Table of Contents

8000.00 | Introduction and Scope

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction for managing and protecting the confidentiality, integrity and availability of CSU information assets. In addition, the policy defines the organizational scope of the CSU information Security Policy.

POLICY STATEMENT

100 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.

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.

200 Scope
The CSU Information Security policy shall apply to the following:

- All campuses.
- 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.

Auxiliaries, external businesses and organizations that use campus information assets must operate those assets in conformity with the CSU Information Security Policy.
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. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

8005.00 | Policy Management

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy defines the CSU Information Security Policy review process.

POLICY STATEMENT

The CSU Information Security Management Department shall be responsible for overseeing a documented annual review of this policy and communicating any changes or additions to appropriate CSU stakeholders. The CSU Information Security policy shall be updated as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations.

The 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 the CSU Information Security policy must be developed by each campus through consultation with campus officials and key stakeholders.

8010.00 | Establishing an Information Security Program

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy defines minimum requirements for CSU Information Security Programs.

POLICY STATEMENT

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 sufficient to provide an acceptable level of information security and must be reviewed at least annually. The campus information security program reviews must be documented.
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 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.

8015.00 | Organizing Information Security

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides guidance for defining the governance structure of CSU Information Security Programs.

POLICY STATEMENT

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. The governance structure must be reviewed at least annually. Review of the campus organizational structure that support the information security program must be documented.

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

8015.S000 Information Security Roles and Responsibilities

Implements:	CSU Policy #8015
Policy Reference:	8015.00 Organizing Information Security

Introduction

The CSU Information Security policy provides guidance for defining the governance structure of CSU Information Security Programs.

a) 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. The governance structure must be reviewed at least annually.
b) Each President (or President-designee) and the Assistant Vice Chancellor for Information Technology Services (or the Vice Chancellor's designee) must appoint a campus information security officer (ISO). The Assistant Vice Chancellor for Information Technology Services (or the designee of the Chancellor) is responsible for the systemwide Information Security Management program and may organize the responsibilities as appropriate.

1.0 Campus President

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

1.2 The President (or President's designee) must identify the specific duties and responsibilities for the ISO, which, at a minimum, include those items identified below. While the role of the Information Security Officer (ISO) may be an additional duty, the President must ensure the appointee has sufficient time to carry out the assigned duties and responsibilities.

1.3 The President may assign additional roles and responsibilities appropriate to the campus.

1.4 Each President must review information security risks at least annually.

2.0 Campus Chief Information Officer (CIO)

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

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

3.0 Campus Information Security Officer (ISO)

The ISO must:

a) Coordinate the campus information security program on behalf of the President.
b) Advise the President and his/her cabinet on all information security matters.
c) Work closely with campus administrators and executive officers on information security matters.
d) Oversee campus information security risk assessment activities.
e) Inform the President (or President-designee) of significant information security risks as they are identified.
f) Oversee the campus information security incident response program in coordination with appropriate campus personnel.
g) Oversee the campus information security awareness and training program.
h) Provide input to the campus budget process regarding prioritization and required resources for information security risk mitigation activities and inputs regarding information security risks of proposed projects.
i) Respond to information security related requests during an audit.
j) Serve as the campus representative on the CSU Information Security Advisory Committee.
k) Avoid conflicts of interest by not having direct responsibility for information processing or technology operations for campus programs that employ protected information.

4.0 Campus Managers

Technical and program (e.g., human resources, registrars, privacy officers, etc.,) managers are responsible for:

a) Ensuring that information assets under their control are managed in compliance with CSU and campus information security policies and standards.
b) Ensuring that staff and other users of information assets under their control are informed of and comply with CSU and campus information security policies and standards.

5.0 Campus Data Owners

5.1 The data authority/owner must:

a) Classify each information asset for which he or she has ownership responsibility in accordance with CSU and campus policies/standards, or legal, regulatory, or contractual requirements.
b) Work with the ISO to define controls for limiting access to and preserving the confidentiality, integrity and availability of information assets that have been classified as requiring such controls.
c) Authorize access to the information asset in accordance with the classification of the asset and the need for access to the information.
d) Ensure that those with access to the information asset understand their responsibilities for collecting, using, and disposing of the asset in accordance with CSU and campus policies/standards, or legal, regulatory, or contractual requirements.
e) Work with the ISO to monitor and ensure compliance with CSU/campus security policies and procedures affecting the information asset.
f) Work with the ISO to identify an acceptable level of risk for the information asset.
g) Work with the ISO, data user, data custodian/steward, and/or other authorized individuals during the investigation and mitigation of information security incidents/breaches affecting the information asset.

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

6.0 Campus Data Custodian/Steward

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

a) Complying with applicable law and administrative policy.
b) Complying with any additional security policies and procedures established by the owner of the information asset and the campus ISO.
c) Advising the owner of the information asset and the campus ISO of vulnerabilities that may present a threat to the information and of specific means of protecting that information.
d) Notifying the owner of the information asset and the campus ISO of any actual or attempted violations of security policies, practices, and procedures.

7.0 Campus Data User

The responsibilities of a data user consist of:

a) Ensuring that he or she does not put any University information asset for which he or she has been given access at risk through his or her own actions.
b) Working with the ISO, data authority, data custodian/steward, and/or other authorized individuals during the investigation and mitigation of information security incidents/breaches affecting the information asset.
c) Performing as appropriate other information security duties as required by other CSU and campus policies/standards, the data owner, or the campus ISO.

8.0 Systemwide Chief Information Security Officer

The Systemwide Chief Information Security Officer must:

a) Provide leadership for the overall CSU Information Security Program
b) Conduct an periodic review and update of the CSU security policy and standards
c) Advise the Chancellor and CSU senior management on matters regarding information security
d) Provide support to information security staff at each campus
e) Develop systemwide information security strategies and metrics

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	5/20/2011	Macklin	Draft Standard	All
1.1	6/17/2011	Moske	Format draft.	All
1.2	11/5/2013	Macklin	Updated § 8 to reflect title change, added 8(e) based on feedback from ITAC. Update other section titles to distinguish between campus and systemwide personnel.	All
New	11/15/13	Moske	Accept Macklin Edits and publish final	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
Click here to enter Review Date	Click here to enter Review Date	Click here to enter Review Date
3/21/2012	ISAC	Reviewed, approved and recommended for CISO review
6/25/2013	ITAC	Reviewed and approved
11/5/2013	CISO	Reviewed and approved

8020.00 | Information Security Risk Management

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for the campus information security risk management program.

POLICY STATEMENT

100 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 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 level 1 and level 2 data as defined in the CSU Data Classification Standard. Identified risks to these information assets must be actively managed by data owners and/or appropriate administrators in order to prioritize resources and remediation efforts.

200 Information Security 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 scope and frequency of the assessment; risk assessment methodology; result of the risk assessment; and, mitigation strategies designed to address identified risks.

300 Information Security 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 process for documenting and tracking decisions related to risk mitigation activities.

400 Information Security Risk Transference
Whenever possible, a risk may be managed by sharing or completely transferring 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, statutes, or regulations can only be transferred if the results will support compliance.

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

500 Information Security 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 protection measures cost more than the potential loss). In the case where resources for the best mitigation strategy are not available, the risk must be addressed to the extent possible using available resources.

Campuses must develop a process for documenting, reviewing and approving accepted risks. Accepted risks must undergo periodic review and approval by appropriate administrators.

600 Information Security 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.

700 Reporting Information Security Risks
The Senior Director of Systemwide Information Security Management must complete a risk assessment of information assets containing level 1 data as defined in the CSU Data Classification Standard at least every two years. The report must include a description of the methodology, the results of the risk assessment, and recommended systemwide mitigation strategies for addressing each identified risk. The report must be certified by the systemwide Information Security Steering Committee and presented to the Chancellor (or Chancellor-designee).

8020.S000 Information Security Risk Management – Exception Standard

Implements:	CSU Policy #8020.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8020.0.shtml

Introduction

A campus may decide to allow exceptions to CSU or campus policies, standards or practices. Campuses must develop criteria for determining the organization with authority to approve an exception (i.e. manager, ISO, CIO, data owner, or combination of personsas appropriate). Exceptions may be granted when the campus decides, after a risk assessment, that there are adequate compensating controls. When adequate compensating controls do not exist, the campus must follow it's risk management process to ensure that the exception is approvied by an appropriate Vice-President or other campus administratior with fiscal responsibility for addressing the result of risk acceptance.When a campus grants an exception or accepts a risk, it must comply with the following minimum standards to identify, monitor and periodically review the exception.

1.0 Exception Process

Each campus must develop a process for documenting, reviewing and approving exceptions.

1.1 The campus exception process must include the following:

a) Required management approval from the requesting organization's appropriate administrator.

b) A description of the nature and types of exceptions which must be reviewed by the campus ISO.

c) A process and timeline for periodic review of granted exceptions in which periodic reviews must be performed at least every three years.

d) A record documenting the exception process including:

   a. Contact information for individual and/or organization requesting the exception.

   b. The policy, standard or other requirement to which exception is being requested..

   c. Justification for the proposed exception.

   d. Description of any proposed compensating control or mitigating circumstance.

   e. Information security risk analysis using the campus risk assessment methodology.

   f. Designation (i.e. "high", "medium") of risk under the campus' risk assessment methodology.

   g. Appropriate approvals.

e) Retention of exception review and approval records for at least 3 years after the exception is withdrawn or expired, or as required by applicable records retention schedule.

2.0 Periodic Review of Granted Exceptions

Exceptions must undergo periodic review and approval by appropriate administrators.

2.1 The exception review process must include:

a) Periodic review as per the schedule established in §1.1(c).

b) Confirmation from the requestor of whether or not the exception remains necessary.

c) Review sufficient to determine if controls remain adequate to mitigate risk.

d) Update of the exception record to reflect changes and record completion of the review including:

   a. Updated approval from changed management or organization.

   b. Any changes in hardware, software, policy or standard relevant to this exception.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	6/10/2014	Macklin	First draft – ISAC development team	All
1.1	2/24/15	Macklin	CISO comments/ISAC development team	1.1, Intro
1.2	3/1/15	Macklin	CISO comments	1.1, Intro
1.3	3/1/15	Macklin	CISO comments	1.1(c)

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
3/2/15	P&S Committee with CISO	CISO comments reviewed and discussed (3/2/15 – 10am). This version includes those comments. Next steps collaborative review.
3/2/15	Leslie DeCato	Added Draft Watermark. Submitting to ISAC/ITAC for Review.
3/3/15	Perry	Reviewed and accepted all (track changes). Submitted to DeCato for ISAC/ITAC Review. Review period will be 3/6/15 to 4/10/15.
6/4/15	Perry (CISO)	Approved for Posting

8020.S001 Information Security Risk Management – Risk Assessment Standard

Implements:	CSU Policy #8020.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8020.0.shtml

Introduction

A campus must develop a process for assessing risks to its information assets. These assessments must be based on established severity and likelihood criteria and managed through ongoing evaluation and review activities.

1.0 Risk Assessment Criteria

Each campus must use a risk assessment model based on established criteria (see Appendix A). The campus must not alter the severity or likelihood classifications contained in Appendix A, but the campus may add criteria and/or numeric weighting based on its unique environment or circumstance.

2.0 Formal Risk Assessment Process

2.1 Establish Criteria

Each campus must establish and document two forms of formal risk assessment criteria. These criteria must be adequately communicated to campus departments:

- Criteria for situations in which a formal risk assessment must be performed (i.e. HIPAA, PCI, protected level 1 data, etc.).
- Criteria for situations in which a formal risk assessment may be necessary as determined by the ISO. If a project meets this criteria then the ISO must be notified about the proposed information asset change or acquisition. The ISO will determine whether a formal assessment needs to be performed.

2.2 Identify Formal Risk Asessment Methodology

Working with the procurement, project teams, change management groups and others as appropriate, campuses must establish and maintain a process for identifying information assets on which established criteria is used to determine if a formal risk assessment is required.

2.3 Required Elements of Formal Risk Assessment

Recognizing that risk assessment activities may vary depending on the nature of the risk being assessed, the following elements must be included:

a) Review Frequency
Formal risk assessments must identify a review cycle to ensure that risk management remains appropriate and effective. The length of the review cycle must comply with all applicable laws, policies, standards, and contracts. (For example, the length of the review cycle for PCI and HIPAA risk assessments must not exceed two years.) The review cycle for systems which were identified as "critical" must not exceed three years.

b) Risk Exposure
Each formal risk assessment must use the established risk assessment criteria (See Appendix A) to establish a risk exposure for the identified system, process, asset, etc.

c) Documentation and Retention
Written records of the formal risk assessment and supporting materials must contain sufficient detail to facilitate periodic review and must be retained for a minimum of 3 years.

d) Approval
The campus ISO is responsible for approving the formal information security risk assessment.

3.0 Informal Risk Assessment Process

Informal risk assessments may be used for those systems, assets, processes, etc. not considered critical to the organization and/or which fail to meet the criteria for formal risk assessment. Records of informal risk assessments may be in the form of email or other notes and should contain a statement of the dependencies, premises and facts upon which the opinion is based.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
0.1	11/25/14	Macklin	First draft – ISAC development team	All
0.3	2/6/14	Macklin	Incoroprated team comments	2
.4	3/10/15	Macklin	Incorporated team comments	2
.5	4/28/15	Luvisi	Incorporated CISO comments	2.3
.6	4/29/15	DeCato	Made Cosmetic changes like font type and size	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
6/3/15	Perry (CISO)	Reviewed: Submitted to ITAC/ISAC. Review Timeframe: 6/11/15 until 7/11/15
7/13/15	Perry (CISO)	Approved for Posting

------APPENDIX A----------

Severity Scale (derived from SANS)

Critical - May allow full access to or control of the application, system, or communication including all data and functionality.

- The attacker is not limited in access after execution, they may be able to escalate privileges.
- Possible disclosure of 500 or more records containing sensitive or confidential information.
- Allows modification or destruction of all critical/sensitive data.
- Total shutdown of a critical service or services.

High - May allow limited access to or control of the application, system, or communication including only certain data and functionality.

