CSU The California State University: Working for California



# THE CALIFORNIA STATE UNIVERSITY SYSTEM-WIDE INFORMATION SECURITY POLICY

**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

This policy was 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 this policy was expedited by utilizing the policies 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 committed to protecting the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the University. This policy and associated standards provides direction and support to campuses for information security in accordance with University requirements and relevant laws and regulations. The CSU information security practices are designed to promote and encourage appropriate use of information assets and are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the University's core mission and campus academic and administrative purposes.

# 2.0 Scope

The Board of Trustees (the Board) of the California State University is responsible for protecting the confidentiality, integrity and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the integrity of the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act. It is the collective responsibility of all users to ensure:

- Confidentiality of personally identifiable information.
- Integrity of data stored on or processed by CSU information systems.
- Availability of information stored on or processed by CSU information systems.
- Maintenance and currency of applications installed on CSU information systems.
- Compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection.

The CSU retains ownership (or stewardship) of information assets owned (or leased) by the CSU or entrusted to the CSU. The CSU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across CSU network services, monitoring actions on the CSU information systems, checking information systems attached to the CSU network for security vulnerabilities, disconnecting information systems that have become a security hazard, or restricting data to/from CSU information systems and across network resources.

This policy shall apply to the following:

- All campuses, including auxiliary units, and external business or organizations that provide goods or services to the CSU.
- Central and departmentally-managed information assets.
- All students, faculty, staff, and consultants employed by the CSU or any other person having access to CSU information assets.
- All categories of information, regardless of the medium in which the information asset is held (e.g. paper, electronic, oral, etc).
- Information technology facilities, software, and equipment (including personal computer systems) owned or leased by the CSU.

This policy may be supplemented, but not superseded, by additional policies and standards adopted by each campus. Policies, standards, and implementation procedures referenced in this policy must be developed by each campus through consultation with campus officials and key stakeholders.

# 3.0 Policy Management

This policy shall be updated to reflect changes in the CSU's academic, administrative, or technical environments, or applicable federal/state laws and regulations. The CSU Information Security Management Department shall be responsible for overseeing an annual review of this policy.

# 4.0 Establishing an Information Security Program

Each campus must establish an *information security program* that contains administrative, technical and physical safeguards designed to protect campus information assets. Each campus information security program must implement a risk-based layered approach that uses preventative, detective, and corrective controls to provide a reasonable level of information security. The campus program must:

- Assign development and management responsibilities for the information security program, including the appointment of an Information Security Officer (ISO).
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held (e.g. paper, electronic, oral, etc.).
- Develop risk management strategies to identify and mitigate threats and vulnerabilities to information assets.
- Establish and maintain an incident response plan.
- Maintain ongoing security awareness and training programs.
- Comply with applicable laws, regulations, and CSU policies.

The campus President is delegated responsibility for implementing an effective information security program. The Assistant Vice Chancellor for Information Technology Services shall exercise the equivalent responsibilities with regard to the Chancellor's Office information security program. The information security program must be reviewed at least annually.

# 5.0 Organizing Information Security

Information security roles and responsibilities need to be identified and defined to achieve security objectives and mitigate risk on each campus. Each campus is responsible for developing, implementing, and documenting the campus organizational structure that supports the University's information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program. Each campus information security organization structure must be reviewed at least annually.

Each President (or President-designee) must appoint a campus ISO.

# 6.0 Information Security Risk Management

Risks to information assets must be actively managed in order to prioritize resources and remediation efforts. Risk management involves the identification and evaluation of risks to information security assets (***risk assessment***) and the development of strategies to reduce the risk to acceptable levels (***risk mitigation***). Campuses must develop risk management processes that identify and assess risks to its information assets and reduce such risks to acceptable levels. The campus risk management processes must be used continuously to ensure that risks to information assets are addressed in a timely manner.

## 6.1 Risk Assessment

Risk assessments are part of an ongoing risk management process. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls.

Individuals designated as owners of critical or protected information assets must develop a schedule for conducting continuous risk assessments of campus information asset. The asset owner must document the frequency of the assessment, risk assessment methodology, result of the risk assessment, and mitigation strategies designed to address identified risks.

## 6.2 Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing appropriate risk-reducing activities recommended as a result of the risk assessment process. Since the elimination of all risk is impossible, campus leadership must balance the cost and effectiveness of the proposed risk-reducing activities against the risk being addressed. Appropriate mechanisms to safeguard information should be selected relative to the security objectives determined by the risk assessment. Controls selected to mitigate risks should include administrative, operational, technical, physical, and environmental measures as appropriate. Mitigation strategies must ensure the confidentiality, integrity, and availability of information assets and be commensurate with risks identified by risk assessments.

For those risks where the risk mitigation strategy involves the use of controls, these controls must ensure that risks are reduced to an acceptable level, taking into account:

- Legal and regulatory requirements and compliance.
- University operation and policy requirements and constraints.
- Cost of implementation, maintenance, and operation.

Each campus must develop and maintain a method for documenting and tracking decisions related to risk mitigation activities.

## 6.3 Reporting Information Security Risks

The ISO must complete a comprehensive risk assessment of all critical and protected assets at least every two years. The comprehensive report should include a description of the methodology used to conduct the comprehensive risk assessment, the results of the risk assessment, and the campus mitigation strategies for addressing each identified risk. The comprehensive report must be certified by the campus President (or his/her designee).

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, those which have been identified during the past year, those which have been accepted (including why and what criteria), and those which are in the process of being mitigated.

# 7.0 Privacy

All users of CSU information technology resources are advised to consider the open nature of information disseminated electronically, especially since the CSU is a public entity, and should not assume any degree of privacy or restricted access to information they create or store on CSU systems. No CSU information system or network resource can absolutely ensure that unauthorized persons will not gain access to community member information or activities. However, the CSU acknowledges its obligation to respect

and protect private information about individuals stored on CSU information systems and network resources.

## 7.1 Collection of Personal Information

In order to comply with state and federal laws and regulations (e.g., Title V, FERPA, California Public Records Act), the CSU may not collect personal information unless the need for it has been clearly established in advance.

Where such information is collected:

- The campus will use reasonable efforts to ensure that personal information is adequately protected from unauthorized disclosure.
- The campus shall store personal information when it is appropriate and relevant to the purpose for which it has been collected.

## 7.2 Access to Personal Information

Except as noted elsewhere in CSU policy, information about individuals stored on CSU information systems may only be accessed by:

- The individual to whom the stored information applies or their designated representatives.
- Authorized CSU employees with a valid CSU-related business need to access, modify, or disclose that information.
- Appropriate legal authorities.

However, appropriate authorized CSU personnel who have followed established campus procedures may access, modify, and/or disclose information about individuals stored on CSU information systems or a user's activities on CSU information systems or network resources without consent from the individual. For example, CSU may take such actions for any of the following reasons:

- To comply with applicable state, federal or international laws or regulations.
- To comply or enforce applicable CSU policy.
- To ensure the confidentiality, integrity or availability of CSU information systems, data, or network resources.
- To respond to valid legal requests or demands for access to CSU information systems, data, or network resources.

If CSU accesses, modifies, and/or discloses information about an individual and/or their activities on CSU information systems or network resources, it will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by CSU policy or applicable laws.

Campuses are advised to consult the CSU *Records Access Manual* to determine which records must be made available for public inspection under the California Public Records Act.

## 7.3 Access to Electronic Data

Individuals who store personally identifiable information (e.g., social security numbers) must use due diligence to prevent unauthorized access and disclosure of confidential, private, or sensitive information.

Browsing, altering, or accessing electronic messages (e.g., email or text) or stored files in another user's account, computer, or storage device (e.g., disks, USB drives) is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for CSU business reasons. This prohibition does not affect:

- Authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individual's job duties.
- Campus response to subpoenas or other court orders.
- Campus response to a request pursuant to public record disclosure laws.

# 8.0 Personnel Security

All users are expected to employ security practices as appropriate to their responsibilities and roles. Users who access protected data must sign a confidentiality (non-disclosure) agreement. This agreement must be regularly renewed.

## 8.1 Employment Requirements

As part of an effective security program, potential employees must be informed of their information protection obligations and their trustworthiness to handle protected information must be considered. Positions involving access to protected information and positions of trust must consider requirements for background checks. Campus personnel procedures must address these elements.

## 8.2 Separation or Change of Employment

Campuses must implement procedures to revoke access upon termination, or when job duties no longer require a legitimate business reason for access, except where specifically permitted by University policy and by the data owner.

Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the University, information system privileges, including all internal, physical, and remote access, must be promptly disabled or removed.

Procedures must be implemented to ensure proper disposition of electronic information resources upon termination.

Electronic and paper files must be promptly reviewed by an appropriate manager to determine who will become the data steward of such files and identify appropriate methods to be used for handling the files.

If any electronic information resources are subject to a litigation hold, the department must ensure preservation of relevant information before final disposition of electronic information resources.

Campuses must verify that items granting physical access such as keys and access cards are collected from the exiting employee. Any access list that grants the exiting employee physical access to a secured campus limited-access area must be updated appropriately to reflect the change in employment status.

Information system privileges retained after separation from the University must be documented and authorized by an appropriate campus official.

# 9.0 Security Awareness and Training

Each campus must implement a program for providing appropriate information security awareness and training to its employees. The campus information ***security awareness*** program must promote campus

strategies for protecting information assets. All employees must participate in security awareness training. When appropriate, information ***security training*** must be provided to individuals whose job functions require specialized skill or knowledge in information security.

## 9.1 Security Awareness

The security awareness program must provide an overview of campus information security policies, and help individuals recognize and appropriately respond to threats to campus information assets. The program must promote awareness of:

- CSU and campus information security policies, standards, procedures, and guidelines.
- Potential threats against campus information assets.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of information assets.

After receiving initial security awareness training, employees must receive follow-up awareness training annually to reflect changes in information security policy and standards.

## 9.2 Security Training

When necessary, the campus information security program must also provide or coordinate training for individuals whose job functions require special knowledge of security threats, vulnerabilities, and safeguards. This training must focus on expanding knowledge, skills, and abilities for individuals who are assigned information security responsibilities.

# 10.0 Managing Third Party Service Providers

Third party service providers must be required to adhere to campus information security policies and standards. A risk assessment must be conducted to determine the specific implications and control requirements for the service provided.

# 11.0 Information Technology Security

Campuses must develop and implement appropriate technical controls to minimize risks to its information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical information systems and protected data from threats.

## 11.1 Malicious Software Protection

Each campus must have procedures in place to effectively detect, prevent, and report malicious software. Electronic data received from untrusted sources must be checked for malicious software prior to being placed on a CSU network or information system.

## 11.2 Network Security

Campuses must appropriately design and segment their networks—based on risk, data classification, and access—in order to secure their information assets. Each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that traverses or resides on the campus network. Campus processes for transmitting or storing critical and protected data must ensure confidentiality, integrity, and availability.

## 11.3 Mobile Devices

Campuses must develop and implement controls for securing protected data stored on mobile devices. Critical or protected data must not be stored on mobile devices unless effective security controls have been implemented to protect the data. Campuses must use encryption, or equally effective measures, on all mobile devices that store critical or protected data. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by a designated campus official. Other effective measures include physical protection that ensures only authorized access to the information asset.

## 11.4 Information System Logs

Campuses must implement logging and monitoring controls on appropriate information systems and network resources. Activity records created by logging and monitoring controls must be reviewed regularly. Server administrators are required to regularly scan, remediate, and report un-remediated vulnerabilities to the system owner or application administrator within a prescribed timeframe. The risk level of a system determines the frequency at which logs must be reviewed. Campus systems must complete a periodic, but not less than annual, risk assessment to ensure they follow the appropriate monitoring requirements. Risk factors to consider are:

- Criticality of business process.
- Information classification associated with the system.
- Past experience or understanding of system vulnerabilities.
- System exposure (e.g., services offered to the Internet).

Access to logging and monitoring data must be protected from unauthorized access. Campuses must ensure that individuals are granted access to data generated from log and monitoring files based on a need to know.

Data generated by logging and monitoring must be retained for a period of time that is consistent with effective use, CSU records retention schedule, regulatory, and legal requirements such as compliance with litigations holds.

# 12.0 Configuration Management

Campuses must develop and implement configuration standards to ensure that information technology systems, network resources, and applications are appropriately secured to protect confidentiality, integrity, and availability.

# 13.0 Change Control

Changes to information technology systems, network resources, and applications need to be appropriately managed to ensure they do not introduce unexpected vulnerabilities or adversely impact existing security protections. Campuses must establish and document a method to manage changes to campus information assets. The process must evaluate the information security impact of changes by taking a risk-based approach to change control.

Changes to critical assets or assets containing protected data will likely require a more rigorous review than changes to non-critical assets. Changes to critical information assets or assets containing protected data must be made in accordance with a formal, documented change control process. Changes which may

impact the security of critical information assets must be identified along with the level of control necessary to manage the change.

Campuses should define and publish the scope of "significant" changes to campus information assets in order to be sure that all affected parties have adequate information to determine if a proposed change is subject to the change management approval process.

## 13.1 Emergency Changes

Only properly authorized persons may make an emergency change to campus information systems, data, or network resources. Emergency changes are defined as changes which, due to urgency or criticality, need to occur outside of the campus' formal change management process. Such emergency changes should be appropriately documented and promptly submitted, after the change, to the campus' normal change management process.

# 14.0 Access Control

On-campus or remote access to critical or protected information assets must be based on operational and security requirements. Appropriate controls must be in place to safeguard unauthorized access to critical and protected information assets. This includes not only the primary operational copy of the information asset, but also data extracts and backup copies.

Campuses must have a documented process for provisioning approved additions, changes, and terminations of access rights and reviewing access of existing account holders. Authorized users and their access privileges should be specified by the data owner, unless otherwise defined by CSU/campus policy.

Access to campus critical information assets and protected data must be denied until specifically authorized.

## 14.1 Granting Access

Access to campus critical information assets and protected data may be provided only to those having a need for specific access in order to accomplish an authorized task and must be based on the principles of need-to-know and least privilege. Authentication controls must be implemented for access to campus critical information assets and protected data.

Authentication credentials used for access to campus critical information assets and protected data must be unique to each individual and may not be shared unless authorized by appropriate campus management. Where approval is granted for shared authentication, the requesting organization must be informed of the risks of such access and the shared account must be assigned a designated owner. Shared authentication privileges must be regularly reviewed and re-approved at least annually.

## 14.2 Granting Access to Third Party Service Providers

Third party service providers may be granted access to campus information assets only when they have a need for specific access in order to accomplish an authorized task. This access must be authorized by an appropriate campus official and based on the principles of need-to-know and least privilege.

Access to campus information assets by third party service providers must not be allowed until it has been authorized, appropriate security controls have been implemented, and a contract/agreement has been signed defining the terms for access.

## 14.3 Segregation of Duties

The principles of separation of duties should be followed when assigning job responsibilities relating to restricted or essential resources. Campuses must maintain an appropriate level of segregation of duties when issuing credentials to individuals who have access to critical information assets and protected data. Campuses must avoid issuing credentials that allow a user to have excessive authority over critical assets or protected data.

## 14.4 Access Review

Campuses must develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate campus managers and data owners must review, at least annually, user access rights to critical information assets. The results of the review must be documented.

### 14.4.1 Access Review – PeopleSoft Applications

Campuses must perform an annual review of access granted to general and technical users of the PeopleSoft application and production databases to determine whether continuing access is necessary and appropriate. The results from the review must be documented using the guidelines provided in the CSU *PeopleSoft Access Review Standard*.

### 14.4.2 Access Review - Privileged Account Holders

Supervisors or other employees must periodically review the system administration work of personnel with access to privileged accounts on shared servers. Such action is intended to provide a periodic audit or review for those system administration functions that are not otherwise audited or reviewed in the course of being completed.

## 14.5 Modifying Access

Modifications to user access privileges must be tracked and logged. Users experiencing a change in employment status (e.g., termination or position change) must have their logical access rights reviewed, and if necessary, modified or revoked.

# 15.0 Information Asset Management

Campuses must maintain an inventory of their information assets containing critical or protected data. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction. Campus must develop and maintain a data classification standard that meet or exceeds the requirements of the CSU *Data Classification Standard*.

The designated owner of the information asset is responsible for:

- Classifying the information asset according to the campus Data Classification Standard.
- Defining security requirements that are proportionate to the value of the information asset.
- Managing the information asset according to the requirements described in the campus Information Asset Management Standard.

Data should not be transferred to another individual or system without approval of the data owner. Before critical or protected data is transferred to a destination system, the data owner should establish agreements to ensure that authorized users implement appropriate security measures.

# 16.0 Information Systems Acquisition, Development, and Maintenance

Campuses must integrate information security requirements into the software development life cycle of information systems that are critical to the University or information systems that contain protected data. The security requirements must identify controls that are needed to ensure confidentiality, integrity, and availability. These controls must be appropriate, cost-effective, and mitigate risks that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of the information asset.

# 17.0 Information Security Incident Management

Campuses must develop and maintain an incident response program that includes processes for investigating, responding, reporting, and recovering from incidents involving loss, damage, misuse of information assets, or improper dissemination of critical or protected information, regardless of the medium in which the breached information is held (e.g. paper, electronic, oral). The campus program must:

- Designate specific personnel to respond to information security incidents in a timely manner.
- Include procedures for documenting the incident, determining notification requirements, implementing remediation strategies, and reporting to management.
- Include processes to facilitate the application of lessons learned from incidents.
- Support the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences.

The campus incident response plans must be tested annually and comply with the CSU Information Security Incident Management Standards.

When a campus determines an incident must be reported to individuals or the media, the campus must immediately notify the Chancellor and Senior Director of Systemwide Information Security Management.

# 18.0 Physical Security

Each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where critical or protected assets are stored. Campuses must protect these areas from unauthorized physical access while ensuring that authorized users have appropriate access. Campus information assets stored in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. The level of protection provided must be commensurate with that of identifiable risks. Campuses must document physical access to limited-access areas and review these access rights annually.

# 19.0 Business Continuity and Disaster Recovery

An information security program needs to support the maintenance and potential restoration of operations through both minor and catastrophic disruptions. Campuses must ensure that its critical information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users. Each campus must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event. The program must be in compliance with the CSU *Executive Order 1014*.

# 20.0 Compliance

The CSU shall, in consultation with the CSU legal staff and other subject matter experts, regularly identify and define laws and regulations that apply to CSU information assets. The CSU shall provide this information to campuses as it develops. Campuses must develop and maintain information security policies and standards that comply with applicable laws and regulations and the CSU policies that apply to campus information assets.

# 21.0 Policy Enforcement

The CSU respects the rights of its employees and students. In support of this policy, campuses must establish procedures which assure that investigations involving employees and students suspected of violating this policy are conducted in a fair and equitable manner. These procedures must comply with appropriate regulations (e.g., California Education Code and Title V), collective bargaining agreements, and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

The University reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of University resources or to protect the University from liability.

Allegations against employees that are sustained may result in disciplinary action. This action may only be administered in a manner consistent with the terms of the applicable, collective bargaining agreements in accordance with the applicable provisions of the California Education Code, and/or civil and criminal prosecution. Student infractions of this policy may be referred to the Office of Student Judicial Affairs. Third party service providers who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements.