



CALIFORNIA STATE UNIVERSITY, SACRAMENTO

INFORMATION SECURITY POLICY

ADOPTED FROM THE CSU SYSTEM-WIDE INFORMATION SECURITY POLICY

Jeff Williams
Information Security Officer
California State University, Sacramento
Information Security Office
6000 J Street
Sacramento, CA 95819-6065
(916) 278 -1999

Table of Contents

1.0 Introduction	3
2.0 Scope	3
3.0 Policy Management	4
4.0 Establishing an Information Security Program	4
6.0 Information Security Risk Management	5
6.1 Risk Assessment	5
6.2 Risk Mitigation	5
6.3 Risk Transference	5
6.4 Risk Acceptance	6
6.5 Risk Monitoring	6
6.6 Reporting Information Security Risks.....	6
7.0 Privacy of Personal Information.....	6
7.1 Collection of Personal Information	6
7.2 Access to Personal Information	7
7.3 Access to Electronic Data	7
8.0 Personnel Security	8
8.1 Employment Requirements	8
8.2 Separation or Change of Employment.....	8
9.0 Security Awareness and Training.....	8
9.1 Security Awareness	9
9.2 Security Training	9
10.0 Managing Third Parties	9
10.1 Granting Access to Third Parties	9
11.0 Information Technology Security.....	9
11.1 Protections against Malicious Software Programs	10
11.2 Network Security.....	10
11.3 Mobile Devices.....	10
11.4 Information Asset Monitoring	10
12.0 Configuration Management.....	11
13.0 Change Control	11
13.1 Emergency Changes	11
14.0 Access Control.....	11
14.1 Granting Access.....	12
14.2 Separation of Duties.....	12
14.3 Access Review	12
14.4 Modifying Access	12
15.0 Information Asset Management.....	12
16.0 Information Systems Acquisition, Development, and Maintenance	13
17.0 Information Security Incident Management	13
18.0 Physical Security.....	13
19.0 Business Continuity and Disaster Recovery	14
20.0 Compliance	14
21.0 Policy Enforcement	14

1.0 Introduction

The Board of Trustees of the California State University (CSU) is responsible for protecting the confidentiality, integrity and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise 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 information which the CSU must protect from unauthorized access.
- Integrity and availability of information stored on or processed by CSU information systems.
- Compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection.

This policy and associated standards provide direction and support to campuses and the Chancellor's Office to assist them in meeting this commitment. The CSU Information Security Policy and Standards are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the CSU's core mission and campus academic and administrative goals.

2.0 Scope

This policy shall apply to the following:

- All campuses, including CSU auxiliary organizations and external businesses or organizations that use campus information assets.
- Central and departmentally-managed campus information assets.
- All users employed by campuses or any other person with access to campus information assets.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

The CSU retains ownership or stewardship of information assets owned (or managed) by 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 campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources.

3.0 Policy Management

This policy shall be updated as necessary 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 and communicating any changes or additions to appropriate CSU stakeholders.

This policy may be augmented, but neither supplanted nor diminished, 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.

4.0 Establishing an Information Security Program

Each campus President and the Assistant Vice Chancellor for Information Technology Services are responsible for the establishment and implementation of 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 an acceptable level of information security and must be reviewed at least annually.

The campus program must:

- Document roles and responsibilities for the information security program.
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic).
- Develop risk management strategies to identify and mitigate threats and vulnerabilities to level 1 and level 2 protected data and information assets as defined in the CSU Data Classification Standard.
- Establish and maintain an information security incident response plan.
- Maintain ongoing security awareness and training programs.
- Comply with applicable laws, regulations, and CSU policies.

5.0 Organizing Information Security

Each campus must develop, implement, and document the organizational structure that supports the campus' 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 and must be reviewed at least annually.

Each President (or President-designee) and the Assistant Vice Chancellor for Information Technology Services (or the Vice Chancellor's designee) must appoint a campus ISO. The Assistant Vice Chancellor for Information Technology Services (or the designee of the Chancellor) is responsible for the system wide Information Security Management program and may organize the responsibilities as appropriate.

6.0 Information Security Risk Management

Risk management involves the identification and evaluation of risks to information security assets (risk assessment) and the ongoing collection of information about the risk (risk monitoring). Once a risk has been identified, campuses must decide to develop and implement strategies to reduce the risk to acceptable levels (risk mitigation), share or shift the risk to another party (risk transference), or assume the identified risk (risk acceptance).

Campuses must develop risk management processes that identify, assess, and monitor risks to information assets containing protected data. Identified risks to these information assets must be actively managed in order to prioritize resources and remediation efforts.

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.

Campuses 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.

