

Information Security Program

For California State University, Los Angeles

REVIEWED AND UPDATED: 2019

INFORMATION TECHNOLOGY SERVICES

Table of Contents

I. Purpose 1
II. Information Security Policy 1
III. Scope 1
IV. General Program Information 2
  A. Information Security Management Team 2
  B. Governance 2
  C. Review of the Information Security Program 3
  D. Access to the Plan 3
V. Definitions 3
VI. Classifications of Data 5
VII. Relevant Areas 6
VIII. Physical Security 6
IX. Inventory Management 7
  A. Reporting Lost or Stolen Equipment 7
  B. Reporting Missing Equipment 7
  C. Data Sanitization 8
X. Risk Assessment and Safeguards 8
  A. Risk Identification 8
  B. Risk Evaluation 9
  C. Risk Mitigation 9
  D. Risk Monitoring and Reporting 10
XI. Information Security Programs 10
  A. Family Educational Rights and Privacy Act (FERPA) Program 11
  B. Gramm Leach Bliley (GLB) Information Security Program 11
  C. Health Information Portability and Accountability Act (HIPAA) 12
  D. Identity Theft Prevention Program 12
  E. Payment Card Industry Data Security Standard (PCI DSS) Program 13
XII. Managing Third-party Service Providers 13
  A. Contracts 14
  B. Granting Access to Third-party Service Providers 14
XIII. Information Security Incident Management 15
  A. Incident Response 15
  B. Security Breach Notification 15
XIV. Emergency Preparedness 16
  A. Disaster Recovery 16
  B. Business Continuity 16
XV. Information Security Awareness Program 16
  A. Information Security Training 16
  B. Information Security Awareness 17

Cal State LA Information Security Program

I. Purpose

California State University, Los Angeles (Cal State LA) establishes this Information Security Program in compliance with the CSU Information Security Policy, Section 8010.0, "Establishing an Information Security Program." Cal State LA recognizes its obligation to protect the technology resources and information assets entrusted to it. Unauthorized access, disclosure, modification or deletion of information assets can compromise the University's mission, violate individual privacy rights and possibly constitute a criminal act.

This University program defines and communicates appropriate and reasonable administrative, technical and physical safeguards designed to:

- Document roles and responsibilities for the information security program.
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g., paper or electronic).
- Document strategies to identify and mitigate threats and vulnerabilities to Level 1 Confidential Data and Level 2 Internal Use Data (herein referred to as protected data) as defined in *ITS-2006-S Information Classification, Handling and Disposal*.
- Document an information security incident response plan.
- Provide ongoing security awareness and training programs.
- Comply with all applicable federal and state laws and regulations, CSU Information Security Policy, and applicable Cal State LA policies, procedures, standards and guidelines.

The Cal State LA Information Security Program and supporting ITS standards and guidelines are not intended to prevent, prohibit or inhibit the sanctioned use of information assets as required to meet University academic and administrative goals.

II. Information Security Policy

Consistent with published CSU Information Security Policies and Standards, Cal State LA Administrative Policy P-008, *Policy for Technology and Information Security Compliance* (2013), establishes the policy and responsibilities for the University. This policy is further supported by related ITS standards and guidelines that facilitate University compliance with the recommendations, audit requirements, actions and safeguards necessary to mitigate risks and protect information assets.

III. Scope

All constituents of the University organization share a responsibility for protecting information resources. A collaborative and unified approach provides the strongest defense against system unavailability, service interruptions, identity theft and fraud.

Consistent with CSU Information Security Policies, the Cal State LA Information Security Program applies to the following:

- Centrally-managed and department-managed systems and information assets.
- All users employed by Cal State LA, auxiliary organizations, third-party service providers and any other person with access to the Cal State LA network resources or information assets. This includes any non-University-owned and non-University-housed computing, electronic storage or mobile devices that may store University protected data.

- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic).
- Information technology facilities, hardware systems, network resources and applications owned by Cal State LA. This includes third-party service providers' systems that access or store Cal State LA protected data, transmit protected data over communication lines, or process credit card payments.

IV. General Program Information

A. Information Security Management Team

The President has designated responsibility for the University information security program to the following individuals:

- **Associate Vice President for Information Technology Services**

  Provides general oversight for the information technology infrastructure, administrative and academic systems, and information security; and provides updates to the Executive Cabinet, as needed.

- **Information Practices/Privacy Officer (IPO) – University Counsel**

  Provides guidance with all legal matters involving information assets and privacy regulations; acts as the University's designated agent with the U.S. Copyright Office to receive and act upon copyright infringement notifications; and provides oversight in investigations involving employees and students suspected of violating the CSU Information Security Policy or federal and state laws and regulations.

- **Information Security Officer (ISO)** – Director of IT Security and Compliance

  Coordinates and oversees University compliance with the Information Security Program; develops and administers all information security standards and guidelines; directs and supports the information security risk management process; coordinates with the internal auditor for independent information security audits; manages security awareness; conducts computer forensic evaluations; leads the Cal State LA-CSIRT team and serves as the University representative on the CSU Information Security Advisory committee (ISAC).

- **Vice Presidents**

  Oversee risk assessment, mitigation and acceptance for their respective division; ensure compliance with state and federal statutes and regulations in accordance with published ITS standards and user guidelines; ensure compliance with information security programs relevant to their respective division; maintain a disaster recovery plan for decentralized systems within the division; and maintain a divisional business continuity plan.

B. Governance

Oversight for Information Technology Services is provided by the associate vice president who reports to the vice president for Administration and Finance, who is a member of the executive cabinet.

The ISO chairs the weekly vulnerability management meeting, which evaluates risk and reviews the remediation status of network and server vulnerabilities.

C. Review of the Information Security Program

The information security program is reviewed annually by the information security officer (ISO) and updated as required. The program may be evaluated and adjusted at any time in light of relevant circumstances, including changes in the University's business arrangements or operations, federal or state regulatory changes, or as a result of testing and monitoring the safeguards.

D. Access to the Plan

Information Technology Services (ITS) is responsible for online publication of the Information Security Program for California State University, Los Angeles. The printed document is maintained by the director of IT Security and Compliance.

V. Definitions

a. **Business Continuity Plan (BCP)**: A document describing how an organization responds to an event to ensure critical business functions continue to be provided without unacceptable delay or change.

b. **Confidential Information:** See Level 1 Confidential Data and Level 2 Internal Use Data in ITS-2006-S Information Classification, Handling and Disposal. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a security violation has occurred.

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 and campus standards and guidelines, and 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 date, restoring data from backup media and fulfilling the requirements specified in CSU security policies and campus standards and guidelines.

e. **Disaster Recovery Plan (DRP)**: A technical document describing how an organization restores critical technology and business systems following an outage or disaster.

f. **Documents:** Includes not only hard copy documents, but audio recordings, videotapes, email, instant messages, word processing documents, spreadsheets, databases, calendars, telephone logs, contact manager information, internet usage files and all other electronic information maintained, created, received or maintained by Cal State LA on computer systems.

g. **Financial Information:** Any information that the University has obtained from employees, alumni, auxiliary agencies, patrons, external program participants or the like in the process of offering a financial product or service, or conducting a program. Offering a financial product or service, or conducting a program includes, but is not limited to, compiling billing information for patrons of venues and events, billing for services to employees or community participants, employee and alumni donations, tracking of financial and other confidential information on internal and external programs.

Examples of Financial Information include bank and credit card account numbers and income and credit histories.

h. **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.

i. **Identifying Information:** Any name or number that may be used alone or in conjunction with any other information to identify a specific person. Identifying information generally includes name, address, telephone number, Social Security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or unique electronic identification number.

j. **Medical Information:** Any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional.

k. **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

l. **Physical Access:** Being able to physically touch, use and interact with information systems and network devices.

m. **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.

n. **Protected Data:** An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medication information. See Level 1 Confidential Data and Level 2 Internal Use Data: Section II Classifications of Data.

o. **Public Information:** Any information prepared, owned, used, or retained by Cal State LA and not specifically exempt from disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

p. **Risk Assessment**: A process by which quantitatively or qualitatively, risks are identified and the impacts of those risks are determined. The initial step of risk management.

q. **Risk Management**: A structured process that identifies risks, prioritizes them and then manages them to appropriate and reasonable levels.

r. **Security Awareness**: Awareness of security and controls, in non-technical terms, conveyed to motivate and educate users about important information security protections that they can either directly control or be subjected to.

s. **Student Financial Information:** Information the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of Student Financial Information include bank and credit card account numbers and income and credit histories.