- The attacker can access the sensitive data or functionality of a user, either limited to a specific piece of data and/or a specific user.
- An outside attacker can execute arbitrary code at the level of the user.
- Ability for a user to access unauthorized functionality.
- Allows limited modification or destruction of critical/sensitive data, either limited to a specific piece of data and/or a specific user.
- Severe degradation of a critical service or services.
- Exposure of sensitive system or application information that provides implementation details that may be used to craft an exploit.
- Breach may be difficult to detect.

Moderate - May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified.

- Weaknesses that can be combined with other vulnerabilities to have a higher impact.
- Disclosure of information that could aid an attacker.
- Any vulnerability that can hinder the detection or investigation of higher impact exploit.
- Fines greater or equal to $10,000 and less than $50,000.

Low - May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified.

- Deviation from a recommended practice or emerging standard.
- May be the lack of a security process or procedure to govern or manage security related activities.
- No direct exposure of data.
- Fines less than $10,000.

- Would not contribute to the exposure of confidential information.
- Would not enable alteration of stored records.
- Would not impact the availability of critical campus systems.

Likelihood Scale

Very High - Exposure is apparent through casual use or with publicly available information, and the weakness is accessible publicly on the Internet.

- Can be exploited by large anonymous population (Any Internet host).
- Vulnerability can be exploited from the general Internet.
- Possible with only publicly available information.
- No specific attack skills are required, such as general user knowledge.

High - The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

- Can be exploited by extended campus population (students, guests)
- Can be exploited by anyone that can reach the network, no authentication required.
- Vulnerability can only be exploited from related networks to which the organization does not control access. (vendors)
- Simple (easily guessable) authentication may be required for exploit.
- Possible with limited knowledge of target configuration.
- Basic attack skills are needed, such as an automated attack (i.e. there exists a metasploit module, or known attack)

Moderate - The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

- Can be exploited by a limited and known population.
- Vulnerability can be exploited through the internal company network or client connection only.
- Simple authentication is required for exploit.
- Vulnerability requires a user to be 'tricked' into taking some action (e.g. a targeted phishing message or a request to go to a website and download a file).
- Possible only with detailed internal information or reasonable guessing.
- Expert technical knowledge is needed such as knowledge of available attack tools.

Low - The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede the vulnerability from being exercised.

- Threat source is employee
- Vulnerability can be exploited through the internal campus network only.
- Single strong authentication is required for exploit.
- Possible only with a significant amount of guesswork or internal information.
- Vulnerability can be exploited with local physical access only and resources have physical access controls, but are still accessible to a large number of people.

Negligible - The threat-source is part of a small and trusted group or controls prevent exploitation without physical access to the target or significant inside knowledge is necessary, or purely theoretical.

- Small and trusted population.
- Vulnerability can be exploited with local physical access only and resources have strong physical access controls.
- A series of strong authentications or multi-factor authentication are required for exploit.
- Possible only with a significant amount of likely detectable guesswork or tightly controlled internal information.
- Attack is theoretical in nature and no known exploit or potential of exploit is currently proven or expected.

Risk Exposure Mapping

		Severity			
		Critical	High	Moderate	Low
Likelihood	Very High	Critical	Critical	High	Moderate
	High	Critical	Critical	High	Low
	Moderate	High	High	Moderate	Low
	Low	Moderate	Moderate	Low	Low
	Negligible	Low	Low	Low	Low

8025.00 | Privacy of Personal Information

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for protecting the privacy of personal information managed by the CSU and guidance for collecting and accessing personal information.

POLICY STATEMENT

100 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 public university 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.

200 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.

300 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 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.

400 Access to Electronic Data Containing Personal Information
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.

8030.00 | Personnel Information Security

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing personnel information security, defines pre-employment requirements, and provides guidance for managing separations or changes in employment status.

POLICY STATEMENT

100 Personnel Information Security
All users are expected to employ security practices appropriate to their responsibilities and roles. 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.

200 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.

300 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.

8030.S000 Personnel Security

Implements:	CSU Policy #8030.000
Policy Reference:	8030.00 Personnel Information Security

6.0 Personnel Security

6.1 Employment Separations and Position Change

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

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

c) It is the responsibility of the employee's manager to identify and define the access privileges needed by the employee to perform the job. The campus must implement a process to ensure that managers evaluate and approve such access privileges within a reasonable period of time after a change in position, job responsibilities, or management reporting structure.

d) Campuses must implement a process to confirm that logical and physical access privileges have been appropriately revoked or changed after separation or position change.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
	8/10/2011	T. Macklin		
	2/21/2012	T. Macklin	Corrected policy reference URL	

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
10/26/12	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	Approved for Posting

8035.00 | Information Security Awareness and Training

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for developing and managing information security awareness and training programs.

POLICY STATEMENT

100 Information 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.

200 Information 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 level 1 or level 2 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.
- CSU and campus notification procedures in the event protected data is compromised.

After receiving initial security awareness training, employees must receive regular updates in policies, standards, procedures and guidelines. The updates should be relevant to the employee's job function, duties and responsibilities.

300 Information Security Training
When necessary, the campus information security program must 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.

8035.S000 Security Awareness and Training

Implements:	CSU Policy #8035
Policy Reference:	8035.00 Information Security Awareness and Training

Introduction

Information Security Awareness and Training programs are a key element of the CSU Information Security Program. Establishment of a campus training and awareness program will ensure that people understand their information security responsibilities and help to reduce the number and impact of information security incidents.

1.0 Campus Security Awareness and Training Program

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

a) Annual review of content, and refresh as necessary to address changes in law, policy or present information security threats.

b) Information security awareness training for new employees. This training must be completed within reasonable proximity to employee start date as established by the campus.

c) Annual information security awareness refresher training for all campus employees who interact with protected Level 1 information assets.

d) Periodic information security awareness refresher training for all campus employees who access information assets on a schedule established by the campus and not to exceed three years.

e) Annual information security training for privileged users (e.g., system and security administrators) who interact with information systems containing protected data.

f) Information security training for the ISO and other managers responsible for developing and coordinating the campus information security program and controls as needed to address changes in law, policy or present information security threats.

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

1.3 Security awareness refresher training may take the form of activities such as brownbag sessions, information on special topics delivered via email and other presentations or publications.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	3/2011	Macklin	Draft Standard	All
1.1	9/2/2011	Moske	Format draft.	All

1.2	6/7/2012	Macklin	ISAC Comments incorporated	All
1.3	9/2/2012	Macklin	Corrections to content and spelling	2.0
1.4	12/13/12	Macklin	ISAC: reword final sentence. Approved.	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
12/13/12	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	Approved for Posting

8040.00 | Managing Third Parties

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing third party relationships and guidance for granting access to third parties.

POLICY STATEMENT

100 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.

200 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.

Third party service providers must not be granted access to campus level 1 or level 2 information assets as defined in the CSU Data Classification Standard until the access has been authorized, appropriate security controls have been implemented, and a contract/agreement has been signed defining the terms for access.

8040.S001 Third Party Security

Implements:	CSU Policy #8040.00
Policy Reference:	8040.00 Managing Third Parties

Introduction

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

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

1.0 Third Party Contract Language

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

a) Include a clear description of the scope of services provided under the contract or purchase order.

b) Clearly state the security requirements for the vendors to ensure that their work is consistent with the CSU security policy and standards.

c) Require compliance with the CSU security policy and standards. Exceptions may only be granted by the campus President (or President-designee) and must be reported to the ISO.

d) Clearly identify any and all types of protected data to be exchanged and managed by the vendor.

e) Identify incident reporting requirements.

f) Require immediate notification of any security breaches associated with Level 1 information.

g) Require notification within a specified period of time of any security breaches associated with all other information.

h) If appropriate, make provisions for CSU to have the ability to inspect and review vendor operations for potential risks to CSU operations or data.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
06/17/2011	Cheryl Washington	Release of New Document	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
02/03/12	ISAC	Approved
06/13/12	William Perry	Approved

8045.00 | Information Technology Security

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing information technology security and guidance for: monitoring CSU information assets; protecting information assets from malicious software; and managing network security and mobile devices.

POLICY STATEMENT

100 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.

200 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 non-quarantined location on a campus network or information system.

300 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.

400 Mobile Devices
Campuses must develop and implement controls for securing protected data stored on mobile devices. 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 level 1 data as defined in the CSU Data Classification Standard. 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.

500 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 for other activities that violate the CSU Responsible Use Policy. Records created by monitoring controls (e.g. logging) must be protected from unauthorized access and reviewed regularly. Campuses must ensure that only individuals who have a “need-to-know” are granted access to data generated from monitoring controls.

Data generated by monitoring must be retained for a period of time that is consistent with effective use, CSU records retention schedules, regulatory, and legal requirements such as compliance with litigation holds. At a minimum, server administrators are required to scan regularly, remediate, and report un-remediated vulnerabilities on critical systems or systems that store protected information within a prescribed timeframe. The risk level of a system determines the frequency at which logs must be reviewed. 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).

8045.S200 Malicious Software Protection

Implements:	CSU Policy #8045.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

1.0 Malicious Software Protection

1.1 All campus information systems must be secured with current versions of campus approved anti-malware software unless otherwise authorized by the campus.

1.2 Campus approved anti-malware software must

a) be capable of detecting, removing, and protecting against malicious software, including viruses, spyware, and adware

b) scan all data in “real time”, including data which is both stored and received by the information system, before data files are opened and before software is executed

c) be capable of tracking and reporting significant actions taken by the software (e.g., deleted or quarantined malware)

d) check for and install updates and signatures at least daily

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

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

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
11/15/2011	Macklin	Incorporation of ISAC Comments	All
1/3/2012	Moske	Formatted	All
1/11/2012	Macklin	Editing, formatting. Final Review	All
3/4/2013	Shaffer	Incorporated changes based on ISAC review	All
3/11/2013	Macklin	Numbering, Musts.	1

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
5/21/2013	ISAC	Reviewed, approved and recommended for CISO review
3/3/2014	CISO	CISO Reviewed, approved. Posted

8045.S300 Network Controls Management

Implements:	CSU Policy #8045.00
Policy Reference:	8045.00 Information Technology Security

Introduction

Campuses must establish a method for documenting the campus network topology, equipment configuration and network address assignments.

1.0 Network Information Requirements

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

1.1 Network topology information containing:

a) The locations and IP addresses of all segments, subnets, and VLANs.

b) Identification of any established security zones on the network and devices that control access between them.

c) The locations of every network drop and the associated switch and port on the switch supplying that connection.

d) A summary representation (e.g., drawing) of the logical design appropriate for managerial discussions.

e) A summary security model appropriate for managerial discussion.

1.2 IP address management

a) Static IP address assignments information sufficient to identify host, contact and device location (for wired ports)

b) Dynamic address server (i.e., DHCP) settings showing:

- Range of IP addresses assigned
- Subnet mask, default gateway, DNS server settings, WINS server settings assigned

1.3 Configuration information network devices such as:

a) Switches

b) Routers

c) Firewalls

d) Any other device critical to the functioning of the network

1.4 Configuration information for devices must include but not be limited to:

a) Net masks

b) Default gateway

c) DNS server IP addresses for primary and secondary DNS servers

d) Any relevant WINS server information

e) Responsible administrator contact information

2.0 Network Documentation Management

2.1 Each campus may determine its specific methods for documentation using any combination of online network tools, databases, or hard copies; however, the resulting information must be in a form and format available for audit and review.

2.2 Each campus must establish a method for self-review of network documentation such that each element is reviewed for accuracy and completeness at least every 36 months, and designated critical system information at least every 12 months.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
10/8/11	Macklin	Incorporation of ISAC and NTA comments	All
11/9/2011	Moske	Formatted	All
1/11/2012	Macklin	Final review	None
12/13/12	Macklin	ISAC Review – Approved to publish.	Intro
9/26/13	Hendricks	Renumbered for consistency	

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
12/13/12	ISAC	Recommended
6/6/13	ITAC	Reviewed
7/16/13	Perry (CISO)	Approved for Posting

8045.S301 Boundary Protection and Isolation

Implements:	CSU Policy #8045.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

Introduction

Campuses must implement controls designed to provide or limit access to networked CSU assets.

1.0 Boundary Protection and Isolation

1.1 Access to campus networks must be controlled by a technical solution which permits only authorized inbound traffic. Campuses must determine, based on risk analysis, the extent to which outbound traffic is blocked or limited.

1.2 The campuses must appropriately separate network access to public information system resources from those which store protected Level 1 and Level 2 information.

1.3 Campuses must establish zoning or separation within internal networks based on established trust relationships, authorized services, and data classification in order to ensure that protected information is not made available to unauthorized persons.

1.4 All unnecessary services (e.g., Web service, SNMP) on any system which is directly accessible from the internet must be disabled.

1.5 All privileged administrator network access to systems which are directly accessible from the internet must be encrypted and authenticated.

1.6 Each campus must maintain documentation as follows:

a) A formal, documented process for approving and testing configuration changes to its network and network control devices.

b) Formal network configuration document that defines all open ports and services on systems directly accessible from the internet.

c) Justification and risk analysis as appropriate for any allowed service or protocol.

d) Annual review for all configurations and firewall rules associated with border devices and/or systems directly accessible from the Internet to determine if the rule is still valid, still necessary and performing the function for which it was requested.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
11/15/2011	Macklin	Incorporation of ISAC Comments	All
1/3/2012	Moske	Formatted	All
1/11/2012	Macklin	Final Review – format	All
6/7/2012	Mackin	Corrected transfer problems – no content change	All
2/19/2013	Macklin	ISAC Comments	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
2/19/13	ISAC	Reviewed, approved and recommended for CISO review
3/03/14	CISO	CISO Reviewed, approved. Posted

8045.S302 Remote Access to CSU Resources

Implements:	CSU Policy #8045.00
Policy Reference:	8045.00 Information Technology Security

Introduction

Campuses must implement controls designed to protect CSU resources from unauthorized access from external hosts while making these resources available to legitimate CSU users who are not on campus.

1.0 Public Access Systems

Public access systems are those made available to the public via the Internet, requiring no special access or authentication process. Examples include, but are not limited to: campus informational web pages and class schedule information.

2.0 Non-Public Access Systems

Non-public access systems, regardless of where they are hosted, are those that are available only after authentication or other special access process. Examples include, but are not limited to: online courses, class registration web pages, and internal campus email systems

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

a) Be authorized and authenticated by use of a unique user identifier.
b) Pass through a campus-approved access control device (e.g., a firewall or access server).
c) Be made using an approved method (e.g. campus-authorized remote desktop service).
d) Use a secure encrypted protocol for the entire session
e) Be logged and tracked consistent with campus logging procedures.

2.2 Non-public access systems must be configured to automatically terminate inactive connections after an appropriate period of time.

3.0 Non-Public CSU-shared Resources

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

3.1 Campuses must identify and communicate:

a) Approved user practices for remote connections.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
10/8/11	Macklin	Incorporation of ISAC and NTA comments	All
11/9/2011	Moske	Formatted	All
1/12/2012	Macklin	Format/Bulleting adjustment	All
7/27/2012	Macklin	Clarified definition remote access compromise	
12/13/2012	Macklin	ISAC: non-public systems may be hosted, CSU shared resources minimum and defn language updated. Reporting of device loss removed as it is covered elsewhere. Approved to publish.	

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
12/13/12	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	Approved for posting

8045.S400 Mobile Device Management

Implements:	CSU Policy #8045.00
Policy Reference:	8045.00 Information Technology Security

Introduction

Campuses must implement controls designed to protect CSU resources that are accessed from or stored on mobile devices.

1.0 Mobile Device Management

As determined necessary by risk assessment, mobile devices must be protected with appropriate security controls. Appropriate security controls can include, but are not limited to:

a) Access control
b) Encryption
c) Strong passwords
d) Anti-virus software
e) Personal firewall

2.0 Storage of Protected Data

2.1 Protected Level 1 data may not be stored on a mobile device unless authorized by appropriate campus administration and encrypted via campus-approved method.

2.2 Each campus must maintain a current inventory of mobile devices that contain protected Level 1 data. This inventory must be reviewed at least annually.

3.0 User Practices for Mobile Devices

3.1 Campuses must identify and communicate approved user practices for mobile device security. Campuses must provide these practices to any individual issued a campus-provided mobile device and include information about mobile device security in security and awareness training material for all campus users.

3.2 Campuses must maintain and publish and a process for users to report if they determine or suspect that any mobile device (including those not provided by campus) which enables access to non-public campus information assets has been lost, stolen, or compromised.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
10/8/11	Macklin	Incorporation of ISAC and NTA comments	All
11/9/2011	Moske	Formatted	All
1/12/2012	Macklin	Final Review	None
2/19/2013	Macklin	ISAC Review/Approved	3.0, 4.0

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
2/19/13	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	Approved for posting

8045.S600 Logging Elements

Implements:	CSU Policy #8045.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

Introduction

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

1.0 Logging Elements

1.1 At a minimum and as appropriate, taking into account the capabilities of the device or application creating the log entries, such controls must track and log the following events:

a) Actions taken by any individual with root or administrative privileges
b) Changes to system configuration
c) Access to audit trails
d) Invalid access attempts (failed login)
e) Use of identification and authentication mechanisms (logins)
f) Notifications and alerts
g) Activation and de-activation of controls, such as anti-virus software or intrusion detection system
h) Changes to, or attempts to change system security settings or control.

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

a) User identification
b) Type of event
c) Date and time
d) Success or failure indication
e) Data accessed
f) Program or utility used
g) Origination of event (e.g., network address)
h) Protocol
i) Identity or name of affected data, information system or network resource.

1.3 Each campus must establish procedures for the retention of logs and monitoring information.

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

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

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
11/15/2011	Macklin	Incorporation of ISAC Comments	All
11/15/2011	Moske	Formatted	All
1/11/2012	Macklin	Format, final review	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
4/23/2013	ISAC	Reviewed, approved and recommended for CISO review
7/16/2013	CISO / Perry	Approved
3/3/2014	CISO	Request to Post

8050.00 | Configuration Management

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing a configuration management program.

POLICY STATEMENT

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

8050.S100 Configuration Management – Common Workstation Standard

Implements:	CSU Policy #8050.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8050.0.shtml

Introduction

Campuses must develop and implement configuration management standards to address information security risks on campus desktop and laptop computers (workstations) along with associated devices which may store data. Other configuration standards include:

- 8050.S200 Configuration Management – High Risk Workstation Standard
- 8050.S300 Configuration Management – Mobile Device Standard
- 8050.s400 Configuration Management – Common Servers Standard
- 8050.S500 Configuration Management – High Risk Server Standard

1.0 Minimum Configuration Features

1.1 Password Management

State owned desktop and laptop computers must comply with the campus password complexity and aging policies.[1]

1.2 Inventory

a) Campus methods for managing computer inventory must have capability of maintaining inventory records for any campus computing devices, such as workstations, laptops, etc.

b) All desktop and laptop computers purchased by the University must be tracked via the campus inventory management system.

c) The campus must establish a periodic inventory process sufficient to ensure that inventory records are current and accurate, and contain information sufficient to support data classification and incident response activities.

d) All devices, including workstations, peripherals, external drives and memory sticks, which store Level 1 protected data must:
   i) Be encrypted using campus approved encryption methods.
   ii) Be tracked and managed via the campus inventory process[2].

1.3 Anti-Virus

[1] Please note CSU Standard 8020.S001 Exception Standard for information to be used for any non-compliant workstation.
[2] See also CSU Standard 8065.S001 Information Security Asset Management § 12.4 (http://www.calstate.edu/icsuam/sections/8000/8065.S001_Information%20Security_Asset_Management.pdf)

Up to date anti-virus software must be installed and maintained on all systems. Regular updates to virus definitions and software must be activated.

1.4 Software Updates

Workstation computers must be configured to allow automatic application of software updates through a patch management system.

1.5 Supported Operating Systems

The desktop or laptop device must use a supported operating system in order to ensure that security vulnerabilities are addressed. Where the campus determines that an exception to this standard applies, the campus exception documentation must include controls sufficient to address the risk.

1.6 Enterprise Management

The workstation must be managed by an appropriate configuration management system, such as a campus enterprise desktop management system, that ensures:

a) The workstation is subject to periodic vulnerability reporting.
b) The success and/or failure of critical patches is reported.

1.7 Inactivity Screen Lock

a) Workstations must be configured with screen locking features to prevent unauthorized access to a machine while not in use.
b) Campuses must identify screen lock time limits appropriate to the purpose of the workstation and the environment in which it is located.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
0.5	6/10/2014	Macklin	First draft – ISAC development team	All
0.6	6/27/14	Macklin	ISAC dev team review	All
0.7	7/22/14	Macklin	Added	1.8
0.9	9/14/14	Macklin	Revised per ISAC review	All
1.0	10/15/14	Macklin	Incorporated campus feedback	§ 1.2(a)
1.1	5/15/15	Macklin	Incorporated feedback from FOA	§ 1.2(b)
1.2	6/9/15	Grayson	Incorporated feedback from Kircher	§ 1.2(b) § 1.2(c) § 1.2(d) 1.4 1.6

1.3	6/17/15	Grayson	Incorporated feedback from Kircher. Cosmetic changes only.	§ 1.2(a) § 1.2(b)

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
06/03/15	Perry (CISO)	Reviewed: Submitted to ITAC/ISAC Review Timeframe:06/09/15 until 07/09/15
7/13/15	Perry (CISO)	Approved for Posting

8050.S200 Configuration Management – High-Risk/Critical Workstation Standard

Implements:	CSU Policy #8050.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8050.0.shtml

Introduction

This standard is intended to provide minimum requirements campuses must implement in order to ensure that those workstations which store or are used to access critical data are protected from unauthorized access.

Other configuration standards include:

- 8050.S100 Configuration Management – Common Workstation Standard
- 8050.S300 Configuration Management – Mobile Device Standard
- 8050.s400 Configuration Management – Common Servers Standard
- 8050.S500 Configuration Management – High Risk Server Standard

1.0 Definitions

A "High Risk" workstation is defined as any workstation that stores or accesses "critical" data or systems.

"Critical data" includes protected level 1 information in such quantities as to require notification of a government entity (i.e. over 500 records under HIPAA or CA 1798.29), or information classified as protected level 1 due to severe risk[1].

"Access to critical systems" means an elevated access privilege[2] to a system which stores protected level 1 information. Examples of this may include access to the Student Health System, access to payment card processing system, access to student financial records, etc.

2.0 High Risk Workstation Governance

2.1 Incorporating Common Workstation Standards

All High Risk Workstations must meet Common Workstation Standards 8050.S100.

[1] See 8065.S02 Information Security Data Classification
http://calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

[2] System support personnel with elevated access required to support campus critical systems or infrastructure may need to utilize the campus Exception process as per the CSU Information Security Risk Mangement – Exception Standard 8020.S000.

2.2 High Risk Workstation Designation

Campuses must implement a process for designating and reviewing the designation of critical or high risk workstations.

2.3 Change Control

The configuration of a High Risk Workstation may not be altered except as approved via the campus Change Control Process.[3]

2.4 Physical Security

High Risk workstations must be physically protected as per the as per the CSU Information Security Standard 8080.S01[4].

3.0 High Risk Workstation Configuration

3.1 Network Protection

In order to protect the high risk workstation from malware and/or data exfiltration, network access must be limited. Additional network protection can be achieved by one or more of the following methods, to be determined by risk assessment:

a) Network traffic limited to the minimum necessary to perform business functions by use of isolated network segment with traffic restricted to authorized inbound and outbound ports and destinations. (Please note that this may be used in combination with a virtual desktop environment for other work functions (web browsing, etc.) in order to address productivity.)
b) Intrusion detection and prevention technologies which address hostile sites, malware, etc.
c) Software defined networking, user based and/or application-defined routing or similar use of technology to control connectivity.

3.2 Protection against "zero day" malware

For high risk workstations with operating systems commonly vulnerable to malware, either restricted outbound network egress (see § 3.2(a)) or application whitelisting must be used in order to protect against "zero-day" malware.

3.3 Host-based Firewall

In order to prevent unauthorized access from other "local" hosts, a Host-Based Firewall must be enabled and configured to restrict access to only authorized hosts.

3.4 Security Event Logging

a) The High Risk Workstation must be configured to log security events:

[3] See CSU Information Security Policy: 8055 Change Control along with associated standard 8055.S001 Change Control Standard

[4] http://www.calstate.edu/icsuam/sections/8000/8080_FINAL_DRAFT_IS_Standard_Physical_Environmental_Security_CW_V5.pdf

b) Campus must identity the logging requirements and configuration settings for the high risk workstation and its application environment including:
    i. Remote or local log storage
    ii. Log retention of at minimum 30 days
c) Log activity must comply with 8045.S600 Logging Elements[5]

3.5 Administrative Accounts

Local administration rights must not be granted to the campus account used for activities such as web browsing. As necessary, the user may be issued a separate local administration account.

3.6 Encryption

High Risk Workstations must use University approved encryption on both the hard drive and removable device peripherals and/or media.

3.7 Remote Support

Remote support applications must be configured to require the user to acknowledge and consent to the remote session.

3.8 High Security Workstation Configuration Checklists

High Risk Workstations must use a current standard secure configuration checklist. Useful resources for developing a checklist include but are not limited to those offered by CIS benchmarks, National Institute of Standards and Technology (NIST USCGB) and/or the Department of Homeland Security. [6]

3.9 Vulnerability Scanning

Periodic vulnerability scans must be completed and assessed in order to verify that operating systems and application are adequately updated (see 8050.S100 Configuration Management § 1.4).

3.10 Peripheral Communications

Peripherals and association communication protocols (e.g. Bluetooth) must either be adequately secured via encryption or disabled in order to avoid unauthorized access and denial of service issues.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
0.1	6/23/2014	Macklin	First draft – ISAC development team	All
0.4	7/22/14	Macklin	After 7/8 ISAC	

[5] See http://www.calstate.edu/icsuam/sections/8000/8045.S600_Logging_Elements.pdf
[6] http://web.nvd.nist.gov/view/ncp/repository (link to it - add to sound business practices.

0.7	9/9/14	Macklin	After 8/26 ISAC Standard Team review	All
0.8	9/9/14	Macklin	Working on… 9.9 meeting	
0.9	9/14/14	Macklin	Changes accepted – publish for ISAC	§ 3.2 and wordsmithing
1.0	9/23/14	Macklin	Incorporated ISAC comments	§ 3.2
1.1	10/14/14	Macklin	Incorporated campus feedback	§ 2.4
1.2	2/24/15	Macklin	Incorporate CISO comment	§ 3.3

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
11/7/14	ISAC	ISAC approved, moved to CISO review
3/2/15	CISO	CISO Reviewed. Next step is collaborative review.
6/4/15	Perry (CISO)	Approved for Posting

8055.00 | Change Control

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing changes to CSU information assets and provides guidance for implementing emergency changes to CSU information assets.

POLICY STATEMENT

100 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 level 2 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 communicate 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.

200 Emergency Changes
Only authorized persons may make an emergency change to campus information assets containing level 1 or level 2 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.

8055.S01 Change Control

Implements: CSU Policy #8055.00
Policy Reference: 8055.00 Change Control

1.0 Introduction

Campuses must establish and document a risk-based process for managing changes to common and shared information assets. Campuses must identify those assets subject to the change control process. However, at a minimum, the campus change management process must include critical and protected information assets.

2.0 Change Management Methodology

The change control review process must include:

a. Identification and documentation of changes.

b. Assessment of the potential impact of changes, including security implications.

c. Identification of a change control authority, which may be vested in either individuals or groups as appropriate.

d. Documented review and approval by the designated change control authority.

e. Methods for scheduling and appropriate notification of significant changes.

f. Methods and standard template for notification to end users of scheduled changes and expected impact.

g. Ability to terminate and recover from unsuccessful changes.

h. Testing procedures to ensure the change is functioning as intended.

i. Communication of completed change details to all appropriate persons.

j. Updating of all appropriate system documentation upon the completion of a significant change.

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

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

3.0 Sample Change Management Methodology

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

	Low Impact Changes	Medium Impact Changes	High Impact Changes
Description of Change	A change intended to repair a fault in an information system or network resource. Such changes can include either the hardware or software components of information systems and network resources.	A change intended to update or upgrade an information system or network resource. Such changes can include major patches or significant changes to system configuration to meet a new policy, security guideline, or campus requirement. Such changes can include either the hardware or software components of information systems and network resources.	A change, which will result in major changes to an information system or network resource. Such changes can include implementing new functions or replacing entire systems. Such changes can include either the hardware or software components of information systems and network resources.
Pre-change Requirements	A change plan, including back-out procedures, must be developed and approved.	A formal risk assessment must be conducted on the change. A change plan, including back-out procedures, must be developed and approved.	A formal risk assessment must be conducted on the change. A change plan, including back-out procedures, must be developed and approved. Information systems or network resources that are being changed must be fully backed up.
Approval Required	• System owner • IT manager	• System owner • IT manager (may include ISO and TSO) • Change control group	• System owner • IT manager (may include ISO and TSO) • Change control group
Post-change Requirements	After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated.	After the change is made, appropriate information system or network resource documentation, operations processes and configuration documentation must be updated. Change results must be logged and reported to change control group.	After the change is made, appropriate information system or network resource documentation, operations processes, and configuration documentation must be updated. Change results must be logged and reported to change control group.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
3/11/2011	Moske	Document Revision: Draft Standards Template	Click here to enter Revision Date

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
9/28/11	Washington	Approved

8060.00 | Access Control

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing access to CSU information assets and guidance for: granting access to CSU information assets; separating duties of individuals who have access to CSU information asset; conducting reviews of access rights to CSU information assets; and modifying user access rights to CSU information assets.

POLICY STATEMENT

100 Access Control
On-campus or remote access to information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard must be based on operational and security requirements. Appropriate controls must be in place to prevent 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.

200 Access Control
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.

300 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 than is required by the employee's job duties.

400 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.

500 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.

8060.S000 Access Control

Implements:	CSU Policy #8060.00
Policy Reference:	8060.00 Access Control

Introduction

Access to campus information assets containing protected data must include a process for documenting appropriate approvals before access or privileges are granted. All changes to user accounts (i.e., account termination, creation, and changes to account privileges) on campus information systems or network resources (except for password resets) must be approved by appropriate campus personnel. Such approval must be adequately documented in order to facilitate auditing of access control practices.

1.0 Access Authorization

Campuses must identify and document individuals who are authorized to define and approve user access to campus information assets. Campuses must document their authorization procedures. Authorizations must be tracked and logged following campus defined processes and must include information appropriate to the nature of the data stored on the information asset. Information should include:

a) Date of authorization
b) Identification of individual approving access
c) Description of access privileges granted
d) Description of business reason for which access privileges were granted

1.1 Granting Access

Authentication controls must be implemented for campus information assets which store or access protected information, and for systems the campus considers critical to operations. Campus-defined controls must take into consideration:

a) The need to validate user identity prior to granting access to protected data.
b) The requirement for unique user accounts and corresponding access privileges.
c) The requirement to deny all access rights until rights are formally approved and assigned.
d) The ability to report repeated failed access attempts.
e) The ability for access rights to be promptly modified or revoked.
f) The need for authentication credentials to be regularly changed.

1.2 User Account Management

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

b) Campuses must establish criteria for expiring, disabling, and removing user accounts on critical systems and campus information systems or network resources that store or access protected information. The period of acceptable inactivity must be based upon the nature of the data and/or the criticality of the system.

c) "Guest" or generic accounts on campus information systems or network resources may be activated only when authorized by appropriate personnel. Any such account created on a critical system must be reported to the campus information security officer.

d) Campuses must establish processes for re-enabling or resetting user accounts once they have been disabled. User identity must be appropriately verified prior to re-enabling or resetting user accounts.

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

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

1.3 Password Management

a) Campuses must identify and implement password criteria which meets NIST Level 1 "Resistance to Guessing Authentication Secret"1 at a minimum. To prepare for InCommon Bronze/Silver implementation, campus should consider meeting NIST Level 2 for "Resistance to Guessing Authentication Secret". Password criteria involves a combination of minimum password length and complexity, password aging, exclusion of dictionary words, and account locking based on failed authentication attempts. Refer to NIST Special Publication 800-63-2 [SP 800-63-2], for a discussion of Authentication Secret complexity and resistance to online guessing. See Appendix A for examples of compliant password criteria and a link to a complexity calculator.

- Complexity: Campuses must implement password complexity standards sufficient to protect against password guessing.
- Failed Attempts: Campuses must identify criteria for disabling (locking) user accounts on critical campus information assets after a number of failed logon attempts, and acceptable timeframes to maintain a disabled state.
- Aging: Campuses must identify and enforce a password change (aging) schedule. The schedule may vary by system or application at the campus' discretion as determined by risk.

b) Critical information systems and those with protected data should use a secure external authentication method, such as a campus directory server.

c) Passwords and credentials that grant access to Level 1 and Level 2 data must not be used as credentials for personal (non CSU) accounts.

d) Password Issuance – When passwords are issued they must be One-Time Passwords/Keys. One-Time passwords (e.g., passwords assigned during account creation, password resets, or as a second factor for authentication) must be set to a unique value per user and changed immediately after first use.

[1] At present, this publication can be located on line at http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-2.pdf

1.4 Password Storage and Transmission

a) Passwords or credentials that grant access to level 1 and level 2 data are classified as level 1 data by the CSU data classification standard. When transmitted electronically, they must be sent via a method that uses strong encryption as per the CSU Information Security Asset Management Standard.

b) All other user account passwords should be protected with strong encryption during storage and transmission.

c) Strong encryption or hash methods must be used to protect any passwords stored in a collection of passwords (database).

d) Campuses may identify service accounts or other low risk applications where password storage or transmission in clear text is appropriate.

2.0 Access Modification

At least annually, appropriate campus managers, data stewards, and/or their designated delegates must review, verify, and revise as necessary user access rights to campus information assets which store or access protected data. All such revisions must be tracked and logged following campus defined processes and must at least include:

a) Date of revision

b) Identification of person performing the revision

c) Description of revision

d) Description of why revision was made

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.1	9/1/2011	Macklin	Incorporate ISAC comments	all
1.2	10/11/2011	Macklin	Incorporate ISAC comments	1.1 – 1.3
1.3	6/1/2012	Arboleda/Harwood	Incorporated CalPoly Pomona comments and Auditor Concerns	1.0, 2.2, 2.3
1.4	6/4/2012	Macklin	Comments to v1.3	All
1.5	6/5/2012	Harwood/Macklin	Final Draft	All
1.6	3/11/2013	Hendricks	Draft Revision Password Mgmt	1.3
1.7	5/2/2013	Macklin	Incorporated comments, Created Appendix A	Primarily 1.3
1.8	5/7/2013	Macklin/Hendricks	Incorporated comments	1.3. 1.4
1.9	5/15/2013	Macklin	Incorporated comments	1.3(a)(1), 1.3(b)

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
6/5/2012	Macklin	Reviewed/Approved
6/5/2012	Perry (CISO)	Approved
5/21/13	ISAC	Recommended Updated Draft
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	Approved for Posting

8060.S000 Access Control - Appendix A

1.0 Examples of password management settings

1.1 Compliant examples of password criteria that Meet NIST Level 1 include but are not limited to:

a) 8 characters, with composition rules, no dictionary check, 90 day lifetime, 3 failed logins lock account for 25 minutes

b) 8 characters, with composition rules, no dictionary check, 180 day lifetime, 3 failed logins lock account for 50 minutes

c) 15 characters, no composition rules, no dictionary check, 180 day lifetime, 3 failed logins lock account for 30 minutes

1.2 Compliant examples of password complexity that meet NIST Level 1 include but are not limited to:

a) Minimum password length of eight (8) characters, password must contain at least three (3) out of the four (4) following character types:

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

b) Minimum password length of fifteen (15) characters, password must use "pass phrase" composed of four (4) words and punctuation

1.3 Compliant examples of failed login attempt lockout settings include but are not limited to:

a) After 8 sequential failed authentication attempts, account is locked for 50 minutes

1.4 Compliant examples of password ageing re-use settings include but are not limited to:

a) Passwords protecting administrative access to Level 1 or Level 2 data must be changed every 90 days

β) Passwords protecting the ability to create application transactions (e.g. create and/or approve purchase requisitions, create general ledger transactions) must be changed every 180 days

χ) Password reuse must be restricted to no more than one in every four (4) password used.

