/policies/ This guideline helps students, faculty and staff meet the University's accepted standards for protecting confidential information that is copied, downloaded, or stored on portable electronic storage media.</p>
<p>ITS-1006-G</p>	<p>User Guidelines for Securing Offices, Workspaces and Documents http://www.calstatela.edu/its/policies/ This guideline is intended to help the campus community protect offices, machines, devices and documents from unauthorized access to confidential, personal and proprietary information.</p>
<p>ITS-1007-G</p>	<p>User Guidelines for Laptop Security http://www.calstatela.edu/its/policies/ This guideline outlines the steps or securing laptops and the personal, confidential and/or proprietary information contained on them.</p>
<p>ITS-1008-G</p>	<p>User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device http://www.calstatela.edu/its/policies/ This guideline outlines the steps users must take to ensure the campus complies with all law and regulations regarding personal and confidential information when desktop or laptop computers and electronic storage devices are lost or stolen.</p>

 Information Classification, Handling and Disposal	Standard No:	ITS-2006-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Interim Issue:	9-2-10	Effective:	9-2-10
Page 16 of 16				

ITS-1017-G	<p>User Guidelines for Safe Disposal of Electronic Storage Media</p> <p>http://www.calstatela.edu/its/policies/</p> <p>This guideline outlines the steps departments and business units, students, faculty and staff should take to remove data and software and appropriately disposition electronic equipment/devices.</p>
ITS-1021-G	<p>User Guidelines for Data Sanitization</p> <p>http://www.calstatela.edu/its/policies/</p> <p>This guideline outlines the tools and procedures for sanitizing various forms of electronic storage media.</p>
ITS-2017-G Pending	<p>User Guidelines for Encryption Security</p> <p>http://www.calstatela.edu/its/policies/</p> <p>These guidelines provide information on approved encryption algorithms, recommended encryption products and specific encryption tools and practices.</p>
ITS-8830	<p>Electronic Data Sanitization Verification</p> <p>http://www.calstatela.edu/its/forms</p> <p>This form must be completed to verify that the electronic storage media was sanitized prior to redeployment to another employee, transfer to another department/division, disposal, or donation to another agency.</p>