California State University, Sacramento

Supplemental Information Security Policies

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 .......................................................................................................................... 4
2.0 Scope .................................................................................................................................. 4
3.0 Policy Management .............................................................................................................. 4

[No addenda required for sections 4.0-5.0 of the CSU Information Security Policy and Standards] ......................................................................................................................... 4

6.0 Information Security Risk Management ............................................................................... 4
  6.1 Risk Assessment ................................................................................................................... 4
  6.2 Risk Mitigation .................................................................................................................... 5
  6.4 Risk Acceptance .................................................................................................................. 5
  6.5 Risk Monitoring .................................................................................................................. 5

[No addenda to section 7.0 of the CSU Information Security Policy and Standards] ......................................................................................................................... 5

8.0 Personnel Information Security .......................................................................................... 5
  8.1 Employment Requirements .................................................................................................. 5
  8.2 Separation or Change of Employment .............................................................................. 5
  8.3 Audit of Physical Access .................................................................................................... 6

9.0 Information Security Awareness and Training .................................................................. 6
  9.1 Security Awareness ............................................................................................................ 6
  9.2 Specific Security Training .................................................................................................. 6

10.0 Managing Third Parties .................................................................................................... 6
  10.1 Granting Access to Third Parties ..................................................................................... 6

11.0 Information Technology Security ..................................................................................... 7
  11.1 Security of Servers and Network Attached Devices ......................................................... 7
  11.2 Protection Against Malicious Software ........................................................................... 8
  11.3 Network Security ............................................................................................................. 8
  11.4 Network Topology .......................................................................................................... 9
  11.5 Wireless and Remote Access .......................................................................................... 9
  11.6 Information Asset Monitoring ......................................................................................... 9

12.0 Configuration Management ............................................................................................... 10

13.0 Change Control .................................................................................................................. 10
  13.1 Emergency Changes ......................................................................................................... 10

14.0 Access Control ................................................................................................................... 10
  14.1 Granting Access .............................................................................................................. 11
  14.2 Separation of Duties ......................................................................................................... 11
  14.3 Access Review ................................................................................................................ 11
14.4 Modifying Access ................................................................. 12
15.0 Information Asset Management ........................................ 12
16.0 Information Systems Acquisition, Development, and Maintenance ................................................................. 12
  16.1 Acquisition .................................................................. 12
  16.2 Development .................................................................. 12
  16.3 Maintenance and Testing .................................................. 13
17.0 Information Security Incident Management .......................... 13
1.0 Introduction
This policy augments the latest version of the CSU Information Security Policy previously adopted by Sacramento State, but neither supplants nor diminishes that policy. This supplemental policy is specifically responsive to the information security audit results reported to Sacramento State in December, 2009. The intent of these supplemental policies is to protect the campus from the risks associated with information security breaches, while at the same time maintaining campus access to essential information technology functions and services. The application of these policies should therefore consistently consider how required information security controls can be implemented with minimal effect on user services. Whenever feasible, user input and collaboration should be obtained prior to the application of these policies to specific information security incidents.

2.0 Scope
This supplemental set of policies has the same scope as the University’s general Information Security Policy, adopted by the campus on May 1, 2009.

This supplemental policy adds delegation to the Information Security Officer (ISO) and Vice President & Chief Information Officer, under the authority of the President, of all needed authority for evaluation, enforcement and implementation of all information security policies and practices campus-wide. The specific aspects of this delegated authority are delineated below and in the Sacramento State general Information Security Policy.

This supplemental policy also delineates the specific practices and procedures required to manage campus-wide information security risk at Sacramento State. Any exceptions or non-compliance related to information security policies and practice must be reviewed, documented and approved through the Risk Acceptance and Exception Process.

3.0 Policy Management
The Information Security Officer is delegated responsibility for conducting an annual review of information security policies and practice, as well as for communicating any recommended changes, additions or deletions to the President. Updates required to reflect changes in Sacramento State’s academic, administrative, or technical environments, or in applicable federal/state laws or CSU regulations shall be recommended to the President as necessary by the Vice President & Chief Information Officer.

[No addenda required for sections 4.0-5.0 of the CSU Information Security Policy and Standards]

6.0 Information Security Risk Management

6.1 Risk Assessment
The Information Security Officer of Sacramento State is required to conduct a comprehensive campus-wide information security risk assessment on at least an annual basis. A report on the results of such risk assessments will be presented to the Vice President and Chief Information Officer and reviewed with the President no later than December 1st of each year. The report must include a description of the risk assessment methodology, the results of the risk assessment, a specific assessment of segregation of duties issues, a listing of any approved policy exceptions, and recommended
mitigation strategies for addressing each identified risk. The President will certify the results of the annual risk assessment, as well as all required mitigation strategies and risk acceptance contained in that report. A copy of the final report will be provided to the CSU Chancellor’s Office and a summary will be distributed on campus.

6.2 Risk Mitigation
Sacramento State will adhere to the attached Information Security Risk Mitigation Process for documenting and tracking all decisions related to risk mitigation. The Vice President and Chief Information Officer, in consultation with the President, must approve all risk mitigation strategies and exceptions to the risk management process in writing.

6.4 Risk Acceptance
The Sacramento State Risk Acceptance and Exception Process must be followed before any non-compliant information security risk may be accepted by the campus. The Vice President and Chief Information Officer, in consultation with the President, must review and approve all such assumed risk. Any such accepted risk will be documented annually as part of the Annual Risk Assessment procedures noted in section 6.1.

6.5 Risk Monitoring
When a potential information security risk is identified or reported, but there is insufficient or conflicting information regarding the likelihood of significant risk at the time of the report, the Information Security Officer will develop a plan using the Risk Monitoring Process. The result of this process will comprise a thorough monitoring and investigation of the potential for information security risk and a plan to mitigate any identified risk. When permitted by law, this assessment will be completed in cooperation with those who operate the at-risk computer/network system(s). The results of any such risk monitoring and review will be submitted to the Vice President & Chief Information Officer in a timely manner and shall include a) a review of the level of risk confirmed; b) a review of the confidentiality of data at risk; and c) a recommendation for timely mitigation of any serious risk.

[No addenda to section 7.0 of the CSU Information Security Policy and Standards]

8.0 Personnel Information Security

8.1 Employment Requirements
Subject to the limits of law and CSU bargaining agreements, all Sacramento State employers must develop procedures to conduct background checks prior to the appointment of any positions involving access to Level 1 information assets, as defined in the Sacramento State Data Classification Standard.

8.2 Separation or Change of Employment
Access and privileges to campus information resources must be removed for all employees on the last day of active work on campus, upon termination of employment, or when job duties no longer provide a legitimate business reason for information access.

Separated employees must follow the Employee Separation Process to secure any confidential information in their possession prior to removal of their access to that information. In addition, both electronic and paper files containing sensitive information that are in the possession of separated employees must be promptly identified and either removed or placed in the possession of an authorized departmental data steward, who shall consult with the
Information Security Officer to identify appropriate methods for transfer or disposal of such files. A separated employee shall be given the opportunity to separate stored personal data from work related data and to retain that personal data.

All information technology assets used by separated employees must be transferred or disposed of in a manner that assures the continued confidentiality of any stored campus data.

If the separating employee is in possession of information resources subject to a litigation hold, the Information Security Officer must be contacted to conduct a final data collection appropriate to that litigation hold.

8.3 Audit of Physical Access
The Information Security Officer must conduct an annual audit of physical access to confidential information resources, included the appropriateness of physical security, key and card access, and controls over access by unauthorized personnel. Any results of the audit indicating levels of risk related to physical access that are deemed unacceptable by the ISO must be reported to the Vice President and Chief Information Officer, including recommendations for mitigation of that risk.

9.0 Information Security Awareness and Training
The Information Security Officer must implement a program to provide regular information security awareness training to all campus employees appropriate to their level of access to campus information assets. All employees with access to Level 1 data and information assets must participate in information security awareness training on at least an annual basis that is specifically targeted at continued protection of those data and assets.

9.1 Security Awareness
At a minimum, this information security awareness program must provide all employees with an overview of campus information security policies applicable to their work and prepare individuals to recognize and appropriately respond to threats to Level 1 and Level 2 data, as defined in the Sacramento State Data Classification Standard.

9.2 Specific Security Training
The Information Security Officer must also provide or coordinate targeted training for individuals whose job functions require special knowledge of safeguards required to counter identified security threats and vulnerabilities. This training must focus on expanding information security knowledge, skills, and abilities specific to the information handling duties of individuals who handle protected data (i.e. Level 1 and Level 2 data).

10.0 Managing Third Parties

10.1 Granting Access to Third Parties
Third party service providers may be granted access to campus information assets when needed to accomplish an authorized and necessary business-related task. All such access must be documented in writing and authorized using procedures approved by the Information Security Officer. All such access shall be based on the security principles of ‘need-to-know’ and ‘least required privilege’ and must be subject to ongoing monitoring and oversight by the Information Security Officer.
11.0 Information Technology Security

11.1 Security of Servers and Network Attached Devices
The Information Security Officer is delegated all necessary authority to set and enforce information security standards for all servers and network attached devices, as well as to monitor, establish and enforce remediation timelines and sanctions for non-compliant systems campus-wide. The primary mechanism for addressing vulnerability will be the management of all identified critical, business and vulnerable systems under campus-wide standards defined by the Information Security Officer.

All critical, business, and vulnerable servers and network attached systems and devices (as classified by the ISO) must be registered in writing with the Information Security Officer. The registration process shall include categorization of the data used by such systems and devices according to the Sacramento State Data Classification Standard and shall also provide other information as required by the Information Security Officer adequate for a full assessment of information security risk on such systems. The Information Security Officer will review the registration data for each registered system or device and then define the risk level for each such system and device based on the following security categories:

**Critical**
- Regulatory requirements (i.e. FERPA, PCI, HIPAA)
- Contains Level 1 data as defined by the Sacramento State Data Classification Standard
- Provides campus-wide infrastructure (i.e. network/telecommunication equipment, HVAC, authentication services)
- Provides mission-critical service (i.e. Learning Management System, Email, Data Warehouse)
- Provides health and safety services
- System cannot be unavailable through unplanned maintenance for more than four (4) hours

**Business**
- Contains Level 2 data as defined by the Sacramento State Data Classification Standard
- Provides key program center or college specific service (i.e. systems used to meet key academic and administrative goals)
- System cannot be unavailable through unplanned maintenance for more than one (1) day

**Vulnerable**
- Systems that exhibit elevated vulnerabilities
- Systems that have an elevated risk of compromise
- Systems that have been compromised

**Client**
- Provide service to a local user or user group but does not provide services to other systems (i.e. desktop, labstation, laptop)
- Provides a local physical service that requires proximity (i.e.
Supplemental Information Security Policy

All Level 1 and Level 2 data stored on campus servers and other network attached devices must be identified to the Information Security Officer in a timely manner and such data must be securely stored and encrypted, as defined by Information Security Office guidelines.

The Information Security Officer must define mandatory standards and management protocols for each information security category above that are appropriate for the assured protection of both privacy and confidential data. These standards and protocols should, at a minimum, address a) physical security; b) access controls; c) configuration management; d) patching and malware protection; d) change management; e) risk management; f) vulnerability management; g) incident response; h) logging and monitoring of security events; i) secure network zoning and j) application acquisition, development and deployment.

All network attached devices must be actively scanned and/or reviewed on an ongoing basis by the Information Security Office vulnerability program. Proactive mitigation must be performed on identified critical and severe security vulnerabilities, under the direction of the Information Security Officer.

All required information security logs, as defined by the ISO, must be maintained, monitored, reviewed and retained following campus Log Management Guidelines.

11.2 Protection Against Malicious Software

All desktop computers, laptop computers, servers and other identified network attached devices must be actively managed by a campus-wide patch and malware management system. The Information Security Office will develop and maintain mandatory, comprehensive, and timely patch management and malware protection standards and processes for all computer and network devices campus-wide. These standards and processes shall be designed to minimize adverse effects of patch and malware management on continued IT operations.

All campus desktops, laptops and lab stations must run current anti-malware software and must be configured according to campus Configuration Management Standards as detailed in Section 12.0. Any exceptions to the use of malware protection under campus guidelines must be approved through the exception process noted under Section 2.0 above. Detection of a malware attack or compromise must be treated as a security event and reported and acted upon as required by Section 17.0 of this policy.

All inbound and outbound email to/from the campus must be protected from malware through processing by the campus-wide email security appliance identified by the Information Security Officer.

11.3 Network Security

All identified campus network devices handling or distributing critical, business, or vulnerable data must be compliant with all institutional information security policies and practices. The Information Security Officer shall define the process for mitigation of vulnerability from non compliant devices, including procedures for the possible removal of the device from the campus network and/or Internet.

All such devices must meet mandatory campus-wide Network Security Configuration Standards, as defined by the Information Security Officer.
11.4 Network Topology
All campus network topology will be determined by the Information Security Officer, in consultation with the Vice President & Chief Information Officer. Network topology will be based on development of secure network zones that will allow all networked devices to be placed in protected zones based on approved access needs, data classification, data value and risk. Special consideration will be given to the need for specialized instructional networks.

At a minimum, zones will be created to:

- Separate Internet-accessible devices from non-Internet-accessible devices
- Separate client systems from service systems
- Separate critical systems
- Separate business systems.
- Allow instructional systems to run unimpeded

All such network devices must comply with baseline security standards defined by the Information Security Officer. All new network devices handling or distributing critical, business, or vulnerable data must undergo a formal review and approval process prior to their attachment to the campus network, under the direction of the Information Security Officer.

Network bridging (i.e. the connection of a single computer to multiple networks) is not permitted unless the methodology used for such bridging is established using standards approved in writing by the Information Security Officer.

11.5 Wireless and Remote Access
All wireless network access must be implemented with mandatory time-outs for inactive wireless sessions, as defined by the Information Security Officer.

The Information Security Officer will oversee a periodic campus-wide wireless network audit to detect and eliminate rogue access points and rogue wireless activity.

The Information Security Officer will set information security requirements for all wireless network deployment and use, as well as establish and enforce remediation timelines and sanctions for non-compliant systems campus-wide.

11.6 Information Asset Monitoring
All Level 1 and Level 2 data found to be lost, stolen, or compromised must be reported immediately to the Information Security Officer, using the policies and procedures detailed in Section 17.0, Information Security Incident Management.

All servers and other applicable network-attached devices must be scanned for vulnerabilities on at least an annual basis and applicable event logs recorded under the direction of the Information Security Officer. The information security risk level of each applicable system, as defined by the ISO, will determine the frequency at which such logs must be kept and reviewed. Risk factors to be considered include:

- Criticality of business process.
- Information classification associated with the system.
- Past experience with system vulnerabilities.
Supplemental Information Security Policy

- System exposure (e.g., services offered to the Internet).

Proactive identification of Level 1 and Level 2 data stored on servers, desktops, and other devices during such scanning and logging must occur and must be reported to the Information Security Officer. All Level 1 and Level 2 data identified must be securely stored, using risk mitigation methods defined by Information Security Officer.

12.0 Configuration Management

‘Configuration management’ addresses how a system and its components are established, changed and/or monitored to ensure they are set up and managed securely. All specified information technology systems, including computers, servers, network devices, and applications must follow campus [Configuration Management Standards](#) in order to ensure maintenance of an appropriate security configuration that protects the campus from risk.