Campuses must select appropriate mechanisms to safeguard the confidentiality, integrity, and availability of information assets containing protected data. Campus mitigation strategies must be commensurate with risks identified by risk assessments. For those risks where the mitigation strategy involves the use of controls, those controls must ensure that risks are reduced to an acceptable level, taking into account:

- Legal and regulatory requirements and compliance.
- Campus 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 Risk Transference

If possible a risk may be managed by sharing or completely moving it to another entity. Campuses may transfer risks if the required actions of the receiving entity are deemed to result in an acceptable outcome should the risk be exploited and damage occurs. Risks associated with potential failure to comply with applicable laws, statues, or regulations can only be transferred if the results will support compliance.

6.4 Risk Acceptance

Risk acceptance occurs when potential risk-reduction activities cannot be found or those identified are determined not to be cost effective (e.g. the protections cost more than the potential loss). In the case where responsible mitigation is possible, but resources are not available, the risk must still be handled under mitigation until the resources can be obtained. Campuses must develop a process for documenting, reviewing and approving accepted risks. Accepted risks must undergo periodic review and approval.

6.5 Risk Monitoring

Sometimes, when a risk is identified, there may be insufficient or conflicting information regarding its likelihood of occurrence or potential impact. Campuses must monitor risks of this nature and develop a plan to gather sufficient information to judge whether the risk should be mitigated, transferred, or accepted.

6.6 Reporting Information Security Risks

The Senior Director of System wide Information Security Management must complete a risk assessment of information assets containing protected data at least every two years. The report must include a description of the methodology, the results of the risk assessment, and recommended system wide mitigation strategies for addressing each identified risk. The report must be certified by the system wide Information Security Steering Committee and presented to the Chancellor (or Chancellor-designee).

7.0 Privacy of Personal Information

All users of campus Information systems or network resources are advised to consider the open nature of information disseminated electronically and must not assume any degree of privacy or restricted access to information they create or store on campus systems. The CSU is a state agency and information stored on campus information systems may be subject to disclosure under state law. No campus information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, the CSU acknowledges its obligation to respect and protect private information about individuals stored on campus information systems and network resources.

7.1 Collection of Personal Information

To comply with state and federal laws and regulations, campuses may not collect personally identifiable information unless the need for it has been clearly established.

Where such information is collected:

- The campus will use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.
- The campus shall store personally identifiable information only 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 campus information systems may only be accessed by:

- The individual to whom the stored information applies or his/her designated representative(s).
- Authorized CSU employees with a valid CSU-related business need to access, modify, or disclose that information.
- Appropriate legal authorities.

When appropriate, authorized CSU personnel following established campus procedures may access, modify, and/or disclose information about individuals stored on campus information systems or a user's activities on campus 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 with or enforce applicable CSU policy.
- To ensure the confidentiality, integrity or availability of campus information.
- To respond to valid legal requests or demands for access to campus information.

If CSU personnel accesses, modifies, and/or discloses information about an individual and/or his/her activities on campus information systems or network resources, staff 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 access or store protected data must use due diligence to prevent unauthorized access and disclosure of such assets.

Browsing, altering, or accessing electronic messages or stored files in another user's account, computer, or storage device 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 to shared files and/or resources based on assigned roles and responsibilities.
- 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.
- Access to implicitly publicly accessible resources such as University websites.
- 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 appropriate to their responsibilities and roles. Users who access protected data must sign a confidentiality (non-disclosure) agreement. This agreement must be renewed upon changes in job classification or departments.

8.1 Employment Requirements

Campuses must develop procedures to conduct background checks on positions involving access to level 1 information assets as defined in the CSU Data Classification Standard

8.2 Separation or Change of Employment

Campuses must implement procedures to revoke access to information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy and by the data owner. Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

Procedures must be implemented to ensure proper disposition of information assets 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 the separating employee is holding resources subject to a litigation hold, the campus must ensure preservation of relevant information until the litigation hold has been revoked, at which point the resource is subject to the normal record retention schedule.

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 limited-access area on the campus must be updated appropriately to reflect the change in employment status.

Each campus must establish procedures to allow for separated employees to obtain such incidental personal electronic information as appropriate.

Information system privileges retained after separation from the campus 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 employees appropriate to their access to campus information assets. The campus information **security awareness** program must promote campus strategies for protecting information assets containing protected data.

All employees with access to protected data and information assets must participate in appropriate information 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 containing protected data as defined in the CSU Data Classification Standard.

The program must promote awareness of:

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

Third parties who access CSU information assets must be required to adhere to appropriate CSU and campus information security policies and standards. As appropriate, a risk assessment must be conducted to determine the specific implications and control requirements for the service provided.

10.1 Granting Access to Third Parties

Third party service providers may be granted access to campus information assets containing protected data as defined in the CSU Data Classification Standard only when they have a need for specific access in order to accomplish an authorized task. This access must be authorized by a designated campus official and based on the principles of need-to-know and least privilege.

Access to campus information assets which store or access protected data 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.

11.0 Information Technology Security

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

11.1 Protections against Malicious Software Programs

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

11.2 Network Security

Campuses must appropriately design their networks—based on risk, data classification, and access—in order to ensure the confidentiality, integrity and availability of 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 is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets 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. Protected data as defined in the CSU Data Classification Standard 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 level 1 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 protected data.

11.4 Information Asset Monitoring

Campuses must implement appropriate controls on the monitoring of information systems and network resources to ensure that monitoring is limited to approved activities. Monitoring must not be conducted for the purpose of gaining unauthorized access, snooping, or other violations of the Responsible Use Policy. Records created by monitoring controls (e.g. logging) must be reviewed regularly.

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

Data generated by 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.

Server administrators are required to scan regularly, 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 undergo a risk assessment at least once per year, to ensure compliance with 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).

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 minimize the risk of introducing unexpected vulnerabilities and ensure that existing security protections are not adversely impacted. Campuses must establish and document a process to manage changes to campus information assets containing level 1 or data as defined in the CSU Data Classification Standard.

Campuses must evaluate the information security impact of changes by taking a risk-based approach to change control.

Changes to information assets which store protected data will likely require a more rigorous review than changes to non-critical assets and must be made in accordance with a formal, documented change control process. Changes that may impact the security of these information assets must be identified along with the level of control necessary to manage the change.

Campuses must define and publish the scope of significant changes to level 1 and level 2 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 authorized persons may make an emergency change to campus information assets containing protected data as defined in the CSU Data Classification Standard. 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 must 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 information assets containing protected data must be based on operational and security requirements. Appropriate controls must be in place to safeguard unauthorized access to protected information assets. This includes not only the primary operational copy of the protected information assets, 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. Access to campus protected information assets must be denied until specifically authorized.

Access to public and shared resources may be excluded from this requirement. Campuses are required to identify and document public or shared resources that are excluded from this requirement. Authorized users and their access privileges must be specified by the data owner, unless otherwise defined by CSU/campus policy.

14.1 Granting Access

Access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of need-to-know and least privilege.

Authentication controls must be implemented for access to campus information assets that access or store 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 Separation of Duties

Separation of duties principles must be followed when assigning job responsibilities relating to restricted or essential resources. Campuses must maintain an appropriate level of separation of duties when issuing credentials to individuals who have access to information assets containing protected data. Campuses must avoid issuing credentials that allow a user greater access or more authority over information assets that store or access protected data than is required by the employee's job duties.

14.3 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 information assets containing protected data. The results of the review must be documented.

14.4 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

Each campus must develop and maintain a data classification standard that meets or exceeds the requirements of the CSU Data Classification Standard.

Campuses must maintain an inventory of information assets containing protected data. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction.

The designated owner of information assets that store protected data 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 must 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 life cycle of 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 protected data.

17.0 Information Security Incident Management

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

- Define and/or categorize incidents.
- Designate specific personnel to respond to information security incidents in a timely manner.
- Include procedures for documenting the information security 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 at preventing or mitigating the risk of similar occurrences.

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

Campus procedures must include the following notification protocol:

- If a breach of level 1 data has occurred, the campus President must notify the Chancellor, the CIO must notify the Assistant Vice Chancellor for Information Technology Services, and the campus ISO must notify the Senior Director of System wide Information Security Management.
- If a breach of level 2 data has occurred, the campus ISO must notify the Senior Director of System wide Information Security Management. The Senior Director will provide the Chancellor with quarterly status reports on level 2 data breaches that have occurred in the CSU.

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 information assets containing protected data are stored. Campuses must protect these areas from unauthorized physical access while ensuring that authorized users have appropriate access. Campus information assets which access protected data that are located 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 rights to campus 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 their 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 Business Continuity Policy.

20.0 Compliance

The CSU shall, in consultation with the CSU Office of General Counsel 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 that ensure 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, collective bargaining agreements, and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

The CSU 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 CSU resources or to protect the CSU from liability.

Allegations against employees that are sustained may result in disciplinary action. Such actions must be administered in a manner consistent with the terms of the applicable collective bargaining agreement, in accordance with applicable provisions of the California Education code, and/or civil or criminal provisions. Student infractions of this policy must be handled in accordance with applicable State laws and related campus judicial processes. Third party service providers who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements.