CSU The California State University: Working for California

THE CALIFORNIA STATE UNIVERSITY SYSTEM-WIDE INFORMATION SECURITY STANDARDS

Contact:

Cheryl Washington
Interim Senior Director, System-wide Information Security Management

The California State University
Office of the Chancellor
401 Golden Shore
Long Beach, CA 90802-4210
(562) 951-4190 phone
cwashington@calstate.edu

October 27, 2008

Acknowledgements

These standards were created through the contracted efforts of CH2M HILL, Inc. and Coalfire Systems. The work of their security professionals and management are greatly appreciated.

The development of these standards was expedited by utilizing the standards of other institutions to include all of the CSU campuses and the State of California (State Administrative Manual Chapter 5300).

We are grateful to all those participating through interviews, data collection, draft reviews, and various meetings, workshops, and consultations.

The support of the CSU faculty, ISOs, and CIOs was a critical element to this project.

Table of Contents

1.0 Introduction

The California State University (the CSU or the University) is a public institution committed to the ideals of academic freedom and freedom of expression. To promote these ideals, the CSU uses and offers access to a variety of information systems, data, and network resources, hereafter referred to as information assets. These standards support and provide additional guidance for those implementing *The California State University System-wide Information Security Policy*. The unauthorized collection, modification, deletion, disclosure, or misuse of CSU information assets can compromise the mission of the University, violate individuals' rights to privacy, or constitute a criminal act.

2.0 Scope

These standards support, and derive their scope from the California State University System-wide Information Security Policy.

3.0 Standards Management

The CSU System-wide Information Security Standards apply to all information assets governed by the system-wide information security policies.

These standards may be updated to reflect changes in the CSU's academic, administrative, or technical environments, or applicable state, federal, or international laws and regulations. The CSU's Senior Director for Information Security Management shall be responsible for coordinating the review and update of this document.

These standards may be supplemented, but not superseded, by additional standards adopted by each campus. These standards must be regularly reviewed and revised as necessary in order to ensure that it meets the CSU information security goals and requirements.

4.0 Information Security Roles and Responsibilities

4.1 Campus President

Each CSU campus President must establish an information security program, which is compliant and consistent with the CSU information security policy and standards. The details of each campus program are left to the President to determine, with the exception of items identified in the CSU information security policy and standards; these items are meant to provide some degree of consistency of approach and application.

- The President (or President designee) must identify the specific duties and responsibilities for the ISO, which, at a minimum, include those items identified below. While the role of the Information Security Officer (ISO) may be an additional duty, the President must ensure the appointee has sufficient time to carry out the assigned duties and responsibilities.
- The President may assign additional roles and responsibilities appropriate to the campus.
- Each President must review information security risks at least annually.
- Each President must annually provide a current campus risk profile report to the Chancellor's Office.

4.2 Chief Information Officer (CIO)

In addition to other duties as defined within the CSU, each campus CIO must:

- Work with the campus ISO to develop procedures and processes which implement the CSU information security policy and standards as directed by the campus President.
- Work with the campus ISO to evaluate the risk introduced by any changes to campus operations and systems.
- Consult with the ISO regarding campus operations and systems to address security.

4.3 Information Security Officer (ISO)

The ISO must:

- Coordinate the campus information security program on behalf of the President.
- Be an advisor to the President and his cabinet on all information security matters.
- Work closely with campus administrators and executive officers on information security matters.
- Oversee campus information security self-assessment activities.
- Inform the President (or President-designee) of significant risks as they are identified.
- Oversee the campus information security incident response program in coordination with appropriate campus personnel.
- Oversee the campus information security awareness and training program.
- Provide inputs to the campus budget process regarding prioritization and required resources for security risk mitigation activities and inputs 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.
- Avoid conflicts of interest by not having direct responsibility for information processing or technology operations for campus programs that employ protected information.

4.4 Campus Managers

4.4.1 Technical Management

IT management must ensure that:

- Information and information systems under their control are managed in compliance with CSU-wide and campus information security policies and standards.
- The campus ISO receives reports indicating the status of the procedures and practices used to implement the required security controls.

4.4.2 Program Management

Campus program managers (e.g., HR manager, registrar, privacy officer) are responsible for:

- Specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility.
- Ensuring that program staff and other users of the information are informed of and carry out information security and privacy responsibilities.

4.5 Data Owner

The responsibilities of a Data Owner consist of:

- Classifying each file or database for which he or she has ownership responsibility in accordance with the need to control access to and preserve the security and integrity of the file or database.
- Defining controls for limiting access to and preserving the security and integrity of files and databases that have been classified as requiring such controls.
- Authorizing access to the information in accordance with the classification of the information and the need for access to the information.
- Ensuring that those with access to the data understand their responsibilities for collecting, using, and disposing of the data only in appropriate ways.
- Monitoring and ensuring compliance with CSU/campus security policies and procedures affecting the information.
- Identifying for each file or database the level of acceptable risk.
- Working with the ISO, data user, data custodian/steward, and/or other authorized individuals during the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of the data.

The ownership responsibilities must be performed throughout the life cycle of the information asset, until its proper disposal. Individuals that have been designated owners of information assets must coordinate these responsibilities with the campus ISO.

4.6 Data Custodian/Steward

The responsibilities of a Custodian of an information asset consist of:

- Complying with applicable law and administrative policy.
- Complying with any additional security policies and procedures established by the Owner of the information asset and the campus ISO.
- Advising the owner 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.
- Notifying the Owner of the information asset and the campus ISO of any actual or attempted violations of security policies, practices, and procedures.

4.7 Data User

The responsibilities of a Data User consist of:

- Ensuring that he or she does not put any University data for which he or she has been given access at risk through his or her own actions.
- Working with the ISO, data authority, data custodian/steward, and/or other authorized individuals in the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of their data.
- Performing as appropriate other information security duties as required by other CSU policies, executive orders, and coded memorandums.

4.8 Senior Director for Information Security Management (SDISM)

The responsibilities of a SDISM consist of:

- Providing leadership for the overall CSU Information Security Program
- Ensuring the annual review and update of the CSU security policy and standards
- Maintaining the CSU Data Classification Standard
- Advising the Chancellor on matters regarding information security
- Providing support to information security staff at each campus

5.0 Information Risk Management

5.1 Risk Management

As appropriate, campuses must manage risks to their information assets. Each campus must establish an information security risk management program to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks. Specific risks that must be addressed include, but are not limited to: those associated with accidental and deliberate acts on the part of campus employees and outsiders; fire, flooding, and electric disturbances; and, loss of data communications capabilities.

The risk management process must include the following:

- Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.
- Identification of the campus information assets that are at risk, with particular emphasis on the applications of Information Technology (IT) that are critical to the campus operations or contain protected data.
- Identification of the threats to which the information assets could be exposed.
- Assessment of the vulnerabilities (i.e., the points where information assets lack sufficient protection from identified threats.)
- Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of the likelihood of such occurrence.
- Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level.
- Selection of cost-effective security management measures to be implemented.
- Preparation of a report, to be submitted to the campus ISO and to be kept on file within the campus, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of remaining risk to be accepted.

5.2 Risk Assessment

Each campus must regularly perform a formal, documented process that assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of campus information assets.

At a minimum, each campus' risk assessment process must include the following:

- Identification of impact and probability of threats to campus information assets.
- Prioritization of threats to campus information assets.
- Identification and prioritization of the vulnerabilities of campus information assets.
- Identification and definition of current security control measures used to protect the confidentiality, integrity, and availability of campus information assets.
- Assessment of the likelihood that a particular threat will exploit specific vulnerabilities on campus information assets.
- Identification of the potential impacts to the confidentiality, integrity, and availability of campus information assets if a particular threat exploits a specific vulnerability.

Campuses must establish and document a method for categorizing and assessing identified risks. An example follows, even though each campus may identify its own methods:

Likelihood of Occurrence

High – A threat is highly motivated and sufficiently capable, and controls to prevent a vulnerability from being exercised are ineffective.

Medium – A threat is motivated and capable, but controls are in place that may impede successful exercise of a vulnerability.

Low – A threat lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, a vulnerability from being exercised.

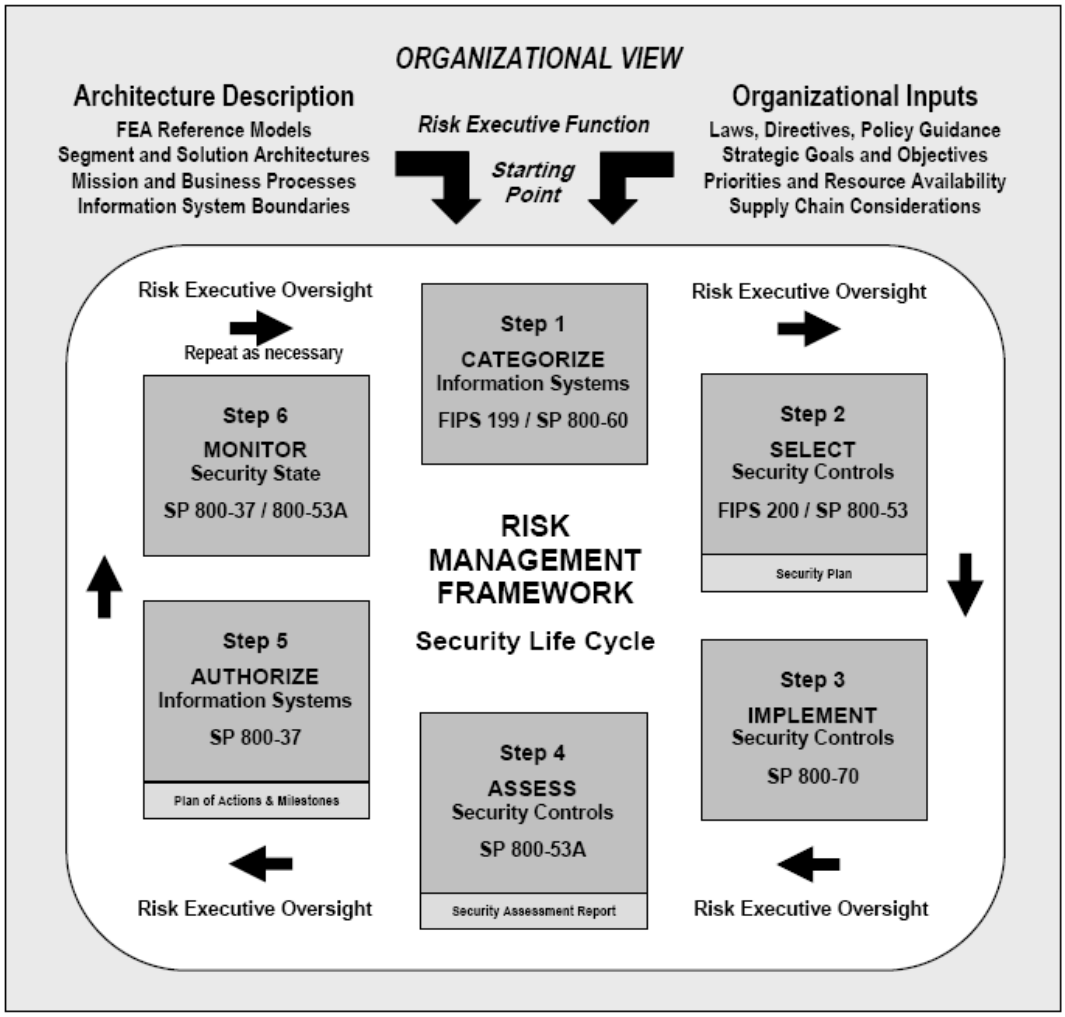
Magnitude of Impact

High – Exploitation of a vulnerability may (1) result in the highly-costly loss of major tangible assets or resources; (2) significantly violate, harm, or impede a campus' mission, reputation, or interest; or (3) result in human death or serious injury.

Medium – Exploitation of a vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.

Low – Exploitation of a vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

For additional information on performing a risk assessment, campuses are encouraged to refer to NIST SP 800-39 (draft) "Managing Risk for Information Systems". The "Risk Management Framework" diagram from that document is provided on the following page.



The risk analysis process must be carried out with sufficient regularity to ensure that the campus' approach to risk management is a realistic response to the current risks associated with its information assets.

5.3 Risk Management Plan

Each CSU campus must develop and regularly update a formal, documented, risk management plan that addresses at a minimum:

- Organization and Scope
- Risk management roles and responsibilities
- Campus leadership commitment
- Risk identification and tracking methodology
- Third party risk management
- Characterization of the campus' information systems based on their function and criticality

This plan does not have to be a separate document and may be combined with other campus planning documentation.

Each campus ISO must review the information security risks at least annually. Significant risks must be presented to the campus President (or his or her designee) for his action or acceptance.

Each campus must develop and maintain a Plan of Action and Milestones (POAM) that describes campus information security initiatives. For each initiative, the POAM must at least contain:

- Identified risk(s)
- Proposed Initiative(s)
- Initiative Owner/Point of Contact (POC)
- Resources Required
- Planned Completion
- Interim Milestones
- Status

On an annual basis, each campus President must submit an Information Security Risk Management Report to the Chancellor's Office. This report must identify the significant risks that have been identified during the past year, those which have been accepted (why and per what criteria), and those which are in the process of being mitigated. This report may be combined with other required risk-related reports.

The CSU Senior Director for Information Security Management (SDISM) must develop the format and process for the Information Security Risk Management Report.

6.0 Personnel Security

6.1 Employment Separations and Position Change

Based on established campus procedures, authorized CSU or campus managers must promptly notify the appropriate department(s) responsible for granting and revoking access privileges regarding all employee separations and job changes.

If an employee is separating from the University, the employee's access privileges (logical and physical) must be terminated by the employee's last day of employment, unless otherwise approved through proper campus procedures. By the last day of employment, an employee must return all campus- and/or CSU-supplied access devices to his or her manager. If an employee has used cryptography on data belonging to CSU and/or a campus, he or she must provide the cryptographic keys to the manager by the last day of employment.

If an employee is changing jobs, it is the responsibility of the employee's new manager (if the job change involves a management change) or existing manager to identify and define the access privileges needed by the employee to perform the new job.

A process for confirmation that logical and physical access privileges have been appropriately revoked or changed must be developed by the campus.

7.0 Security Awareness and Training

7.1 Campus Security Awareness and Training Program

Each campus ISO will be responsible for overseeing development and coordination of the campus information security awareness and training program. At a minimum, each campus program must include:

- Annual review and refreshing of content, if necessary.
- Annual acceptable use awareness training for students.
- Information security awareness training for new employees within a timeframe established by each campus.
- Annual information security awareness refresher training for all campus employees who interact with campus information assets.
- At least every two years, information security training for privileged users (e.g., system and security administrators) who interact with information systems containing protected data.
- At least every two years, information security training for the ISO and other managers who are responsible for developing and coordinating the campus information security program and controls.

Ongoing security awareness outreach for all persons who use or access campus information assets. Information security awareness and training activities must be recorded and available for internal audit.

Campuses must ensure that all individuals with authorized access to personal information sign an acknowledgment to demonstrate both their receipt of CSU/campus information security policies and requisite training.

7.2 Program Content

Each campus information security awareness and training program must include, as appropriate:

- Appropriate CSU and campus information security policies and standards.
- Significant campus information security controls or processes.
- User responsibilities and required actions.
- The secure use of campus information assets (e.g., log-on procedures, allowed protocols).
- Likely security threats to campus information assets.
- CSU and campus legal and regulatory responsibilities for protecting information assets.
- Information security best practices (e.g., how to construct a good password, how to prevent computer viruses).

8.0 Third Party Services Security

Campuses must ensure that when critical or protected information is shared with third parties, it is either specifically permitted or required by law and that a written agreement is executed between the parties that identifies the applicable laws, regulations, and CSU/campus policies, standards, procedures, and security controls that must be implemented and followed to adequately protect the information asset.

The agreement must also require the third-party, and any of its subcontractors with whom it is authorized to share the data, to share only the minimum information necessary, to securely return or destroy the personal information upon expiration of the contract, and to provide immediate notification to the campus, whenever there is a breach of Level 1 data.

8.1 Third Party Contract Language

When developing a contract, each campus must address the following:

- Include a clear description of the scope of services provided under the contract or purchase order.
- Clearly state the security requirements for the vendors to ensure that their work is consistent with the CSU security policy and standards.
- Require compliance with the CSU security policy and standards. Exceptions may only be granted by the campus President (or President-designee) and must be reported to the ISO.
- Clearly identify any and all types of protected data to be exchanged and managed by the vendor.
- Identify incident reporting requirements.
- Require immediate notification of any security breaches associated with Level 1 information.
- Require notification within a specified period of time of any security breaches associated with all other information.
- If appropriate, make provisions for CSU to have the ability to inspect and review vendor operations for potential risks to CSU operations or data.

9.0 Information Technology Security

9.1 Network Controls Management

Each CSU campus must develop and maintain documentation of its network structure and configuration. At a minimum, the following information must be included:

- IP address management
  - Static IP address assignments
  - Dynamic address server (i.e., DHCP) settings showing:
    - Range of IP addresses assigned
    - Subnet mask, default gateway, DNS server settings, WINS server settings assigned
    - Lease duration time
- Network topology information containing:
  - The locations and IP addresses of all segments, subnets, and VLANs.
  - Identification of any established security zones on the network and devices that control access between them.
  - The locations of every network drop and the associated switch and port on the switch supplying that connection.
  - All subnets on the network and their relationships including the range of IP addresses on all subnets and net mask information.

  - All Wide Area Network (WAN) or Metropolitan Area Network (MAN) information including network devices connecting them and IP addresses of connecting devices. A summary representation (e.g., drawing) of the logical design appropriate for managerial discussions.
  - A summary representation (e.g., drawing) of the logical design appropriate for managerial discussions.
  - A summary security model appropriate for managerial discussion.
- Configuration information on at least the following network devices:
  - Switches
  - Routers
  - Firewalls
  - Any other device important to the functioning of the network
- Configuration information for devices must include but not be limited to:
  - IP address
  - Net mask
  - Default gateway
  - DNS server IP addresses for primary and secondary DNS servers
  - Any relevant WINS server information
  - Any other pertinent information related to device
  - Responsible administrator contact information
- Network connection information must include:
  - Type of connection to the Internet or other WAN/MAN.
  - Provider of Internet/WAN/MAN connection and contact information for sales and support.
  - Configuration information including net mask, network ID, and gateway.
  - Physical location where the cabling enters the campus and circuit number.

Each campus may determine its specific methods for documentation using any combination of online network tools, databases, or hard copies; however, the resulting information must be in a form and format which is available for audit and review. Each campus must establish a method for self-review of network documentation such that each element is reviewed for accuracy and completeness at least once a year.

9.2 Remote Access

Public access systems are those made available to the public via the internet, requiring no special access or authentication process. Examples include, but are not limited to: campus informational web pages and class schedule information. Non-public access systems are those which are available only after authentication or other special access process. Examples include, but are not limited to: online courses, class registration web pages, and internal campus email systems.

All remote access (wired or wireless) to non-public campus information assets must:

- Be authorized and authenticated by use of a unique user identifier.
- Pass through a campus-approved access control device (e.g., a firewall or access server).
- Be made using an approved method (e.g. campus-authorized remote desktop service).
- Use a secure encrypted protocol.

- Be logged and user activity tracked consistent with campus procedures implementing logging standards.

Remote access to non-public CSU-shared resources (e.g., CMS) must, at a minimum, meet the same access criteria described above for campus information systems and data.

Campuses must identify and communicate:

- Approved user practices for remote connections.
- Approved methods and protocols for remote access.
- A process for user reporting of suspected compromise of their remote device.

Campus mechanisms for remote access must include an appropriate method for terminating inactive or inappropriate remote connections.

An inventory of approved access control devices must be maintained by each campus and reviewed at least annually.

9.3 Mobile Device Management

As determined necessary by risk assessment, campus-provided mobile devices must be protected with appropriate security controls. Appropriate security controls can include, but are not limited to: access control, encryption, strong passwords, anti-virus software, and/or personal firewall.

Protected Level 1 data may not be stored on a mobile device unless authorized by appropriate campus administration and encrypted via campus-provided method. Each campus must maintain an inventory of mobile devices which are authorized to contain protected Level 1data.

Campuses must identify and communicate approved user practices for mobile device security and a process for users to report if they determine or suspect that any mobile device or a non-campus-provided (i.e., personal) mobile device which enables access to non-public campus information assets has been lost, stolen, or compromised.

9.4 Boundary Protection and Isolation

Campus networks must be protected at all ingress and egress points by a device or devices which permit only authorized inbound and outbound traffic; all other traffic must be blocked. The campus must appropriately separate network access to public information system resources from those which store protected Level 1 and Level 2 information. Campuses must establish zoning or separation within its internal networks based on established trust relationships, authorized services, and data classification in order to ensure that protected information is not made available to unauthorized persons.

All unnecessary services (e.g., Web server, SNMP) on any campus border device must be disabled. All management connections across a network to campus border devices must be encrypted and authenticated. Direct management connections (i.e., console connections) do not require encryption.

Each campus must have:

- A formal, documented process for approving and testing configuration changes to its network and network control devices.
- Formal, documented network configurations that define all open ports and services.
- Documented justification for any allowed service or protocol.

Protocols known to carry substantial risk of exploit (e.g. telnet, FTP) may be allowed only after risk analysis and justification. Border device configurations and rule sets must be reviewed and revised, as necessary, at least annually.

9.5 Malicious Software Protection

All campus information systems of the type commonly affected by malicious software must have current versions of campus approved software ("anti-malware software") capable of detecting, removing, and protecting against malicious software, including viruses, spyware, and adware.

Such software must scan all data in "real time", including data, which is both stored and received by the information system. Such scanning must take place before data files are opened and before software is executed. The software must be capable of tracking and reporting significant actions taken by the software (e.g., deleted or quarantined malware).

Anti-malware software must check for and install updates and signatures at least daily.

Unless appropriately authorized, users must not bypass or turn-off anti-malware software installed on campus information systems.

Each campus must develop and implement controls to filter and limit unsolicited e-mail messages (e.g., spam).

9.6 Logging Elements

Each campus must identify and implement appropriate logging and monitoring controls for its information assets. These controls must take into consideration the technical capabilities of each resource.

At a minimum and as appropriate, such controls must track and log the following events:

- Actions taken by any individual with root or administrative privileges
- Changes to system configuration
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Alarms raised by an access control system
- Activation and de-activation of controls, such as anti-virus software or intrusion detection system.
- Changes to, or attempts to change system security settings or controls

For each of the above events, the following must be recorded, as appropriate:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Data accessed
- Program or utility used
- Origination of event (e.g., network address)

- Protocol
- Identity or name of affected data, information system or network resource

Each campus must establish procedures for the retention of log and monitoring information which must be consistent with any CSU data retention schedules.

Critical servers, at a minimum, must store a copy of their log data on another device; this copy must be protected from unauthorized access.

Each campus must establish methods for time synchronization of logging and monitoring activities.

9.7 Secured Infrastructure

Public network jacks or wireless access points (WAP) at campuses must not be located on privileged networks or subnets.

9.8 Patch Management

Each campus must develop and maintain processes for the routine identification, evaluation, and application of software patches. These procedures and processes must include:

- Methods for checking with vendors and other resources for available patches.
- Methods for testing and evaluating available patches.
- A method for generating a status report useful to determine whether or not vulnerable systems have been patched.
- Methods for making a recommendation to apply a patch. If the recommendation is not to install a patch (particularly a security related patch), then the rationale must be documented and reviewed by the campus ISO for inclusion in the campus risk management process.
- A nominal timeline for the patching process.

9.9 Information System Inventory Management

Each campus must develop and maintain an inventory of information systems. At a minimum, the inventory must include:

- System name
- Operating system and version
- Applications
- Installed patches (both OS and application)
- Administrator(s)

Each campus may determine its specific methods for creating and maintaining the inventory. The inventory may exist among multiple reports, data stores, or tools; however, the resulting information must be in a form and format which is available for audit and review.

10.0 Change Control

Campuses must establish and document a method for change management to manage changes to campus information assets.

The process must include:

- Identification and documentation of changes.
- Assessment of the potential impact of changes, including security implications.
- Identification of a change control authority, which may be vested in either individuals or groups as appropriate.
- Documented review and approval by the designated change control authority.
- Methods for scheduling and appropriate notification of significant changes.
- Methods and standard template for notification to end users of scheduled changes and expected impact.
- Ability to terminate and recover from unsuccessful changes.
- Testing procedures to ensure the change is functioning as intended.
- Communication of completed change details to all appropriate persons.
- Updating of all appropriate system documentation upon the completion of a significant change.

Significant changes made to a common or shared CSU information asset (e.g., CMS) must be appropriately reviewed and approved by a centralized CSU change control oversight group.

Significant changes made to a campus-specific information asset must be appropriately reviewed and approved by the designated change control authority.

While each campus may identify its own change control methods, an example follows:

	Low Impact Changes	Medium Impact Changes	High Impact Changes
Description of Change	A change intended to repair a fault in an information system or network resource. Such changes can include either the hardware or software components of information systems and network resources.	A change intended to update or upgrade an information system or network resource. Such changes can include major patches or significant changes to system configuration to meet a new policy, security guideline, or campus requirement. Such changes can include either the hardware or software components of information systems and network resources.	A change, which will result in major changes to an information system or network resource. Such changes can include implementing new functions or replacing entire systems. Such changes can include either the hardware or software components of information systems and network resources.

	Low Impact Changes	Medium Impact Changes	High Impact Changes
Pre-change Requirements	A change plan, including back-out procedures, must be developed and approved.	A formal risk assessment must be conducted on the change. A change plan, including back-out procedures, must be developed and approved.	A formal risk assessment must be conducted on the change. A change plan, including back-out procedures, must be developed and approved. Information systems or network resources that are being changed must be fully backed up.
Approval Required	• System owner • IT manager	• System owner • IT manager (may include ISO and TSO) • Change control group	• System owner • IT manager (may include ISO and TSO) • Change control group
Post-change Requirements	After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated.	After the change is made, appropriate information system or network resource documentation, operations processes and configuration documentation must be updated. Change results must be logged and reported to change control group.	After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated. Change results must be logged and reported to change control group.

11.0 Access Control

Access to campus information assets must include a process for documenting appropriate approvals before access or privileges are granted. All changes to user accounts (i.e., account termination, creation, and changes to account privileges) on campus information systems or network resources (except for password resets) must be approved by appropriate campus personnel. Such approval must be formally documented.

11.1 Access Authorization

Campuses must identify and document individuals who are authorized to define and approve user access to campus information assets. Campuses must document their authorization procedures. Authorizations must be tracked and logged following campus defined processes and must include information such as:

- Date of authorization
- Identification of individual approving access
- Description of access privileges granted
- Description of why access privileges granted

11.2 Granting Access

Authentication controls must be implemented for campus information assets. Campus-defined controls must take into consideration:

- Validating user identity prior to granting access to system resources or data.
- Uniquely identifying users and their corresponding access privileges.
- Denying all access rights until rights are formally assigned.
- Detecting and warning about repeated failed access attempts.
- Allowing access rights to be promptly modified or revoked.
- Allowing authentication credentials to be regularly changed.

11.3 User Account Management

Unless otherwise authorized, all users of campus information assets must be identified with a unique credential that establishes identity. This unique credential must not be shared with others except where authorized as an exception to this standard. User credentials must require at least one factor of authentication (e.g., token, password or biometric devices).

Campuses must establish criteria for disabling inactive user accounts on campus information systems or network resources. The period of acceptable inactivity must be based upon the results of a risk assessment.

All "guest" or generic accounts on campus information systems or network resources must be disabled or removed unless specifically authorized based upon the results of a risk assessment.

Campuses must establish criteria for disabling user accounts on campus information systems or network resources after five (5) failed logon attempts.

Campuses must establish processes for re-enabling or resetting user accounts once they have been disabled. User identity must be appropriately verified prior to re-enabling or resetting user accounts. If automated, these processes must take into consideration potential risk to determine the lockout time.

System administrators of campus information systems and network resources must have individual user accounts on the information systems and network resources they administer or use utilities such as "sudo" or "Run As" to perform system administration tasks. System administrator accounts must not be used for non-administrative uses (e.g., browsing the Web while logged in as administrator).

Campuses must establish criteria for creating application or system-level access accounts. These accounts must be assigned appropriate stewards and reviewed annually.

Unless specifically authorized, workstation administrator accounts must not be used for non-administrative purposes.

11.3.1 Password Management

Campuses must identify and communicate acceptable password criteria. The criteria may vary by system or application at the campus' discretion based upon a risk assessment.

For strong passwords the following minimum characteristics are required:

- Minimum length is eight (8) characters
- Must contain at least three (3) out of the four (4) following character types:

- At least one uppercase alphabetic character (A-Z)
- At least one lowercase alphabetic character (a-z)
- At least one special character
- At least one number (0-9)

Campuses must identify and communicate a password change schedule. The schedule may vary by system or application at the campus' discretion based upon a risk assessment. A sample schedule follows:

- Passwords with administrative access to Level 1 or Level 2 data must be changed every 90 days.
- Passwords with ability to create application transactions (e.g., create purchase requisitions, approve purchase requisitions, create general ledger transactions) must be changed every 180 days.
- Password reuse must be restricted to no more than once every four (4) uses.
- First-time passwords (e.g., passwords assigned by IT administrators upon account creation or during password resets) must be set to a unique value per user and changed immediately after first use.

Campus information systems and network resources must not display, transmit, or store passwords in clear text.

11.4 Access Modification

At least annually, appropriate campus managers, data stewards, and/or their designated delegates must 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 and must at least include:

- Date of revision
- Identification of person performing the revision
- Description of revision
- Description of why revision was made

11.5 CSU PeopleSoft Access Review

In accordance with CSU policy, campuses are required to conduct an annual review of general and technical user access to PeopleSoft applications and databases. The intent of the review is to verify the following:

- Access privileges assigned to users are based on a need to access the information in order to perform their job duties.
- Administrative access to production environments granted to technical personnel during an upgrade or implementation are removed at the conclusion of the project.
- Only authorized faculty and administrative personnel have the ability to modify grades.
- Individuals are granted authority to override matching rules as is appropriate for their job function.
- Passwords for system accounts are tightly controlled.
- Campuses have appropriately segregated duties between individuals with full access to make changes to applications, databases or programs.

The PeopleSoft applications include reports to facilitate this review. These reports identify users and the access rights they have been assigned. Periodic reviews of these reports must confirm authorized users only have access to the minimum set of privileges needed to perform their job functions. Additionally, CMS has the following documents available on its web site to aid in the conduct of the reviews:

- ***PeopleSoft Security: User Access Rights Validation Process Guide*** – identifies best practices and provides a recommended set of processes and tools for the performance of periodic reviews.
- ***Guidelines to Secure PeopleSoft Data***
- Some technical personnel are granted system administrative access to the PeopleSoft production environments during an upgrade or implementation. Campuses must ensure this access is removed at the conclusion of the upgrade or implementation.
- Within the Student application, only authorized faculty and administrative personnel have the ability to modify grades. Campuses must regularly review user rights to change grades to ensure this access right is appropriate and necessary.
- Select individuals on campuses may have been granted the ability to override matching rules in the Finance application. Campuses must regularly review these access privileges to determine if they are appropriate and necessary.
- Campuses must complete a ***Certification of Annual Systems Access Review*** form. This is an acknowledgement by each campus Vice President that the review has been conducted in conformity with the CSU's policy requirement.
- Campuses must complete a ***Report of Annual Systems Access Review Cover Sheet***. This document records the date(s) the review was conducted, the name(s) of the person(s) performing the review, and the description(s) of the review process employed by the campus.
- Campuses must complete a ***Schedule of Findings***. This is a two part report:
  - **Part 1** – Reports all exceptions noted as a result of reviewing each user's access rights.
  - **Part 2** – Allows campuses to address issues stemming from KPMG's interim procedures, specifically segregation of duties and password security. Campuses must report their progress on resolving issues and the corrective actions taken on all issues.
- The completed documentation must be sent to the Chancellor's Office.

12.0 Asset Management

Each campus must provide for the integrity and security of its information assets by identifying ownership responsibility, as defined with respect to the following:

- Owners of the information within the campus.
- Custodians of the information.
- Users of the information.
- Classification of information to ensure that each information asset is identified as to its information class in accordance with law and administrative policy.

12.1 Data Ownership

Campuses must assign ownership of each information asset containing Level 1 or Level 2 protected data. Normally, responsibility for automated information resides with the manager of the campus program that

employs the information. When the information is used by more than one program, considerations for determining ownership responsibilities include the following:

- Which program collected the information.
- Which program is responsible for the accuracy and integrity of the information.
- Which program budgets the costs incurred in gathering, processing, storing, and distributing the information.
- Which program has the most knowledge of the useful value of the information.
- Which program would be most affected, and to what degree, if the information were lost, compromised, delayed, or disclosed to unauthorized parties.

12.2 Data Classification

The designated owner of an information asset is responsible for making the determination as to how an asset must be classified (e.g., Level 1, Level 2, or Level 3). Data stored on campus hardware or media (both paper and electronic) must be classified per CSU's *Data Classification Standard* listed in Appendix A of this document.

12.2.1 Use of the CSU Data Classification Standard

Campuses may elect to move or add data elements from one classification level to another classification level with higher protection requirements, but never to a classification level with lower protection requirements. For example, a data element classified as Level 2 can be moved to a Level 1 classification but it cannot be moved to a Level 3 classification.

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

12.2.2 Maintaining the CSU Data Classification Standard

The CSU's Senior Director for Information Security Management (SDISM) must determine what data will be designated Level 1 data and must identify appropriate minimum controls.

The SDISM must establish a process for the review and maintenance of the data classification standard. The SDISM must review the classification standard on an annual basis.

12.3 Data Handling

Data owners are responsible for determining special security precautions that must be followed to ensure the integrity, security, and appropriate level of confidentiality of their information. Data stored on campus hardware or media must be appropriately labeled and protected according to its classification.

When Protected Level 1 data is electronically sent, it must be sent via a method that uses strong encryption.

When Protected Level 2 data is electronically sent, it must be protected using approved campus processes.

12.4 Data Storage

Each campus must develop and implement appropriate controls for securing critical or protected data stored, distributed, or accessed on electronic media and hardware. These controls must ensure the confidentiality, integrity, and availability of the asset.

Campus electronic media and hardware must be 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.

Campus protected data must be appropriately labeled, transported via a delivery mechanism that can be tracked, and provided to users only after being authorized by appropriate campus personnel.

12.5 Data Retention

All data on campus hardware and electronic and non-electronic media must be retained and disposed of in accordance with CSU Executive Order 1031.

Information that has been identified as or is reasonably believed to be relevant to an existing or potential legal proceeding must be retained while the matter is ongoing. The appropriate campus management must notify the individuals and/or IT organizations holding the information as to its eligibility for retention or disposition.

12.6 Data Backup

Campuses must develop backup schedules for electronic media.

Information systems or files that contain critical or protected data must be backed up using a schedule which is based on the value of the information asset.

Transportation procedures for backup media containing protected data must be documented and reviewed annually.

Backups of campus electronic media, records of the backup copies, and documented restoration procedures must be stored in secure locations with an appropriate level of physical and environmental protection.

12.7 Encryption

When encryption is used to protect campus information systems, data, or network resources, the following minimum requirements must be met:

- Strong cryptography (e.g., Triple-DES, AES, etc.,) must be used. The cryptography must be certified by NIST or a similar organization.
- Documented procedures and responsibilities for key management must be established. The procedures must address key rotation, key storage, key selection, key escrow, and key handling.

12.7.1 Data in Transmit

As deemed necessary, protected information must be transmitted using encryption measures strong enough to minimize the risk of the information's exposure if intercepted or misrouted.

12.7.2 Data in Storage

Encryption of information in storage presents risks to the availability of that information, due to the possibility of encryption key loss. Therefore, the use of encryption must take into account the nature of the information resources and the University's requirements for their timely or continued availability.

Records subject to the disclosure under the California Public Records Act or required to be accessible for defined periods of time in compliance with CSU records disposition schedules shall be available to appropriate University officials at all times. Other information that may be required to conduct the University's business shall also be available when needed. Therefore, at least one copy (the authoritative

copy) of any such information shall be stored in a known location in unencrypted form, or if encrypted, the means to decrypt it must be available to more than one person.

12.8 Media Re-use

Protected data stored on campus electronic media and hardware must be securely and thoroughly erased before such items can be re-used. Such data must be sanitized using campus-approved erasure tools or services.

12.9 Data Disposal

Assets containing protected information must be sanitized prior to disposal. The sanitization process must remove all information from media such that data recovery is not possible. The sanitization process must comply with appropriate environmental, health and safety regulations.

Campus electronic and non-electronic media and hardware which contains protected data no longer required for legitimate organizational purposes must be disposed of according to Executive Order 1031 but be consistent with any pending litigation holds. The following disposal methods must be used:

- Non-electronic media must be cross-cut shredded, incinerated, or pulped.
- Electronic media must be purged, degaussed, shredded, or otherwise physically destroyed so that the protected data cannot be reconstructed. If a data deletion program is used for protected Level 1 data, it must write random data.
- Campus back-up (e.g., tape, optical) media must be physically destroyed or degaussed.

Campuses must track the disposal of equipment which may have contained protected data. At a minimum, such tracking must identify:

- Date of disposal
- Description of items to be disposed
- Name and title of person(s) performing the disposal

13.0 Management of Information Systems

Each campus must develop and maintain appropriate procedures and processes for the acquisition, upgrade, and maintenance of information systems. At a minimum, these procedures and processes must include methods for:

- A needs assessment and justification for development or procurement.
- Definition of requirements for functionality, performance, reliability, interoperability with other information systems, security, and recovery prior to start of development or procurement.
- Identification of security risks, development of associated security controls, and documentation of resulting residual risk.
- Determination of the classification of data being processed.
- Determination of user access being provided.
- Identification, coordination, and approval of security requirements.
- Protection of campus data during development and testing.
- Documentation and validation of security controls.

- Secure transition to operations to include back out planning.
- Routine inspection to ensure the configuration integrity of the operational environment.
- Secure disposition and disposal of information systems and data at their end of life.
- A clear separation of duties between development, test, and production environments for critical systems or those containing protected level 1 information.
- Use of secure coding guidelines (e.g., OWASP, SCARE, SPSMM).
- Appropriate change control.

Campuses must conduct appropriate testing of all developed or procured applications and information systems before deployment in a production environment. Such applications and information systems must be appropriately documented prior to deployment in a production environment.

As determined necessary by risk assessment, application code created by a campus must be appropriately reviewed before being used in a production environment.

13.1 Web Application Coding

Web software applications created by campuses must be developed per secure coding guidelines such as the Open Web Application Security Project (OWASP) guidelines. Before being placed into a campus production environment, such applications must be reviewed and tested to ensure that the following vulnerabilities are addressed:

- Un-validated input
- Inadequate access control
- Inadequate authentication and session management
- Cross-site scripting (XSS) attacks
- Buffer overflows
- Injection flaws
- Improper error handling
- Insecure storage
- Denial of service
- Insecure configuration management

13.2 Using Protected Data in Non-Production Environments

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

13.3 Testing Security Controls

Campuses must test the information system's security controls. This test must verify the controls are working properly and must be conducted prior to deploying the system into a production environment. Campus must document the test plan(s) and test results. Previously deployed systems must be tested as part of any significant upgrade or as may determined by risk assessment.

13.4 Deployment into Production Environments

Campuses must remove all test data and test accounts before deploying an information system into a production environment. Once in the production environment, campuses must conduct regular risk assessments to ensure the system has security controls that appropriately protect the confidentiality, integrity and availability of the system.

Protected data must not be displayed in any user documentation.

14.0 Information Security Incident Management

Proper incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents. In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences.

Each campus must develop incident management plans and procedures that address, at a minimum, the following:

- **Computer Security Incident Response Team (CSIRT)** – Each campus shall identify the positions responsible for responding to an incident.
- **Protocol for escalation and internal reporting** – Campus procedures shall outline the method, manner, and progression of internal reporting, so as to ensure that:
    - Appropriate campus officials are informed about appropriate security incidents.
    - The CSIRT is assembled.
    - The incident is addressed in the most expeditious and efficient manner.
- **Protocol for security incident reporting** – Any actual or suspected breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately.

14.1 Investigating

Each campus must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. For the purposes of this standard, incidents include, but are not limited to, the following:

- **Data** (includes electronic, paper, or any other medium):
    - Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any Level 1 or Level 2 data.
    - Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
    - Deliberate or accidental distribution or release of personal information by a campus, its employee(s), or its contractor(s) in a manner not in accordance with law or CSU/campus policy.
    - Intentional non-compliance by the custodian of information with his/her responsibilities.
- **Inappropriate Use and Unauthorized Access** – This includes tampering, interference, damage, or unauthorized access to campus computer data and computer systems. This also includes, but is not limited to: successful virus attacks, web site defacements, server compromises, and denial of service attacks.

- **Equipment** – Theft, damage, destruction, or loss of campus IT equipment, including laptops, tablets, integrated phones, personal digital assistants (PDAs), or any electronic devices containing or storing confidential, sensitive, or personal data.
- **Computer Crime** – Use of a campus information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.
- **Any other incidents that violate campus policy**.
- Each campus must document and develop appropriate procedures and processes for investigating information security events and incidents.

14.2 Evidence Collection and Handling

Each campus must develop and maintain procedures and processes for evidence handling. At a minimum, the campus must address its access to forensic resources (either internal or through external arrangements) and its criteria for contacting law enforcement.

If a campus chooses to maintain its own forensic capability, the campus must maintain procedures and processes for:

- A method for labeling all items to include:
  - Date/time collected
  - Name and contact information for collection agent
  - Location of collection
  - Unique identification scheme
  - Detailed description of the item
- A method for logging all evidence collected
- Identification of a secure location for evidence storage
- A method for tracing evidence custody to include at a minimum the following information:
  - Date/time evidence removed from storage
  - Date/time evidence returned to storage
  - Name/contact information of handler
  - Disposition of evidence (e.g., forensic exam or court)

14.3 Incident Reporting

Each campus must formally define a point of contact (POC) for information security incident reporting. A campus POC can be an individual (e.g., ISO) or an organization [e.g., IT Help Desk or Computer Security Incident Response Team (CSIRT)]. A formal, centralized method (i.e., email or phone number) for reporting information security incidents to campus POCs must be provided to users.

Each campus must identify and communicate means for users and third parties to report suspected incidents. This information must be part of routine security awareness activities. Any user who observes or suspects that an information security incident is occurring with a campus' information systems, data, or network resources must promptly report the incident to the campus' POC. Third parties who observe or suspect that an information security incident is occurring with a campus's information systems, data, or network resources must promptly report the incident to their campus business contact. A user must not prevent or obstruct another user from reporting an information security incident in the above manner.

Each campus' POC must implement feedback processes to ensure that those reporting information security incidents are appropriately acknowledged.

14.4 Internal Notifications

Each campus must inform the Chancellor's Office of any security incidents requiring notification of users (e.g., violations of California information privacy laws). The notification process must include the following steps:

- The campus President must contact the Chancellor.
- The campus ISO must contact the Senior Director of Information Security Management.
- A description of the incident must be sent to the SDISM.
- If the incident will be made public, then the campus must:
  - Prepare a press release
  - Send the press release to the SDISM

15.0 Physical and Environmental Security

Physical and environmental security controls prevent unauthorized physical access, damage, and interruption to campus' information assets. Campus controls must be adequate to protect critical or protected data. Such controls must:

- Manage control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by campus staff and outsiders.
- Prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

15.1 Security Zones

Each campus must regularly review its physical areas and identify them per the table below.

Zone	Brief Description	Necessary Controls
Public	No critical systems are located in the area.	None. Access to this area can be unrestricted.
Shared Access	An area containing at least one critical system. Persons in the area of the system include those who do not have authorization to the system or the information it contains.	Appropriate physical access controls and construction must be implemented to restrict access from the public area to the Campus Limited Access Area. Access to the Campus Limited Access Area must be limited to only persons having a need for specific access in order to accomplish a legitimate task.
Campus Limited Access Area	An area containing one or more critical systems. Persons accessing the area are limited to those who have authorization to the system or the information it contains. All others are restricted.	Appropriate physical access controls and construction must be implemented that limit access to the area to only persons having a need for specific access in order to accomplish a legitimate task. The controls must enforce the principles of need to know and least possible privilege.

Zone	Brief Description	Necessary Controls
		All physical access to such areas must be tracked and logged. At a minimum, such tracking and logging must provide: • Date and time of access • User ID performing access Visitors to such areas must sign a visitor's log prior to being granted physical access. The log must document the visitor's name, the authorizing employee, the date and time for ingress, and egress and purpose of access.

15.2 Work Area Security

Campuses must establish and communicate user guidelines for securing protected data in work areas. This includes data in electronic and non-electronic form. The guidelines must address:

- Not leaving protected data unattended.
- Limiting the viewing of protected data from unauthorized users.
- Time based application or system locking.

15.3 Viewing Controls

Once logged into, campus information systems that can access protected data must not be left unattended or unsecured. Activation of automatic locking software or log off from the systems must occur when information systems are unattended for more than 20 minutes.

The display screens for all campus information systems that have access to protected data must be positioned such that data cannot be readily viewed by unauthorized persons (e.g., through a window, by persons walking in a hallway, or by persons waiting in reception or public areas). If it is not possible to move a display screen to meet the above requirement, a screen filter must be used.

15.4 Data Center Access

An entry system must record the date, time, and identification of all persons entering a campus data center. Data center walls, doors, and windows must be constructed with sufficient strength to deter entry by an intruder. Cameras must monitor and record the date and time of all entry and exit points of a campus data center. Recording must be retained for at least two weeks before being overwritten.

Appendix A – CSU Data Classification Standard

Classification	Description	Examples
Level 1 Confidential	Confidential Information is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential information is information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result is severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU's reputation, and legal action could occur. Level 1 information is intended solely for use within the CSU and limited to those with a "business need-to know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information.	• Passwords or credentials • PINs (Personal Identification Numbers) • Birth date combined with last four digits of SSN and name • Credit card numbers with cardholder name • Tax ID with name • Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name • Social Security number and name • Health insurance information • Medical records related to an individual • Psychological Counseling records related to an individual • Bank account or debt card information in combination with any required security code, access code, or password that would permit access to an individual's financial account • Biometric information • Electronic or digitized signatures • Private key (digital certificate) • Vulnerability/security information related to a campus or system • Attorney/client communications • Legal investigations conducted by the University • Third party proprietary information per contractual agreement • Sealed bids
Level 2 Internal Use	Internal use information 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.	**Identity Validation Keys (name with)** • Birth date (full: mm-dd-yy) • Birth date (partial: mm-dd only) **Student Information-Educational Records** (Excludes directory information) including: – Grades – Courses taken – Schedule – Test Scores – Advising records – Educational services received – Disciplinary actions

Classification	Description	Examples
	Non-directory educational information may not be released except under certain prescribed conditions.	Non-directory student information may not be released except under certain prescribed conditions **Employee Information** Including: • Employee net salary • Employment history • Home address • Personal telephone numbers • Personal email address • Payment History • Employee evaluations • Background investigations • Mother's maiden name • Race and ethnicity • Parents and other family members names • Birthplace (City, State, Country) • Gender • Marital Status • Physical description • Photograph **Other** • Library circulation information. • Trade secrets or intellectual property such as research activities • Location of critical or protected assets • Licensed software
Level 3 Public	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. Level 3 information may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.	**Campus Identification Keys** • Campus identification number • User ID (do not list in a public or a large aggregate list where it is not the same as the student email address) **Student Information** • Educational directory information (FERPA) **Employee Information (including student employees)** • Employee Title • Status as student employee (such as TA, GA, ISA) • Employee campus email address • Employee work location and telephone number • Employing department

Classification	Description	Examples
	Publicly available data may still subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.	• Employee classification • Employee gross salary • Name (first, middle, last) (except when associated with protected data) • Signature (non-electronic)