Information Security Roles and Responsibilities	Standard No.	ITS-2005-S	Rev:	
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	7-22-11	Effective:	7-22-11
				Page 1 of 23

Table of Contents

1 Purpose 2
2 Entities Affected by this Standard 2
3 Definitions 2
4 Standards 4
4.1 Delegations 4
4.2 Duties And Responsibilities 4
4.2.1 President 5
4.2.2 Vice President for Information Technology Services and Chief Technology Officer (VP ITS) 5
4.2.3 Information Security Officer (ISO) 5
4.2.4 University Counsel and Information Privacy Officer 7
4.2.5 Assistant Vice President of Human Resources Management 7
4.2.6 Judicial Affairs Officer 8
4.2.7 Assistant Vice President for Academic Personnel 8
4.2.8 Director of Procurement and Contracts 8
4.2.9 University Police 9
4.2.10 Property Management 9
4.2.11 Internal Audit 9
4.2.12 All Management Personnel Plan (MPP) employees 10
4.2.13 Identity Theft Department Administrators 11
4.2.14 Third-party Service Providers 11
4.2.15 Technical Service Providers 12
4.2.16 System Administrators 14
4.2.17 Application Developer Responsibilities 15
4.2.18 Data Stewards 15
4.2.19 Employees 16
4.2.20 Data Users 17
4.3 Committees, Groups and Teams 18
4.3.1 Executive Officers and Vice Presidents 18
4.3.2 ITS Advisory Committee 18
4.3.3 Information Technology Consultants Council 18
4.3.4 GET Leadership Team 18
4.3.5 Patch Management Committee 19
4.3.6 Campus Security Incident Response Team (CSIRT) 19
5 Contacts 19
6 Applicable Federal and State Laws and Regulations 20
7 Related Documents 21

1 Purpose

The purpose of this standard is to establish formal guidelines for assigning responsibility and duties related to managing and operating CSULA information systems and the Information Security Program.

Effective and efficient information security programs require clear direction for and commitment from members of the University. Involvement from all stakeholders to assess needs and risks, design processes to implement controls and measure program effectiveness as well as to enforce program criteria are needed.

The roles and responsibilities detailed herein are the foundation for information security, technology security and Information Security Program duties and responsibilities, and all campus constituents should use this document as a resource for developing and updating individual position descriptions.

2 Entities Affected by this Standard

This standard applies to all individuals who are responsible or have contact with University information including, among others, faculty, staff, students, administrators, third-party service providers, consultants, volunteer employees and users as well as groups that have information security responsibilities. The roles and responsibilities assigned in this standard impact the entire University.

3 Definitions

a. Application Developer: A user who usually performs the duties of a systems analyst or application programmer and has access to a University computing resource for the purpose of developing an application for use on that system or for any other system deemed appropriate and permissible.

b. Database Administrator: A person responsible for the physical design or management of a database.

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: 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 campus standards and guidelines.

e. Data User: Individuals who need and use University data as part of their assigned duties or in fulfillment of their role (e.g., employees, students, visitors, etc.)

f. Information Security Officer (ISO): The CSULA Information Security Officer is the director for IT Security and Compliance.

g. 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.

h. Level 2 Internal Use Data: Internal use data is information which 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.

i. 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.

j. Protected Data: A comprehensive term that includes both Level 1 and Level 2 classifications of information.

k. 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.

l. System Administrator: Individuals who manage, operate, support campus information systems or manage networks. Duties generally include installation, support of operating system and application software, security, troubleshooting and training.

m. Technical Service Providers: All employees classified in the Information Technology classification series (e.g., Analyst/Programmer, Operating Systems Analyst, Information Technology Consultant, Network Analyst, Equipment/Systems Specialist, and Operations Specialist).

n. Third-party Service Providers: Refers to an entity that is undertaking an outsourced activity on behalf of the University or is performing system administrator duties on their offsite system that contains University protected data (e.g., vendors, vendor's subcontractors, business partners, consultants, etc.).

4 Standards

The *CSU System-wide Information Security Standards* apply to all information assets governed by the system wide information security policies, including all information assets held and managed by CSULA. These CSU standards support and derive their scope from *the California State University System-wide Information Security Policy*. CSULA has developed Information Technology Services Standards as a campus-specific supplement to the CSU standards in order to delineate roles, responsibilities, procedures, business processes and requirements applicable to this campus. All CSULA standards support but do not supersede the *CSU System-wide Information Security Policy* or *CSU System-wide Information Security Standards*.

The following standards specify delegations and designate specific roles and responsibilities to implement and manage the CSULA Information Security Program.

4.1 Delegations

The Board of Trustees of the California State University (CSU) has delegated to the president the responsibility for establishing an information security program for CSULA, which is compliant and consistent with the CSU information policy and standards.

The president has delegated to the vice president for Information Technology Services and chief technology officer (CTO) the responsibility of overseeing the development, implementation, maintenance and enforcement of the University's Information Security Program and approval of the initial program and all subsequent changes to the program.

The vice president for Information Technology Services and chief technology officer has delegated to the information security officer (ISO) the responsibility for coordinating and overseeing the Information Security Program.

4.2 Duties And Responsibilities

The following individuals are responsible for the minimum duties identified below and may have duties and responsibilities in various categories. For example, administrative officials are also considered employees and data users. These roles and responsibilities must be included in individual position descriptions to ensure acknowledgement of and compliance with these requirements. Other duties may be assigned, as needed.

4.2.1 President

The president has the following responsibilities under the Information Security Program:

- Review and consider changes to the Information Security Program recommended by the vice president for Information Technology Services and chief technology officer.
- Review the annual Information Security Report presented by the CTO that includes an updated risk assessment and associated policy adjustments.
- Notify the Chancellor of a breach of security to California residents whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.
- Provide an annual current campus risk profile report to the Chancellor's Office.

4.2.2 Vice President for Information Technology Services and Chief Technology Officer (VP ITS)

The vice president for Information Technology Services and chief technology officer has the following responsibilities under the Information Security Program:

- Consult with the Information Security Officer regarding campus operations and systems to address security including the evaluation of risk to campus operations and systems and the development of procedures and processes.
- Notify the president and the assistant vice chancellor for Information Technology Services, Chancellor's Office, of a breach of security to California residents.
- Lead information technology (IT) staff in carrying out technology support for information security ensuring the security of all University information systems and protection of the confidentiality, availability, privacy and integrity of all data on such systems.
- Be an advisor to the president and his/her cabinet on all information security matters.
- Review and present to the president an annual Information Security Report that includes an updated risk assessment and associated policy adjustments.
- Present technology and information security projects, training initiatives, state and federal regulation changes to the ITS Advisory Committee for discussion.
- Review and approve the ITS Procurement Approval forms for all University procurements of computers, systems, technology equipment and software applications to ensure compliance with all security laws, regulations and policies.
- Grant exceptions to third-party contract security language and report such exceptions to the Information Security Officer and the director of Procurement and Contracts.

4.2.3 Information Security Officer (ISO)

The information security officer has the following responsibilities under the Information Security Program:

- Coordinate the Information Security Program on behalf of the VP ITS.
- Be an advisor to the VP ITS on all information security matters.
- Notify the VP ITS and the senior director of system wide information security management, Chancellor's Office, of a breach of security to California residents.
- Oversee campus information security self-assessment activities.

- Monitor and analyze reported security alerts.
- Chair the Campus Security Incident Response Team (CSIRT).
- Supervise the development, updating and deployment of the ITS Disaster Recovery Plan, ITS Business Continuity Plan and ITS Management Disaster Preparedness Plan.
- Serve as the campus Identity Theft Program Administrator.
- Oversee the campus information security awareness and training program.
- Develop and maintain a Plan of Action and Milestones (POAM) that describes campus information security initiatives.
- Provide input to the VP ITS on the campus budget process regarding prioritization and required resources for security risk mitigation activities and input regarding security risks of proposed projects.
- Respond to information security related requests during an audit.
- Serve as the campus representative on the CSU Information Security Advisory Committee.
- Establish and document a method for categorizing and assessing identified risks.
- Develop and present to the VP ITS an annual Information Security Report that includes a formal risk management plan with associated policy adjustments.
- Review and present monthly reports to coordinate security program changes with the ITS directors including violations of the security program and security policies.
- Serve on the ITS Change Management Committee.
- Appoint a representative from IT Security and Compliance to serve on the ITS Patch Management Committee.
- Assess the impact of new laws or regulations on the Information Security Program.
- Approve all changes to external network configuration and rule changes for firewalls and VPN connections. At a minimum, review firewall configuration rules and logs at least once per quarter.
- Administer user account and authentication management, including additions, deletions, and modifications. Ensure users are provided the minimum necessary access required to perform their duties.
- Review and approve or deny all system access requests as appropriate.
- Oversee the security program operations within the ITS division.
- Supervise periodic internal ITS audits and assessments to measure the effectiveness for the Information Security Program and internal security controls, and assist with coordination of the annual external security assessment performed by an independent security auditor.
- Ensure compliance with copyright protection for all software (internally developed and purchased) as outlined in *ITS-1016-G User Guidelines for Protecting Copyrighted Materials*.
- Assist the campus internal auditor in enforcing the document/media handling and disposal policy through a quarterly audit.
- Establish and maintain a third-party service provider management program with the assistance of the director of Procurement and Contracts to implement controls required to protect systems and data that are accessed by third-party service providers.

- Enforce the media/information classification program and review all requests for non-public information sharing.
- Investigate any potential or actual information security breaches.
- Ensure that all individuals with authorized access to protected information sign an acknowledgment to demonstrate both their receipt of CSU/campus information security policies and requisite training.
- Ensure that there is a method for self-review of network documentation such that each element is reviewed for accuracy and completeness at least once a year.
- Identify and communicate approved user practices for remote connections, approved methods and protocols for remote access, and a process for user reporting of suspected compromise of their remote device.
- Provide the guidelines for maintenance and annual review of an inventory of mobile devices authorized to contain protected Level 1 data.
- Identify and enforce a password change schedule as outlined in *ITS-5002-S Creating CMS/PeopleSoft User IDs and Passwords* and *ITS-2008-S Password Standards for Personal Systems*.

4.2.4 University Counsel and Information Privacy Officer

The University counsel and information privacy officer has the following responsibilities under the Information Security Program:

- Identify all laws and regulations that the organization needs to comply with regarding information security.
- Advise the ISO and the ITS department on information security compliance.
- Review and provide comment on proposed information security standards and guidelines.
- Along with the director of Procurement and Contracts, review agreement or contract language related to information security requirements.
- Coordinate and approve the University's response to public record requests covered under the Public Records Act.
- Review and approve as appropriate all requests for confidential IT information.
- File with the United States Copyright Office to serve as the University's designated agent to receive notifications of claimed infringement as specified under the Digital Millennium Copyright Act (DMCA).

4.2.5 Assistant Vice President of Human Resources Management

The assistant vice president of Human Resources Management has the following responsibilities under the Information Security Program:

- Establish appropriate background check standards for various positions and perform initial background checks in accordance with these standards.
- Ensure that the IT department is promptly notified of employee terminations, department transfers and pending terminations.
- Assist in the investigation of alleged security violations by individual staff to determine if disciplinary action is appropriate.
- Interpret, recommend and impose sanctions and discipline regarding information security violations in accordance with existing policy and practice.

4.2.6 Judicial Affairs Officer

The Judicial Affairs officer has the following responsibilities under the Information Security Program:

- Assist in the investigation of alleged security violations by students to determine if disciplinary action is appropriate.
- Interpret, recommend and impose sanctions and discipline regarding information security violations in accordance with existing policy and practice.

4.2.7 Assistant Vice President for Academic Personnel

The assistant vice president for academic personnel has the following responsibilities under the Information Security Program:

- Assist in the investigation of alleged security violations by individual faculty members or student academic employees to determine if disciplinary action is appropriate.

4.2.8 Director of Procurement and Contracts

The director of Procurement and Contracts has the following responsibilities under the Information Security Program:

- Along with the university counsel and the ISO, reviews information security agreement and contract language.
- Ensure that the following specifics are included in all agreements, contracts and service orders for those third-party service providers having access to systems and data and to campus offices and areas:
  - A clear description of the scope of services provided under the contract or purchase order.
  - Clause that indicates the information provided is protected and for the sole purpose of the specific business need for which the contract exists.
  - A protected information clause requiring the service provider to implement appropriate measures to safeguard protected information, including appropriate disposal after the intended use is satisfied, and restrictions from sharing any such information with any other party, unless authorized.
  - A clause requiring compliance with the CSU security policy and standards. Exceptions may only be granted by the VP ITS and must be reported to the ISO.
  - Clear identification of any and all types of protected data to be exchanged and managed by the third-party service provider.
  - A clause that requires the third-party service provider, or any of its subcontractors with whom it is authorized to share the data, to share only the minimum information necessary, protect accounts and passwords, securely return all information or certify destruction of information upon expiration of the contract, and provide immediate notification to the ISO whenever there is a breach of Level 1 Data and provide notification within a specified period of time of any security breaches associated with any other information.

- Notification to the vendor that liability for legal repercussions and expenses related to recovery or disclosure activities when information security incidents are caused by the third-party service provider may be incurred.
- A clause that requires the third-party service provider to abide by all legal standards and obligations of California Civil Code (Sections 1798.29, 1798.82, 1798.84, 1798.85), also referred to as SB 1386, and The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) when accessing or handling confidential University data, or working in areas where confidential data may be in use by others or otherwise exposed. The University interprets SB 1386 to include both electronic and written documentation.
- If appropriate, a provisions for CSU to have the ability to inspect and review third-party service provider operations for potential risks to CSU operations or data.

- Review and confirm appropriate administrators have conducted due diligence in determining the adequacy of the third-party service provider's system of safeguarding information prior to executing a contractual relationship with the third-party service provider.

4.2.9 University Police

University Police has the following responsibilities under the Information Security Program:

- Receive and investigate all reports of potential criminal law violations involving University information resources.
- Provide form *ITS-2804 Lost or Stolen Computer or Electronic Storage Device Report* to owners of stolen or lost desktop or laptop computers or electronic storage devices for completion at the time a theft report is filed. Include a copy of the report with the police report.
- Notify the ISO of all theft reports filed for stolen or lost desktop, laptop computers or electronic storage devices.

4.2.10 Property Management

The property management supervisor has the following responsibilities under the Information Security Program:

- Ensure departments complete a formal physical inventory of equipment at least every three years.
- Ensure that form *ITS-8830 Electronic Data Sanitization Verification* is included and correctly executed for the disposal of any equipment that may have contained protected data.

4.2.11 Internal Audit

The internal auditor has the following responsibility under the Information Security Program:

- Manage external information security assessments and audits performed by independent security auditors.

- Review quarterly reports of user access controls (*ITS-2824 Review of Decentralized Systems Access Controls*) from departments with decentralized systems.
- Conduct a campus wide risk assessment and compliance review of each of the "Relevant Areas" defined in the CSULA Gramm Leach Bliley Information Security Program.
- Ensure compliance with document and media handling and disposal policies by performing a quarterly audit with the assistance of the ISO.

4.2.12 All Management Personnel Plan (MPP) employees

Division vice presidents are the officers with primary responsibility for information collected, maintained or that has been identified as primarily utilized or "under stewardship" by their respective divisions. Management Personnel Plan employees have the following responsibilities under the Information Security Program:

- Ensure employees have completed any and all confidentiality compliance forms.
- Ensure employees have received appropriate training regarding computer security and the handling of information.
- Take corrective action to respond to issues identified by an information security review.
- Take appropriate measures for implementation of, and compliance with, the Information Security Program and applicable laws and regulations, policies and procedures, within their areas. Enforce specific information security controls applicable to respective areas and specific roles.
- Appoint an Identity Theft Administrator to oversee the department's red flag program for all departments that provide student loans and collects payment for services.
- Apply sanctions and discipline for security violations in accordance with existing policy and practice in coordination with Human Resources Management, Academic Affairs or Judicial Affairs.
- Support the ISO and the VP ITS in the reporting, investigating, assessing and resolution of potential or actual security violations. In the event protected data is stolen or otherwise compromised, the department or division is responsible for the notification to affected individuals and associated costs.
- Secure any information that is created, managed or stored, and for any information acquired or accessed from other University systems. This responsibility includes:
  - Classifying, handling and disposing of data in accordance with the information security standards.
  - Protecting essential records and information from loss, destruction and falsification.
  - Maintaining information as an asset of the University.
  - Completing periodic risk assessments.
- Periodically review all users' access levels to ensure they are still appropriate, and take appropriate action to correct discrepancies or deficiencies. Ensure employees have the access required, and only the access required, to perform their jobs.

- Notify Human Resources Management and the ITS Help Desk of any change in employment status (e.g., separation, department transfer) that impacts access requirements.
- Ensure that any parties who need to work in areas that may contain protected data and do not have an Information Confidentiality/Non-disclosure Agreement in place (e.g., contractual agreement) sign an Information Confidentiality/Non-disclosure Agreement.
- Complete a formal physical inventory of equipment at least every three years.
- Maintain and review annually an inventory of mobile devices authorized to contain protected data.
- Ensure all computers and electronic storage media are sanitized prior to re-deployment, disposal or donation.

4.2.13 Identity Theft Department Administrators

Under the Fair and Accurate Credit Transactions Act of 2003 (FACTA) 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. Since the University provides student loans and collects payment for some services, it is considered a creditor and the FACTA Red Flag Rules apply. Identity theft department administrators have the following responsibilities under the Identity Theft Prevention Program:

- Review and evaluate the methods utilized to open covered accounts and to allow access to covered accounts.
- Know about previous occurrences of identity theft.
- Ensure staff are aware of all red flags for each occurrence category.
- Develop, document, monitor and update internal business processes and procedures that detect, prevent and mitigate identity theft.
- Train staff on the department's internal procedures.
- Report red flag incidents to the director for IT Security and Compliance.

4.2.14 Third-party Service Providers

Third-party service providers such as vendors, vendor's subcontractors, business partners, and consultants having access to systems, data or campus offices and areas are subject to CSULA information security policies and have the following responsibilities under the Information Security Program:

- Require all of their employees having such access to sign an Information Confidentiality/Non-Disclosure Agreement to be granted access to any CSULA network, system or data.
- Ensure that information provided is protected and only used for the sole purpose of the specific business need for which the contract exists.
- Implement appropriate measures to safeguard protected information, including appropriate disposal after the intended use is satisfied and restrictions from sharing such information with any other party, unless authorized.

- Implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically managed information.
- Upon termination of services, return all information or certify destruction of information according to the agreement or specific terms of the contract.
- Protect accounts and password(s) and any other protection the account has, as well as reporting suspected misuse or information security incidents to the appropriate party.
- Abide by all CSULA security policies and legal standards and obligations of California Civil Code (Sections 1798.29, 1798.82, 1798.84, 1798.85), also referred to as SB 1386 and The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) when accessing or handling confidential University data, or working in areas where confidential data may be in use by others or otherwise exposed. The University interprets SB 1386 to include both electronic and written documentation.
- Share data with other parties only as authorized by the University and then share only the minimum information necessary. Protect accounts and passwords. Securely return or destroy the personal information upon expiration of the contract.
- Provide immediate notification to the campus whenever there is a breach of Level 1 Confidential Data. Any notifications of security breaches associated with all other information should be accomplished as outlined in the contract.
- Provide documentation to verify Payment Card Industry (PCI) compliance if collecting, processing, or transmitting credit card information.

Third-party service providers may also be required to follow other responsibilities (e.g., system administrator) depending on the services that they will be performing.

In the event of an information security incident caused by a third-party service provider, the entity may be held liable for legal repercussions and expenses related to recovery or disclosure activities.

4.2.15 Technical Service Providers

Technical service providers include all employees classified in the Information Technology classification series (i.e., Analyst/Programmer, Operating Systems Analyst, Information Technology Consultant, Network Analyst, Equipment/Systems Specialist, and Operations Specialist).

Technical service providers have the following responsibilities as required by their specific position description under the Information Security Program:

- Abide by federal and state laws, applicable regulations, CSU policies, CSULA standards, guidelines and procedures, and contractual agreements.
- Follow information security best practices for managing infrastructure and services.

- Deploy, manage and monitor technical security safeguards justified by the risk assessment. At a minimum, technical safeguards will include: perimeter security, access controls, vulnerability management, configuration management, virus protection and event log analysis and reporting.
- Recommend security procedures to end-users.
- Maintain current inventories of software licenses.
- Maintain daily troubleshoot logs.
- Monitor all systems for possible breaches of security policy.
- Maintain daily back-up systems and business continuation support.
- Develop and maintain documentation of the network structure and configuration in a form and format which is available for audit and review.
- Maintain an inventory of approved access control devices and review at least annually.
- Formally document a process for approving and testing configuration changes to networks and network control devices under the technical service provider's administration.
- Formally document network configurations that define all open ports and services.
- Document justification for any allowed service or protocol.
- Ensure public network jacks or wireless access points are not located on privileged networks or subnets.
- Develop and maintain processes for the routine identification, evaluation and application of software patches.
- Develop and maintain an inventory of information systems in a form and format which is available for audit and review.
- Establish and document a method for change management to manage changes to campus information assets.
- Ensure campus electronic media and hardware are located and stored in secure locations that are protected by appropriate physical and environmental controls. The level of protections provided by these controls must be commensurate with identified risks to the media and hardware.
- Appropriately label campus protected data and transport it via a delivery mechanism that can be tracked and provided to users only after being authorized by appropriate campus personnel.
- Develop backup schedules for electronic media.
- Develop and maintain appropriate procedures and processes for the acquisition, upgrade and maintenance of information systems.
- Conduct appropriate testing of all developed or procured applications and information systems before deployment in a production environment.
- Except where unavoidable, not use protected data for testing or development purposes.
- Test the information system's security controls.
- Remove all test data and test accounts before deploying an information system into a production environment.
- Establish procedures for the retention of log and monitoring information that are consistent with the CSU System-wide Records/Information Retention and Disposition Schedules.

- Establish methods for time synchronization of logging and monitoring activities.

4.2.16 System Administrators

System administrators are individuals who manage, operate or support campus information systems or manage campus networks.

System administrators have the following responsibilities under the Information Security Program:

- Offer service in the most efficient, reliable and secure manner while considering the needs of the total campus community.
- Abide by federal and state laws, applicable regulations, CSU policies, CSULA guidelines, standards and procedures and contractual agreements.
- Complete the appropriate access application, review and approval process for each system administered.
- Do not create system administrator access rights or share access rights with any other employees, students, vendors or guests who do not have these roles.
- Limit access to system administrator accounts and passwords and grant access only on a “need to know” basis.
- Notify the director of IT Security and Compliance or the VP ITS if being requested to perform an action that conflicts with federal or state laws, applicable regulations, CSU policies, CSULA guidelines, standards or procedures or contractual agreements.
- Ensure the availability, usefulness, integrity and security of the systems, data and networks being managed.
- Exhibit the highest level of professional ethical conduct.
- Before a server is installed and placed on a campus network, ensure that it is in an appropriate and compliant state to meet minimum baseline and security standards. In addition, all resource requirements (hardware and software) and system management requirements (people) for both current and future needs must be in place or planned for to ensure the machine remains in “top running order.”
- Ensure that all hardware and software products are installed and maintained in a manner consistent with license agreements.
- Monitor performance and capacity planning and intercede where needed to prevent misuse or misappropriation of system resources. Monitoring is required to ensure that system resources are not being misused.
- Monitor sources of system alerts and apply operating system and software product patches and security upgrades in a timely manner.
- Maintain necessary precautions to safeguard the systems against “corruption, compromise or destruction.” This includes performing scans for diagnostic problem resolution and/or assessing network traffic into or out of the systems.
- Avoid viewing the contents of a user's files or messages. If such content is exposed and becomes known to the system administrator, it should be treated as confidential and private.

- Take immediate action if information is uncovered that indicates a security breach has occurred. User accounts, services or systems cannot be capriciously shut down. However, in those instances where a suspected security incident will endanger the confidentiality, availability or integrity of both the system and the files and data of others, specific accounts may be shut down or access to services or systems closed that appear to be linked to the problem. Immediately after the emergency action is taken, the director of IT Security and Compliance must be notified and an appropriate review conducted to follow-up on the emergency action.
- Take reasonable and appropriate steps to see that all the terms of the hardware and software license agreements are faithfully fulfilled on all systems, networks and servers for which they are responsible.
- Based on campus guidelines or standards, management or lawful grounds, inspect, monitor and/or suspend access privileges determined to be necessary or appropriate in order to maintain the integrity of the computer system, network or protection of other users (e.g., hacking in progress, virus or spam attack, illegal video downloading blocking network traffic).
- Use the special access to information and other special computing privileges only in performing official duties. Such access shall not be used to satisfy idle curiosity. Access to users' information shall be governed by relevant University policies, procedures and guidelines as well as state and federal laws.
- Develop, test, maintain and document effective computer and network security procedures and take reasonable precautions to guard against corruption of software, damage to hardware or facilities, or unauthorized access. This includes installing system patches, security software and conducting periodic security audits as appropriate for the resource being managed. Systems should be configured to run only necessary system services which limits the potential vulnerability of the system.
- Develop appropriate backup procedures and disaster recovery plans.

4.2.17 Application Developer Responsibilities

Application developers have the following responsibilities under the Information Security Program:

- Apply data transfer methods that maintain the integrity and security of the data using encryption methods when applicable.
- Apply security patches and close security holes in applications when they are known.
- Test and fix applications for common security risks.
- Document codes so that others can maintain them.
- Document software installations so that others can perform maintenance.

4.2.18 Data Stewards

Data stewards have the following responsibilities under the Information Security Program:

- Specify and monitor the integrity and security of information assets and the use of those assets within their areas of program responsibility.

- Ensure that program staff and other users of the information are informed of and carry out information security and privacy responsibilities.
- Comply with any additional security policies and procedures established by the data owner of the information asset and the campus ISO.
- Notify the campus ISO of any actual or attempted violations of security policies, practices and procedures.
- Determine how an asset must be classified (i.e., Level 1, Level 2 or Level 3).
- Classify each data element or file type (e.g., SSN, DOB, charitable contributions), category of files (e.g., financial aid disbursements, grades, personnel data) or database (e.g., student administration, human resources management, contributor relations) for which he or she has stewardship responsibility in accordance with the need to control access to and preserve the security, integrity and retention of the file or database.
- Define controls for limiting access to and preserving the security and integrity of files and databases that have been classified as requiring such controls.
- Document an appropriate approval process before access or privileges are granted to campus information assets. All changes to user accounts on campus information systems or network resources must be approved by appropriate campus personnel. Such approval must be formally documented and retained for audit purposes.
- Authorize access to the information in accordance with the classification of the information and the need for access to the information.
- Ensure that those with access to the data understand their responsibilities for collecting, using and disposing of the data only in appropriate ways.
- Monitor and ensure compliance with CSU security policies, and campus standards, guidelines and procedures affecting the information.
- Advise the respective vice president of the information asset and the campus ISO of vulnerabilities that may present a threat to the information and of specific means of protecting that information.
- Work with the ISO, data user or other authorized individuals during the investigation and mitigation of information security incidents or breaches affecting the integrity and confidentiality of the data.
- At least annually, review, verify and revise as necessary user access rights to campus information assets. All such revisions must be tracked and logged following campus defined processes.

4.2.19 Employees

Employees are required to comply with security policies, procedures and practices established by the CSU, University, college, department and other units, and have the following responsibilities under the Information Security Program:

- Adhere to ITS user guidelines and standards currently in effect and posted at http://www.calstatela.edu/its/policies.
- Not store Level 1 and Level 2 confidential data on a mobile device unless encrypted, authorized by supervisor and reported to the ISO.
- Access protected information only as relevant and necessary to perform job-related duties. Under no circumstance may protected information be used for personal gain.

- Sign an Administration Systems Confidentiality Agreement which includes acknowledgement to comply with CSU and CSULA information security policies, standards, guidelines and procedures.
- Request investigations when there is evidence or reason to believe that a violation of security is occurring or has occurred.
- Retain and dispose of all data on campus hardware and electronic and non-electronic media in accordance with CSU Executive Order 1031.
- Participate in appropriate training regarding the security of information and sign a Training Document and Compliance Form, which is provided upon completion of online training.
- Not send unencrypted “protected data” over any network.
- Not remove University records from campus or the office where they are maintained unless in the performance of job duties and with the department administrator’s permission.

4.2.20 Data Users

A user has the following responsibilities under the Information Security Program:

- Comply with all federal, state and local laws pertaining to the protection of protected data as well as campus guidelines, standards and procedures meant to protect the security of campus information, computers and systems. Links to all applicable laws are available at http://www.calstatela.edu/its/policies.
- Use secure passwords to access any campus computer used to access the campus network.
- Protect the privacy of passwords. Do not share passwords with others. Accounts created for an individual are for the specific use by that individual only. Users are responsible for any use of their account.
- Request investigations when there is evidence or reason to believe that a violation of security is occurring or has occurred.
- Refrain from installing software that has the potential of compromising the security of the computer systems or the integrity of data.
- Use only those computing resources for which authorization has been issued. Do not attempt to obtain system privileges to which authorization has not been granted or give unauthorized access to others.
- Never attempt to intercept, capture, alter or interfere in any way with the normal transmission data on any computer or network, without prior authorization from the person or persons responsible for that resource.
- Work with the appropriate authorities in the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of their data.
- Not bypass or turn off anti-malware software installed on campus information systems unless appropriately authorized.
- Develop and implement controls to filter and limit unsolicited e-mail messages (e.g., spam).
- Not use University resources for illegal downloading and peer-to-peer file sharing of copyrighted works, including music, pictures, movies and other published materials.

4.3 Committees, Groups and Teams

The University relies on members of all campus committees to be liaisons for disseminating security information discussed at their meetings and soliciting feedback and suggestions from their constituents to bring back to the meetings or share on the mailing list associated with the committee on which they serve. The goal of all committees is to broaden the collaborative effort across all University divisions.

The following are committees in place as of this writing. The committee structure is flexible and will change in response to changing needs. These committees have specific responsibilities under the Information Security Program.

4.3.1 Executive Officers and Vice Presidents

These individuals are responsible for executive endorsement and top-down communications of the information security program.

4.3.2 ITS Advisory Committee

This committee has the following responsibilities under the Information Security Program:

- Informing, discussing and soliciting input regarding the status, impact and constituent communications for information security.
- Reviewing and approving, as appropriate, pending information security policies prior to executive review.
- Reviewing and approving, as appropriate, significant changes made to a campus-specific information asset.

4.3.3 Information Technology Consultants Council

This group will discuss information security as part of its review of operational issues and service improvements. The members of this group have a special responsibility for the protection of information assets outside the management of Information Technology Services. It has the following responsibilities under the Information Security Program:

- Ensuring that the assets managed by the schools, colleges and administrative units they represent are managed consistent with all requirements of the Information Security Program.
- Communicating all security concerns of the schools, colleges and administrative units that they represent to the assistant director of Baseline Services.

4.3.4 GET Leadership Team

The GET Leadership Team has the following responsibilities under the Information Security Program:

- Ensuring that the technical aspects meet the requirements of the Information Security Program.
- In accordance with CSU policy, conducting an annual review of general and technical user access to PeopleSoft applications and databases.
- Reviewing the security implications of and approving, as appropriate, significant changes made to a common or shared CSU information asset.

4.3.5 Patch Management Committee

The Patch Management Committee has the following responsibilities under the Information Security Program:

- Ensuring that all security software patches are evaluated, tested and deployed in a timely manner.
- Maintaining a log of dates, deployed patches and detailed explanations for software patches that are not deployed.

4.3.6 Campus Security Incident Response Team (CSIRT)

The primary responsibility of this committee is to prepare for and respond to information security and technology incidents and as such it is an integral part of the ITS planning process. This committee is chaired by the director for IT Security and Compliance/ Information Security Officer (ISO), and is comprised of two distinct teams – a technical team and an incident response team.

The technical team consists of specially-trained security analysts, senior network analysts, operations specialists and desktop specialists from ITS. The technical team provides planning feedback directly to the VP ITS regarding changing legislative requirements for information security; hardware and software requirements for intrusion detection and intrusion prevention; user awareness training; vulnerability assessments; patch management; log management; network traffic shaping; firewall management and forensic tools. In addition, members of the technical team participate in all ITS projects to ensure information security compliance and security best practices are incorporated during the planning and implementation phases.

The incident response team includes the technical team as well as representatives from Public Safety, Public Affairs, University Counsel, Human Resources and representatives from any affected division(s).

5 Contacts

a) For questions regarding specific department procedures, contact the department administrator or Information Technology Consultant (ITC).

b) Address questions regarding these standards to: ITSecurity@calstatela.edu.

c) An up-to-date list of approved encryption products is available at: http://www.calstatela.edu/its/desktop/encryptiontools/.

d) Instructions for WinZip file encryption are available at: http://www.calstatela.edu/encrypt.

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 This is 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/prdecember2000all8parts.pdf This is a federal law that protects the privacy of health records.
U.S. Copyright Office	**United States Digital Millennium Copyright Act** For a comprehensive summary, visit: http://www.copyright.gov/legislation/dmca.pdf The legislation implements two 1996 World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The DMCA also addresses a number of other significant copyright-related issues.
Fair Credit Reporting Act (FCRA)	**Fair Credit Reporting Act (FCRA), U.S. Code, Title 15 § 1681 et seq.** For the complete text as amended October 2001, visit: http://www.ftc.gov/os/statutes/fcra.htm This is the federal law that protects consumer credit and credit reporting.
Fair and Accurate Credit Transactions Act of 2003 (FACTA)	**Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Red Flag Rules** For the business alert summary, visit: http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm 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**
Government Code Sections 14740-14769	**State Records Management Act** http://www.leginfo.ca.gov/.html/gov_table_of_contents.html This is a state law that provides 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
Executive Order 1031	**System-wide Records/Information Retention and Disposition Schedules Implementation** http://www.calstate.edu/EO/EO-1031.html http://www.calstate.edu/recordsretention This Executive Order provides for the implementation of the California State University (CSU) System-wide Records/Information Retention Schedules.
CSU Information Security Policy	**The California State University System-wide Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.

ID/Control #	Title
ITS-1005-G	**User Guidelines for Portable Electronic Storage Media** http://www.calstatela.edu/its/policies/ This guideline is intended to help 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.
ITS-1006-G	**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.
ITS-1007-G	**User Guidelines for Laptop Security** http://www.calstatela.edu/its/policies/ This guideline outlines the steps for securing laptops and the personal, confidential or proprietary information contained on them.
ITS-1008-G	**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 laws and regulations regarding personal and confidential information when desktop or laptop computers and electronic storage devices are lost or stolen.
ITS-1016-G	**User Guidelines for Protecting Copyrighted Materials** http://www.calstatela.edu/its/policies/ This guideline outlines the steps the campus takes when receiving copyright infringement notifications, settlement letters or preservation notices from copyright holders or their representative agents.
ITS-1018-G	**User Guidelines for Identity Theft Prevention** http://www.calstatela.edu/its/policies/ This guideline establishes an 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.
ITS-1021-G	**User Guidelines for Data Sanitization** http://www.calstatela.edu/its/policies This guideline defines the appropriate data sanitization tools and procedures to meet security standards.

ID/Control #	Title
ITS-2017-G	**User Guidelines for Encryption Security** http://www.calstatela.edu/its/policies This guideline provides information on approved encryption algorithms, recommended encryption products and specific encryption tools and practices.
ITS 2804	**Lost/Stolen Computer/Electronic Storage Device Report** http://www.calstatela.edu/its/forms This form is used to report a lost or stolen computer or electronic storage device to University Police and IT Security and Compliance.
NA	**Administration Systems Confidentiality Agreement** http://www.calstatela.edu/its/policies/confidentiality.htm This document identifies rules related to access of Administration Systems and includes a signed acknowledgement