VI. Classifications of Data

Cal State LA utilizes the California State University (CSU) Data Classification Standard, which outlines three levels of information classification. The CSU Data Classification Standard applies to all information generated and/or maintained by the University, such as student, research, financial, health and employee information, except when superseded by grant, contract or federal copyright.

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 security violation has occurred.

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.

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.

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, telephone listing, email address, photograph, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, date of attendance, grade level, enrollment status, degrees, honors and awards received, and the most recent previous educational agency or institution attended by the student. For bargaining unit student employees, directory information also includes: the name of the department employing the student, the student employee's telephone listing within the department, the student employee's email address within the department, and the student employee's job classification.

A detailed list of University-specific examples of levels 1, 2 and 3 data is available by clicking on the link in the above descriptions or by viewing *ITS-2006-S Information Classification, Handling and Disposal.*

VII. Relevant Areas

Relevant areas, those areas required to comply with information security policies, are defined as all offices and individuals campus wide engaged in the following services, activities or practices:

- Administrative offices and data owners of University administrative systems (i.e., Student Administration, Human Resources Management and Financials).
- Academic and administrative offices that maintain decentralized systems (i.e., systems not centrally located in the data center and not maintained by ITS).
- Academic and administrative offices that handle electronic or printed personnel records, financial records, transactional records or student records.
- Academic and administrative offices that transmit confidential information to off-site locations as part of a periodic review or submission requirement.
- Academic, administrative and auxiliaries that collect or handle credit card transactions.
- Centers, institutes and clinics that provide services and acquire personal, financial, medical or health insurance information from participants or constituents.
- Faculty serving as directors, coordinators, principal investigators or program directors for programs collecting confidential information.
- Faculty, staff and administrators with contracts to use, access or provide confidential information to or receive from a non-campus entity (e.g., government databases, science databases).
- Performing arts organizations that collect patron information.

Responsibilities

i. Each relevant area is responsible for identifying, assessing the risk, and securing all University protected data under its supervision in accordance with all privacy guidelines.

ii. Vice presidents have oversight responsibility for the information security policies, processes and practices of each relevant area within their respective divisions, and for appointing a responsible data owner for each identified area.

iii. The Information Technology Services division will create, maintain and publish standards, guidelines, procedures and tools to assist relevant areas in protecting against anticipated threats to the security or integrity of University protected data in any format (e.g., electronic, hard copy, microfiche, etc.) and guard against the unauthorized access and use of such information.

VIII. Physical Security

Departments must protect areas containing protected data from unauthorized physical access while ensuring that authorized users have appropriate access. Examples of these areas include data centers, server rooms, department or individual offices containing decentralized systems and offices with smart copiers, printed documents or other materials containing protected data.

Responsibilities

i. Each division must identify physical areas that must be protected from unauthorized physical access.

ii. All employees must lock their computers [Control-Alt-Delete] when unattended.

iii. Employees, when possible, must secure documents and other materials 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.

IX. Inventory Management

As required by CSU Information Security Policy 8065.0, "Information Asset Management," the University must have a process for documenting the handling, storage, retention and disposition of Levels 1 and 2 Confidential Data. This includes both the data and the device(s) containing the data. To manage this process, the University must develop and maintain an equipment inventory business process that ensures:

- Physical equipment inventory is current, complete and accurate;
- A formal process is in place to report lost, stolen or missing computers and electronic storage devices;
- All missing equipment is evaluated for the presence of Levels 1 and 2 Confidential Data; and
- Computers are data sanitized (degaussed) prior to disposal.

Responsibilities

A. Reporting Lost or Stolen Equipment

Owners of lost or stolen desktop or laptop computers or electronic storage devices must take two actions immediately upon discovery of the loss:

- Notify University Police so a theft/loss report can be filed.
- Complete form *ITS-2804 Lost or Stolen Computer or Electronic Storage Device Report* and submit it to ITSecurity@calstatela.edu. This form is provided to the equipment owner by University Police at the time a theft report is filed, and a copy of this report is filed with the police report.

IT Security and Compliance will evaluate the data content and its vulnerability to determine whether notification to California residents is required under California Civil Codes 1798.29 and 1798.82.

B. Reporting Missing Equipment

Departments are responsible for verifying whether equipment identified as missing during routinely scheduled Property Office inventories contains Levels 1 and 2 Confidential Data. Department administrators or designees must check the appropriate boxes on the Property Office missing inventory spreadsheets to indicate whether missing equipment a) contained, b) did not contain, or c) is unknown to contain protected data.

IT Security and Compliance will evaluate all missing equipment that contained Levels 1 and 2 Confidential Data by reviewing the department's data backup to determine whether notification to California residents is required under California Civil Codes 1798.29 and 1798.82

Vice presidents will review and sign the risk acceptance letter provided by IT Security and Compliance.

C. Data Sanitization

Data sanitization is the process of deliberately, permanently, irreversibly removing or destroying the data stored on an electronic storage device. These devices include, but are not limited to, the following: computer and laptop hard drives, magnetic disks, flash memory devices, CDs and DVDs, smartphones, Zip disks, and USB storage devices (e.g., flash drives, iPods, and portable hard drives). A device that has been sanitized has no usable residual data remaining and even advanced forensic tools should never be able to recover erased data.

ITS and department ITCs are responsible for a) performing the data sanitization process on University-owned computers and electronic storage media, b) signing the *Electronic Data Sanitization Verification* form, and c) submitting the signed copy to Property Management (for donation or disposal) or the requesting department (for reassignment or relocation), as appropriate.

Property Management is responsible for ensuring that data sanitization has occurred prior to the relocation, reassignment, donation or disposition of University-owned electronic storage media and retaining all *Electronic Data Sanitization Verification* forms.

X. Risk Assessment and Safeguards

As required by CSU Information Security Policy 8020.0, "Information Security Risk Management," the University must develop risk management processes that identify, assess and monitor risks to information assets containing Levels 1 and 2 Confidential Data. Identified risks must be actively managed by the data owner or appropriate administrator. The campus must prepare an annual review of risks to measure its ongoing success at controlling, preventing and mitigating risks, and report the results to the Chancellor's Office.

Responsibilities

A. Risk Identification

i. The University requires risk identification be applied to the electronic content of every system, server, desktop, laptop, smartphone, tablet and electronic storage device used for University work purposes.

ii. The University includes paper documents and electronic media (e.g., microfiche, CDs, DVDs, unencrypted flash drives, etc.) in its risk identification process.

iii. The University includes physical security in its risk identification process.

iv. Vice presidents shall identify any employees in their respective relevant areas that work with protected data.

v. Vice president shall ensure designated employees participate in the annual campus risk assessment, if requested to do so.

vi. IT Security and Compliance shall perform vulnerability scans of networks and servers on a weekly basis.

vii. IT Security and Compliance shall conduct an annual review of decentralized systems and review risks to Level 1 confidential data.

viii. IT Security and Compliance shall conduct an annual review of user access forms for administrative and decentralize systems.

ix. All employees shall identify potential risks within their work environment.

x. IT Security and Compliance shall run a monthly Spirion scan to assist employees with identifying electronic files containing Level 1 confidential data so that they can encrypt or safely dispose files.

xi. All employees shall review the Spirion scan results and encrypt or safely dispose of files.

xii. University Police shall inform the director of IT Security and Compliance immediately upon notification of lost or stolen electronic equipment.

xiii. All departments shall promptly report missing equipment to Property Management for evaluation of the possible loss of Levels 1 and 2 Confidential Data.

xiv. All “relevant areas” shall identify potential and actual risks to security and privacy of protected data.

B. Risk Evaluation

i. ITS will utilize tools, monitors, subscription alerts and the like to keep current on all potential threats to the network and its data.

ii. ITS will keep records of patching activity for environments and systems under its management and review its procedures for patches to its software environments at least annually.

iii. Vice presidents will review the consolidated annual report of identified risks. The report will be consolidated from individual Information Security Risk Assessment Worksheets submitted during the annual review process.

iv. Vice presidents will be responsible for decisions regarding mitigation (risk reduction), transference (share with or shift to another party) or acceptance of identified risks (risk assumption) within their respective divisions.

v. The director of IT Security and Compliance will evaluate all missing, lost or stolen electronic equipment to determine if a security breach has occurred.

C. Risk Mitigation

i. ITS will implement the highest level of security protection (e.g., firewalls, anti-virus, anti-spam, server farms, V-LAN topology, etc.) as deemed necessary and feasible to protect centrally managed University assets.

ii. ITS will assure that patches for the software environments (e.g., operating system, system software, database management systems and application packages) for centrally managed servers and centrally managed desktops, laptops and Open Access Labs (OALs) are reasonably up-to-date.

iii. ITS will ensure the physical security of all centrally managed servers that contain or have access to protected data.

iv. Vice presidents will ensure the physical security of all decentralized servers and sensitive work areas that contain or have access to protected data within their respective divisions.

v. In accordance with the CSU data retention schedule, the University will maintain a record of those members of the University community who have approved access to protected data contained in the Student Administration, Human Resources Management and Financials

systems. Human Resources Management will be responsible for including the original user's account request form in each employee's official personnel file.

vi. Vice presidents will ensure decentralized system data owners maintain a record of those members of each department who have approved access to protected data contained in those decentralized systems.

vii. Vice presidents will ensure that all employees in their respective divisions utilize available tools (e.g., Spirion) to identify, encrypt or securely dispose of all documents containing confidential information on computers and electronic storage media.

viii. ITS will issue user guidelines and standards to inform the campus of risks and threats, standard business practices to prevent or mitigate them and recovery measures.

ix. All University constituents shall follow the guidelines outlined in *ITS-1027-G User Guidelines for Encryption Security* to ensure all protected data is encrypted in transit and at rest.

x. All University constituents shall follow the standards outlined in *ITS-2008-S Password Standards t*o ensure passwords to access networks and systems meet minimum security requirements.

xi. All University constituents shall follow the guidelines outlined in *ITS-1021-G User Guidelines for Data Sanitization* to ensure all workstations and electronic storage media are sanitized prior to relocation, reassignment, disposal or donation.

D. Risk Monitoring and Reporting

i. IT Security and Compliance will prepare the annual online risk assessment survey tool and notify the designated participants to conduct the risk assessment. Participants shall be identified by the vice presidents of each division.

ii. All "relevant areas," as described in Section VII, shall conduct an annual data security review using a risk assessment survey tool provided by IT Security and Compliance.

iii. IT Security and Compliance will produce an annual consolidated report with the results of the risk assessment survey for all vice presidents and the internal auditor.

iv. IT Security and Compliance will produce an executive summary of security risks and provide it to the president annually for review and approval.

XI. Information Security Programs

Whenever new federal and state statutes are enacted or data security standards are created or updated, the information security officer will evaluate whether the University conducts any business processes that apply to the new statue or standard. If the University is required to comply, an Information Security Program will be established to meet the specific objectives. The purposes of these programs are to:

- Notify the University of the data security standard.
- Identify the University constituents who must participate in the program.
- Assign administrative responsibility for the program.
- Outline compliance requirements of the data security standard.
- Define the specific steps that constituents must follow to comply with the data security standard.
- Inform constituents of all required self-assessments, tests, reports, questionnaires, certifications and the like that may be required on an annual or semi-annual basis.

A. Family Educational Rights and Privacy Act (FERPA) Program

Summary. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) protects the privacy of student education records. FERPA is a federal law that applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Administrative Procedure 011 *Student Records Administration* (2005) is the published campus policy and procedure for maintaining student records.

Responsibilities.

i. Only those individuals who have been authorized as having a legitimate reason to access student education records can do so. Access to student education records is strictly limited to the specific information and data that is relevant and necessary for those authorized individuals to perform their job-related duties.

ii. All faculty, staff and students, including temporary employees, student assistants, teaching associates and consultants, must comply with federal law, University policies and Executive Order 796 regarding the access and use of student education records.

iii. All faculty and staff are required to complete the online FERPA training every two years and submit a renewal certificate of completion to Human Resources Management for continued access to the University network and systems.

B. Gramm Leach Bliley (GLB) Information Security Program

Summary. The Gramm-Leach-Bliley Act (GLB Act), also known as the Financial Modernization Act of 1999, is a federal law that includes provisions to protect consumers' personal financial information held by financial institutions. A portion of these regulations are applicable to colleges and universities and require that the University appoint an information security coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to protected data and information, oversee service providers and contracts, and evaluate and adjust the plan. All offices and individuals campus wide who are engaged in the following activities or practices are required to participate in the Gramm Leach Bliley Information Security Program:

- Academic and administrative offices that handle electronic or printed personnel records, financial records, transactional records, or student records.
- Academic and administrative offices that transmit confidential information (protected data) to off-site locations as part of a periodic review or submission requirement.
- Centers and Institutes that provide services and acquire personal or financial information from participants or constituents.
- Faculty serving as directors, coordinators, principal investigators or program directors for programs collecting protected data.
- Faculty, staff and administrators with contracts to use, access or provide protected data to or receive from a non-campus entity (e.g., government databases, science databases).
- Performing arts organizations that collect patron information.

Responsibilities.

i. All departments that handle or maintain protected data must perform a risk assessment of their areas and put safeguards in place to secure personally identifiable, financial and student financial information.

ii. Administrators are responsible for educating all department personnel about information security best practices in their respective areas.

iii. Oversight must be provided to service providers who are given access to protected data or may come in contact with protected data while carrying out contracted service responsibilities.

C. Health Information Portability and Accountability Act (HIPAA)

Summary. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a broad federal law. Two components of HIPAA, the Privacy Rule and the Security Rule, govern the privacy of an individual's health information. The Privacy Rule regulates the use and disclosure of Protected Health Information (PHI). The Security Rule compliments the Privacy Rule and identifies standards and implementation specifications that organizations must meet in order to be compliant. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (ePHI).

The California State University (CSU) has limited the scope of its compliance obligations by taking on "hybrid entity" status under HIPAA and formally designating CSU health care components [*Designation of Health Care Components for Purposes of the Health Care Portability and Accountability Act of 1996 (HIPAA)* - CSU Executive Order 877]. As a hybrid entity, only the designated CSU health care components, and not the entire institution, are required to comply fully with HIPAA.

Responsibilities.

i. All departments, services, clinics and individuals that collect, maintain, access, transmit or receive protected health information on paper or electronically must implement administrative, physical and technical safeguards to ensure the appropriate security of all health information received, maintained or transmitted.

Complete program details are outlined in *ITS-1028-G User Guidelines for HIPAA Compliance*.

D. Identity Theft Prevention Program

Summary. On October 31, 2007, the Federal Trade Commission and the federal financial institution regulatory agencies passed the final legislation to incorporate new sections 114 and 315 into the Fair and Accurate Credit Transactions Act of 2003 (FACTA). These new sections are referred to as the Red Flag Rules. Under the Red Flag Rules, every financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, is required to establish a documented Identity Theft Prevention Program that provides for the identification, detection and response to patterns, practices or specific activities - known as "red flags" - that could indicate identity theft. Examples of red flag activities include unusual account activity, address discrepancies, fraud alerts on a constituent's consumer report provided by a Credit Reporting Agency, or the attempted use of suspicious account applications.

Since the University provides student loans and collects payment for some services, it is considered a creditor and the FACTA Red Flag Rules apply.

Responsibilities.

i. All University departments and employees responsible for providing student loans and/or collecting payment for services must participate in the Identity Theft Prevention Program.

ii. Departments must first determine whether there are covered accounts within the business processes of their respective areas. Generally covered accounts distribute reimbursable University funds; extend, renew or continue credit; and allow the account owner to make multiple payments or transactions.

Complete program details are outlined in *ITS-1018-G User Guidelines for Identity Theft Prevention*.

E. Payment Card Industry Data Security Standard (PCI DSS) Program

Summary. The PCI DSS, a set of comprehensive requirements for enhancing payment card data security, was developed in 2004 by the founding payment brands of the PCI Security Standards Council, which included American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International. The purpose was to facilitate the broad adoption of consistent data security measures on a global basis.

In May 2018, version 3.2.1 was released. It is recognized that since Universities collect credit card information and process credit card payments, there is a contractual obligation for them to adhere to the PCI DSS, as well as credit card association, rules and regulations. Federal requirements continue to be updated through new versions, as needed.

Responsibilities.

i. All officials or administrators with responsibilities for managing University credit card transactions and those employees who are entrusted with processing, transmitting or handling cardholder information in a physical or electronic format must participate in the PCI DSS Program.

ii. All computers and electronic devices involved in processing payment card data are governed by PCI DSS. By adhering to these standards the University's liability is limited and the processing of credit cards may continue.

iii. The PCI Compliance officer for the university coordinates all PCI assessment and security activities.

Complete program details are outlined in *ITS-1025-G User Guidelines for Collecting and Processing Credit Card Information*.

XII. Managing Third-party Service Providers

As required by CSU Information Security Policy 8040.0, "Managing Third Parties," third-party service providers may be granted access to University protected data only when they have a need for specific access in order to accomplish an authorized task. This access must be reviewed and authorized by the data owner and/or a designated campus official; access must be based on need-to-know and least privilege; appropriate security controls must be implemented; and a signed contract or agreement in place defining the terms and duration for access.

A. Contracts

Contracts with service providers will include, to the extent possible, the following provisions:

- An explicit acknowledgment that the contract allows the contract partner access to confidential information;
- A specific definition of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- A guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
- A guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
- A provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- A provision requiring immediate notification in the event an employee assigned to the campus terminates employment;
- A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
- A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles California State University, Los Angeles to immediately terminate the contract without penalty;
- A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
- A provision ensuring that the contract's protective requirements shall survive any termination agreement.

B. Granting Access to Third-party Service Providers

Third-party service providers must adhere to all appropriate CSU and Cal State LA information security policies, standards, guidelines and information security programs. Service providers requiring a system account and/or password to perform maintenance on University computer systems must complete the appropriate system access form and sign an Information Confidentiality/Non-disclosure Agreement. Such service providers will be required to provide immediate notice of any terminations of personnel dedicated to providing full-time campus or backup support.

Responsibilities.

i. The director of Procurement and Contracts, the vice president for Administration and CFO, and/or university counsel/IPO are responsible for reviewing service provider contracts for the University and for ensuring all provisions are incorporated into contracts prior to award.

ii. The director of IT Security and Compliance will provide standard contract templates for University constituents' use that include all the above provisions:

- *ITS-2827 Information Security Contract Language for Third-party Service Providers with Direct Data Access* is for providers such as system designers; equipment or system installers; maintenance technicians; application developers; consultants; student service providers that require the use of University protected data and recipients of University protected data for reporting purposes. These providers are generally granted access to

the equipment or protected data to perform the specific tasks and responsibilities detailed in the approved Purchase Requisition, service contract, scope of work or other official procurement document.

- *ITS-2828 Information Security Contract Language for Third-party Service Providers with Indirect Data Access* is for providers such as office equipment installers or maintenance personnel; painters; electricians; plumbers; carpet installers or cleaners; furniture delivery or assembly personnel and the like. These providers may come in contact indirectly with protected data in the work area such as that visible on a computer screen, in use at a desk, or laying on a file cabinet, copies or fax machine.

Both templates are available on the ITS website, in the Service Catalog, under Procurement > Forms

XIII. Information Security Incident Management

In accordance with CSU Information Security Policy 8075.0, "Information Security Incident Management," the University maintains an incident response team to investigate, respond to, report and recover from security incidents involving loss, damage or misuse of University information assets.

A. Incident Response

The University will maintain an established, trained Campus Security Incident Response Team (CSIRT), headed by the director of IT Security and Compliance, to ensure effective response to information security incidents and to assist in the protection of University protected data. Rapid response and collective actions are required to counteract security violations and activities that lead to information security breaches and incidents, and to return to a normalized and secure state as quickly as possible, while minimizing the adverse impact to the University.

Responsibilities.

i. Any actual or suspected breach in any type of media (e.g., electronic, paper, verbal, microfiche, etc.) must be reported immediately to the ITS Help Desk at 323-343-6170 or the director of IT Security and Compliance at 323-343-2600.

ii. Lost or stolen computers, laptops, tablets, smartphones or other electronic storage media must be reported immediately to both University Police and IT Security and Compliance.

iii. Any computers, laptops, tablets, smartphones or other electronic storage media identified as missing during scheduled Property Management inventories must be verified for the existence of protected data and the division vice president must approve acceptance of any risk.

B. Security Breach Notification

California Civil Code Sections 1798.29, 1798.82, 1798.84 and 1798.85, 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 California residents are involved.

The Information Security Officer will work closely colleges, divisions, departments as well as the Chancellor's Office to ensure that the campus complies with applicable laws regarding notification of security breaches involving personal information.

XIV. Emergency Preparedness

A. Disaster Recovery

Disaster recovery plans shall be created to outline all the detailed roles, responsibilities and steps required to restore those systems and services critical to campus operations following a minor, intermediate and major disruption, outage, failure or destruction.

Responsibilities

i. The associate vice president for Information Technology Services is responsible for development, review and maintenance of the disaster recovery plan for all centralized systems under ITS management.

ii. The associate vice president for Information Technology Services is responsible for publishing a redacted copy of the ITS Technical Disaster Recovery on the ITS website to inform the campus of the duration that systems may be unavailable during an event.

iii. Each vice president is responsible for identification, development and maintenance of a disaster recovery plan for all decentralized systems, servers and critical workstations within his or her respective division.

B. Business Continuity

Business continuity plans shall be created to describe how departments and divisions will continue to perform their routine work and provide necessary services while the critical department or campus systems, networks and communications are unavailable and being restored.

Responsibilities

i. The director for Environmental Health and Safety is responsible for overseeing the University's business continuity business process.

ii. The associate vice president for Information Technology Services is responsible for publishing a redacted copy of the ITS Business Continuity Plan on the ITS website to inform the campus of ITS services that will be available or will be suspended during ITS disaster recovery.

iii. Each vice president is responsible for creating a business continuity plan for his or her respective division.

XV. Information Security Awareness Program

As required by CSU Information Security Policy 8035.0, "Information Security Training and Awareness", Information Technology Services is responsible for developing and delivering a multi-faceted security awareness program to provide appropriate training and awareness to all students and employees.

A. Information Security Training

i. The CSU Information Security Training was combined in 2018 with FERPA Training. All faculty and staff are required to take online FERPA training every two years and submit a renewal certificate of completion to Human Resources Management for continued access to the University network and systems.

ii. Technical Training. Information Technology Services technical employees are required by position description to participate in online, in-house or vendor-provided training programs as appropriate to maintain their technical knowledge and skill levels. A requirement for employee training must be incorporated into all technology procurements involving third-party service provider installations. ITS will provide awareness and training to campus Information Technology Consultants (ITCs) through a formal committee process. ITS will provide relevant technical support documentation to the campus-at-large through the ITS website.

iii. Information Security Program Training. The information security officer will conduct specialized training with managers, departments and/or service areas when new information security programs are established or changes occur to existing programs. (See Information Security Programs.)

B. Information Security Awareness

The following are acceptable methods for providing information security awareness to the University-at-large. The director of IT Security and Compliance is responsible for initiating information security awareness communications.

i. ITS Standards. Based on International Organization for Standardization (ISO) and CSU Policy, standards define relevant campus information security elements, such as business process security, hardware and software management, and Board of Trustees' audit compliance requirements, to ensure conformity, consistency and compliance with prescribed technology standards. Standards are publically available at ITS Standards.

ii. ITS User Guidelines. User guidelines explain specific typical steps for campus constituents to meet the requirements of federal and state laws and statutes, CSU Information Security Policy, Board of Trustees' audit requirements, ITS standards and information security best practices. User guidelines are publically available at ITS User Guidelines.

iii. Access to Relevant Legislation. ITS will maintain a website containing links to all relevant federal and state laws to which the University must comply.

iv. IT Security Website. IT Security and Compliance will maintain a web presence devoted exclusively to information security updates, programs, information resources, tips and current threats.

v. Alerts and Advisories. ITS will maintain an automated method for immediate notification of security threats. Users can view and follow *MyCalStateLA Tweets* via Twitter on the ITS home page.

vi. Student Event Participation. ITS will participate in organized student events to disseminate information on security awareness to students.

vii. Videos. ITS will create and display relevant information security videos targeted toward student awareness. Videos will be displayed at common student gathering locations, such as the ITS Help Desk, Open Access Labs (OALs) and on the IT Security website.