13.0 Change Control

Any changes to the configuration or management of servers, computers, and other network attached devices must be done in a manner that ensures continued information security. Therefore, all campus information and network systems designated as critical, business and vulnerable (see 11.1) must follow [Change Management Standards](#), as defined by the Information Security Officer. Formal review and approval by the Information Security Officer or his designees is required prior to deployment of all changes identified by the ISO as having significant potential for increasing information security risk. Changes typically defined as ‘significant’ include, but are not limited to: implementation of new information technology production systems; software and operating system version upgrades; implementation of new or removal of existing security components; as well as other system changes as defined by the Information Security Officer.

13.1 Emergency Changes

It is recognized that emergency changes to campus information assets are sometimes required to maintain business processes. Emergency changes are defined as changes which, due to urgency or criticality, must occur outside the campus formal change management process. Such emergency changes must be authorized in writing by the Information Security Officer. Emergency changes may be pre-authorized by submitting formal emergency change procedures to the Information Security Officer for prior review and acceptance. Any such emergency changes must be promptly documented to the Information Security Officer.

14.0 Access Control

All campus employees implementing and supporting authentication and access control processes must comply with the campus [Access Control Standards](#), as defined by the Information Security Officer. All account provisioning and de-provisioning campus-wide must take place only under standards set by the Information Security Officer and must use the defined campus-wide identity management system. All accounts will be housed only in the unified University Active Directory Domain, unless written exceptions are approved through the ISO.

All campus users of information and network systems will be provided a unique campus-wide account that must be used for computer and network access. Sacramento State prohibits any sharing of accounts used for access to information and network systems, unless such shared accounts are approved in writing by the ISO as meeting a business or instructional need that cannot be provided by more secure means. Any such approved shared accounts must be
assigned a designated owner responsible for all shared account activity and must be reviewed and approved annually by the Information Security Officer.

Administrative accounts for information and network system access must be established only using standards and procedures required by the Information Security Officer. Such administrative accounts must only be used when elevated permissions are required for authorized business needs and must not be used on unsecured systems. Local administrative access may be removed when it does not conform to this policy.

On at least an annual basis, all users must update their campus password(s) using the official campus-wide password management program. Password strength and configuration requirements will be established only by the Information Security Officer.

All exceptions to the above access control policies must be approved in writing using the procedures identified in Section 2.0.

14.1 Granting Access
Secure authentication controls must be used for all access to campus information assets that access, store or distribute Level 1 or Level 2 data. Access to Level 3 data may also be subject to secure authentication controls, as defined by the Information Security Officer.

14.2 Separation of Duties
Review, implementation and enforcement of required separation of duties principles and processes for the handling of Level 1 and Level 2 data is delegated to the Information Security Officer, with all related actions certified in writing to the Vice President & Chief Information Officer and reported to the President. All processes used for account handling and authentication must maintain an appropriate level of separation of duties when issuing credentials to individuals who have access to information assets containing Level 1 and Level 2 data. The campus must avoid issuing credentials that allow a user greater access to or authority over information assets than is required by the employee’s assigned job duties.

On at least an annual basis, Sacramento State will complete a formal campus-wide process to review, monitor, and ensure compliance with separation of duties and access controls over the granting of access to critical systems.

14.3 Access Review
The Information Security Officer will develop procedures to detect unauthorized access and privileges assigned to users that exceed the required access rights needed to perform their job functions.

All access rights for Level 1 and Level 2 data and elevated access must be reviewed annually and the results of such reviews documented by the Information Security Officer and reported to the Vice President & Chief Information Officer. Users who access Level 1 or Level 2 data as defined in the CSU Data Classification Standard must sign an approved system-wide confidentiality (non-disclosure) agreement, with special attention to staff members who are granted elevated access.
14.4 Modifying Access

All transfers and other changes in employment status affecting data access rights must be reported to the Information Security Officer in a timely manner. All required changes in account access and account privileges must be made promptly in the central campus identity management system.

15.0 Information Asset Management

The Information Security Officer will maintain an inventory of all known information assets containing Level 1 and Level 2 data. Such 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 Sacramento State Data Classification Standard.
- Managing security controls over such data according to campus standards, including reporting discrepancies and problems promptly to the Information Security Officer.
- Managing the information asset according to the requirements described in the campus Information Asset Management Standard.

Such data must not be transferred to another individual or system without formal approval of the authorized data owner. Before Level 1 or 2 data may be transferred, the data owner must complete the approved Data Authorization Process to establish written agreements ensuring that authorized users implement appropriate security controls over the transferred data.

All computer and network devices must be disposed of using the Disposition of Protected Data process.

16.0 Information Systems Acquisition, Development, and Maintenance

The Information Security Officer is delegated all necessary authority to set and enforce standards for the appropriate security of all software and web applications, as well as to monitor, establish and enforce remediation timelines and sanctions for non-compliant systems campus-wide. The Information Security Officer will establish security standards for the acquisition, development, deployment and maintenance of all software and web applications handling sensitive information and/or that are accessible from off campus.

16.1 Acquisition

All campus software and web application acquisitions or upgrades involving handling of Level 1 and/or Level 2 information and/or access from off campus must be reviewed and approved by the Information Security Officer or his designee(s) in writing prior to purchase. All acquisitions must follow the campus Application Acquisition Process.

16.2 Development

Application and advanced web development involving protected classes of information (Level 1 and Level 2) is a distinct and limited activity engaged in by only a few campus employees. All application and web developers must familiarize themselves and follow the campus Application Development Standards to ensure they are employing secure procedures for any application or web development involving Level 1 and/or Level 2 data. All application code for such applications must be reviewed and approved in writing by the Information Security Officer or his designee(s) prior to deployment. All significant changes in application code must also be reviewed for vulnerabilities prior to deployment. All applications or
web processes handling, processing or storing critical and business information must be housed only within secure data centers identified by the Information Security Officer on systems meeting all applicable security policies and standards.

16.3 Maintenance and Testing
Access to source code and other critical system resources during testing, development, or production must be limited to only authorized personnel with an authorized work-related need.

17.0 Information Security Incident Management
All information security incidents must be reported in a timely manner to the Information Security Officer. Security incidents include theft, loss, damage or compromise to information systems and data, known vulnerabilities and exploits, website defacement or compromise, successful malware attacks, denial of services, and other security events as defined by the Information Security Officer. The Incident Reporting Process used must:

- Define and categorize incidents.
- Require reporting of the loss of any computer or network device, with special attention to those potentially containing Level 1 and Level 2 data.

The Incident Response Standard must be used to define, investigate, and respond to all information security incidents. The response process must:

- Be prompt and timely, mitigating risk and threat as quickly as possible;
- Designate specific personnel to respond to information security incidents in a timely manner;

- Include procedures and guidelines for documenting the information security incident that:
  - Identify the types, volume, and costs of security incidents to ensure the campus monitors trends and risks;
  - Determine notification requirements;
  - Implement remediation strategies;
  - Report to executive 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 following notification process is required for information security incidents:

- If a breach of Level 1 data has occurred, the Information Security Officer or Vice President/CIO will immediately notify the President, who will then notify the Chancellor; the Vice President and Chief Information Officer will immediately notify the CSU Assistant Vice Chancellor for Information Technology Services; and the campus Information Security Officer must notify the Senior Director of System-wide Information Security Management.

- If a breach of Level 2 data has occurred, the campus Information Security Officer must notify the Vice President and Chief Information Officer and the Senior Director of System-wide Information Security Management.
The campus information security incident response plan must be reviewed and tested annually by the Information Security Officer, with results reported to the Vice President and CIO.