Information Classification, Handling and Disposal	Standard No	ITS-2006-S	Rev A
	Owner	IT Security and Compliance	
	Approved by	Sheryl Okuno, Director IT Security and Compliance	
	Issued	2-29-12	Revised 6-22-17
			Page 1 of 14

Table of Contents

1. Purpose 2
2. Related California State University Policies and Standards 2
3. Entities Affected by These Standards 3
4. Definitions 3
5. Standards 5
   - 5.1 Information Classification 5
     - 5.1.1 Level 1 Confidential Data 6
     - 5.1.2 Level 2 Internal Use Data 7
     - 5.1.3 Level 3 Public Information 8
   - 5.2 Information Handling 10
   - 5.3 Information Disposal 11
6. Contacts 12
7. Applicable Federal and State Laws and Regulations 13

Information Classification, Handling and Disposal			
	Standard No	ITS-2006-S	Rev A
	Owner	IT Security and Compliance	
	Approved by	Sheryl Okuno, Director IT Security and Compliance	
	Issued	2-29-12	Revised 6-22-17
			Page 2 of 14

1. Purpose

Cal State LA 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.

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

2. Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
8020.0	**Policy**	**Information Security Risk Management**
8020.S000	*Standard*	*Information Security Risk Management – Exception Standard*
8020.S001	*Standard*	*Information Security Risk Management – Risk Assessment Standard*
8025.0	**Policy**	**Privacy of Personal Information**
8060.0	**Policy**	**Access Control**
8060.S000	*Standard*	*Access Control*
8060.0	**Policy**	**Access Control**
8065.0	**Policy**	**Information Asset Management**
8065.S000	*Standard*	*Information Security Asset Management*
8065.S02	*Standard*	*Information Security Data Classification*
8080.0	**Policy**	**Physical Security**
8080.S01	*Standard*	*Physical and Environmental Security*

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3. Entities Affected by These Standards

This standard applies to all Cal State LA users, third-party service providers and any other person accessing Cal State LA protected data or information systems containing protected data.

4. Definitions

a) Confidential Information: See Level 1 Confidential Data and Level 2 Internal Use Data. Confidential information must be interpreted in combination with all information contained on the computer to determine whether a violation has occurred.

b) Data Sanitization: The process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory or mobile 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 Owner: Person identified by law, contract or policy with responsibility for granting access to and ensuring appropriate controls are in place to protect information assets. The duties include, but are not limited to, classifying, defining controls authorizing access, monitoring compliance with CSU security policies, University standards and guidelines, an identifying the level of acceptable risk for the information asset. A data owner is usually a member of management, in charge of a specific business unit and is ultimately responsible for the protection and use of information within that unit.

d) Data Steward: Also known as Data Custodian. An individual who is responsible for the maintenance and protection of the data. The duties include, but are not limited to, performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media and fulfilling the requirements specified in CSU security policies and University standards and guidelines.

e) 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.

f) Electronic Storage Media: Electronic or optical data storage media or devices including, but not limited to, the following: computer hard drives, laptops, smart phones, tablets, magnetic disks, CDs, DVDs, flash drives, memory sticks, tapes and any emerging technology capable of processing or storing data. 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 Cal State LA 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. Its 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. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

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.

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 or patented materials, white papers, research papers, business continuity and other business operating plans, email 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, email, hand-held peripherals, CDs, DVDs, mobile 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 Sacramento-based center provides storage and retrieval of records/information covered by the Records Retention and Disposition Schedules that are not active enough to justify continued retention on the campus, but which must be available on a reference basis for a specified period of time or be retained to satisfy legal requirements.

5. 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:

5.1 Information Classification

Document classification is critical to maintain staff and student privacy as well as protect valuable information assets of the organization. Cal State LA 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 owner 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 owner 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.

5.1.1 Level 1 Confidential Data

Description	Examples
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. Its 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. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred. Level 1 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 Confidentiality Agreement and an Access and Compliance form. 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.	o Passwords or credentials o PINs (Personal Identification Numbers) o Birth date combined with the last four digits of SSN and name o Credit card numbers with cardholder name or expiration date and/or card verification code o Tax ID with name o Driver's license number, state identification card and other forms of national or international identification (such as passports, visas, etc.) in combination with name o Social Security number and name o Health insurance information with name o Medical records related to an individual o Psychological counseling records related to an individual o 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 o Electronic or digitized signatures o Private key (digital certificate) o Vulnerability/security information related to a campus or system o Attorney/client communications o Legal investigations conducted by the University o Third-party propriety information per contractual agreement o Sealed bids o Employee name with personally identifiable employee information ▪ Biometric information ▪ Electronic or digitized signatures ▪ Personal characteristics

5.1.2 Level 2 Internal Use Data

Description	Examples
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 cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory student information may not be released except under certain prescribed conditions. 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 Confidentiality Agreement and an Access and Compliance form. 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.	o Identity Validation Keys (name with) ▪ Birth date (full: mm-dd-yy) ▪ Birth date (partial: mm-dd only) o Student name with personally identifiable education records ▪ Grades ▪ Courses taken ▪ Schedule ▪ Test scores ▪ Advising records ▪ Educational services received ▪ Disciplinary actions o Employee Information ▪ Employee net salary ▪ Employment history ▪ Home address ▪ Personal telephone numbers (including emergency contacts) ▪ Personal email address ▪ Payment History ▪ Employee evaluations ▪ Disciplinary actions ▪ Background investigations ▪ Mother's maiden name ▪ Race and ethnicity ▪ Parents and other family members names ▪ Birthplace (city, state, country) ▪ Gender ▪ Marital Status ▪ Physical description ▪ Photograph (voluntary for public display) o Donor Information ▪ Donor name

Description	Examples
	▪ Home address ▪ Home, Business, Cell, and Other phone ▪ Email address ▪ Giving history (last 8 gifts or transactions might be pledges) ▪ Employment information as defined above **Other** o Library circulation information o Trade secrets or intellectual property such as research activities o Location of critical or protected assets o Licensed software

5.1.3 Level 3 Public Information

Description	Examples
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 University review or disclosure procedures to mitigate potential risks of inappropriate disclosure.	o University Identification Keys ▪ Campus identification number (CIN) ▪ User ID (do not list in a public or a large aggregate list where it is not the same as the student email address) ▪ Email o **Student Information** **Educational directory information[1] (FERPA) includes:** ▪ Name ▪ Address ▪ Telephone number ▪ Email address ▪ Photograph ▪ Date and place of birth ▪ Major field of study ▪ Participation in officially recognized activities and sports ▪ Height and weight of members of athletic teams

[1] Cal State LA 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 semester in the Cal State LA Schedule of Classes and submitting it to the Records Office. All requests for student directory information **must** be directed to the Records Office.

- Dates of attendance
- Grade level
- Enrollment status
- Degrees, honors and awards received
- Most recent previous educational agency or institution attended by the student

o **Bargaining unit student employee directory information includes:**

- Name of the department employing the student
- The student employee's telephone number within the department
- The student employee's email address within the department
- The student employee's job classification

o **Employee Information (including student employees) includes:**

- Employee title
- Status as student employee (such as TA, GA, ISA)
- Employee campus email 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)

o **Donor Information**

- Constituent Code
- Class of
- Degree
- Academic Org
- Major
- Employment information as defined above
- Job title

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, email or memorandum, the classification of that file, document, report, email or memorandum must be of the highest applicable level of classification. If additional guidance is needed, then the University ISO must be consulted.

Each department/division will maintain an inventory of areas where Cal State LA Levels 1 and 2 Confidential Data is stored.

5.2 Information Handling

All paper and electronic media that contains protected data must be secured. Employees, when possible, must secure documents containing protected data by locking documents in their desk, cabinet or a secure, designated area when out of the office. Document security may be achieved through locking the door to a private office.

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 owner 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 or cloud 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 Confidential data is electronically sent, it must be sent via a method that uses strong encryption. When Level 2 Internal Use Data 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. University protected data must be transported via a delivery mechanism that can be tracked, and provided to users only after being authorized by appropriate University 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 Cal State LA Administrative Procedure 707, *Records Retention, Management and Disposition*.

Data owners 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.

5.3 Information Disposal

Documents and media must be destroyed according to the CSU System wide Records/ Information Retention and Disposition Schedule (CSU Executive Order No. 1031) and Cal State LA 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 University 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.

Cal State LA 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, surplused, 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 University electronic media and hardware must be securely and thoroughly erased before such items can be re-used. Such data must be sanitized using University-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. Cal State LA 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.

6. 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 department Information Technology Consultant (ITC) or 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 ITC.

d. For a list of University ITCs, visit http://www.calstatela.edu/itc

e. Find a current list of recommended encryption tools at: http://www.calstatela.edu/its/services/software/encryptiontools.php

f. Find up-to-date instructions for WinZip encryption and Microsoft Office 2010, 2013 and 2016 file encryption at: http://www.calstatela.edu/encrypt

g. For questions regarding these guidelines or information security, contact IT Security and Compliance at itsecurity@calstatela.edu.

h. Information about FERPA requirements is available online at http://www.calstatela.edu/ferpa.

7. 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.
Federal Privacy Act of 1974	**Federal Privacy Act of 1974** http://www.usdoj.gov/opcl/privacyact1974.htm This is a federal act that establishes a code of fair information practices governing the collection, maintenance, use and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Gramm-Leach-Bliley Act 15 USC, Subchapter I, Sec. 6801-6809	**Gramm-Leach-Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of non-public 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/prdecember2000all8parts.pdf This is a federal law that protects the privacy of health records.
Fair and Accurate Credit Transactions Act of 2003 (FACTA)	**Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Red Flag Rules** http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf This is a federal law that requires financial institutions and creditors to develop and implement written identity theft prevention programs.
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
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.8** http://www.leginfo.legislature.ca.gov/ This is a state law that, as amended by SB 1386 (2003), AB 1298 (2007) and SB 24 (2011), provides information on safeguarding personal information, requires notification to California residents whose personal information was or is reasonably believed to have been acquired by unauthorized individuals and requires notification to the Attorney General if more than 500 residents are involved.