8065.00 | Information Asset Management

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing CSU information assets.

POLICY STATEMENT

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 level 1 or level 2 data as defined in the CSU Data Classification Standard. 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.

Critical or protected 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.

8065.S001 Information Security Asset Management

Implements:	CSU Policy #8065.00
Policy Reference:	8065.00 Information Asset Management

12.0 Asset Management

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

a) Owners of the information within the campus.

b) Custodians of the information.

c) Users of the information.

d) Classification of information to ensure that each information asset is identified as to its information class in accordance with law and administrative policy.

12.1 Data Ownership

Campuses must complete an inventory identifying Level 1 protected data. Campuses must assign ownership of each information asset containing Level 1 protected data. Normally, responsibility for Level 1 protected data resides with the manager of the campus program that employs the information. When the information is used by more than one program, considerations for determining ownership responsibilities include the following:

a) Which program collected the information.

b) Which program is responsible for the accuracy and integrity of the information.

c) Which program budgets the costs incurred in gathering, processing, storing, and distributing the information.

d) Which program has the most knowledge of the useful value of the information.

e) Which program would be most affected, and to what degree, if the information were lost, inaccurate, compromised, delayed, or disclosed to unauthorized parties.

12.2 Data Classification

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

12.2.1 Use of the CSU Data Classification Standard

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

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

12.2.2 Maintaining the CSU Data Classification Standard

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

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

12.3 Data Handling

a) Data owners are responsible for identifying procedures that must be followed to ensure the integrity, security, and appropriate level of confidentiality of their information, subject to ISO review. These procedures may include but are not limited to methods for or restrictions on storage of hardcopy, verbal communication of data, etc. Data stored on campus hardware or media must be appropriately labeled and protected according to its classification.

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

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

12.4 Data Storage

a) Each campus must develop and implement appropriate controls for securing protected data. These controls must ensure the confidentiality, integrity, and availability of the asset.

b) Campus electronic media and hardware on which protected data is stored, distributed or accessed must be located and stored in secure locations that are protected by appropriate physical and environmental controls. Hardcopy material containing protected data must be stored in a locked enclosure.

c) The level of protections provided by these controls must be commensurate with identified risks to the media and hardware including appropriate inventory records and labeling of content.

d) Where the combination of assessed risk, technical feasibility and operational practicality allow, protected level 1 data stored electronically must be encrypted using strong encryption methods.

12.5 Data Retention and Disposition

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

Information that has been identified as or is reasonably believed to be relevant to an existing or potential legal proceeding must be retained while the matter is ongoing in accordance with established campus procedures.

12.6 Data Backup

Information systems or files must be backed up using a schedule which is based on the value of the information asset and the requirements of the campus business continuity plan.

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

Backup media containing protected level 1 data must be encrypted using strong encryption methods.

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

13.0 REVISION CONTROL

Last Revised:

FINAL:

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	6/20/2011	Macklin	Draft Standard	All
1.1	6/20/2011	Moske	Format draft.	All
1.2	6/22/2011	Macklin	Incorporating ISAC comments	§ 12.3 – 12.5
1.3	9/1/2011	Macklin	Added hardcopy restriction to	§ 12.4
1.4	9/14/2011	Macklin	Modified to scope “Protected Level 1”	§ 12.1
1.5	10/11/2011	Macklin	Updated with comments from ISAC	§ 12.3, § 12.6
1.6	1/17/2012	Macklin	Updated with comments from ISAC	§ 12.3, § 12.6

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
10/26/12	ISAC	Recommended
6/5/13	ITAC	Reviewed
7/16/13	Perry (CISO)	Approved for Posting

The California State University
INFORMATION SECURITY MANAGEMENT

Information Security Data Classification Standards

8065.S02 Information Security Data Classification

Implements: CSU Policy #8065.00
Policy Reference: 8065.00 Information Asset Management

1.0 Introduction

This document describes the three levels of data classification that the University has adopted regarding the level of security placed on the particular types of information assets. The three levels described below are meant to be illustrative, and the list of examples of the types of data contained below is not exhaustive. Please note that this classification standard is not intended to be used to determine eligibility of requests for information under the California Public Records Act or HEERA. These requests should be analyzed by the appropriate legal counsel or administrator.

Classification Description: Level 1 - Confidential

Access, storage and transmissions of Level 1 Confidential information are subject to restrictions as described in CSU Asset Management Standards.

Information may be classified as confidential based on criteria including but not limited to:

a) Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.

b) Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU's reputation, and legal action could occur.

c) Limited use - Information intended solely for use within the CSU and limited to those with a "business need-to know."

d) Legal Obligations - Information for which disclosure to persons outside of the University is governed by specific standards and controls designed to protect the information.

Examples of Level 1 – Confidential information include but are not limited to:

- *Passwords or credentials that grant access to level 1 and level 2 data*
- *PINs (Personal Identification Numbers)*
- *Birth date combined with last four digits of SSN and name*
- *Credit card numbers with cardholder name*
- *Tax ID with name*
- *Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name*
- *Social Security number and name*
- *Health insurance information*
- *Medical records related to an individual*
- *Psychological Counseling records related to an individual*
- *Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account*
- *Biometric information*
- *Electronic or digitized signatures*
- *Private key (digital certificate)*
- *Law enforcement personnel records*
- *Criminal background check results*

Classification Description: Level 2 – Internal Use

Access, storage and transmissions of Level 2 - Internal Use information are subject to restrictions as described in CSU Asset Management Standard.

Information may be classified as "internal use" based on criteria including but not limited to:

a) Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.

b) Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary.

Examples of Level 2 – Internal Use information include but are not limited to:

- *Identity Validation Keys (name with)*
  - *Birth date (full: mm-dd-yy)*
  - *Birth date (partial: mm-dd only)*
- *Photo (taken for identification purposes)*
- *Student Information-Educational Records not defined as "directory" information, typically:*
  - *Grades*
  - *Courses taken*
  - *Schedule*
  - *Test Scores*
  - *Advising records*
  - *Educational services received*
  - *Disciplinary actions*
  - *Student photo*
- *Library circulation information.*
- *Trade secrets or intellectual property such as research activities*
- *Location of critical or protected assets*
- *Licensed software*
- *Vulnerability/security information related to a campus or system*
- *Campus attorney-client communications*
- *Employee Information*
  - *Employee net salary*
  - *Home address*
  - *Personal telephone numbers*
  - *Personal email address*
  - *Payment History*
  - *Employee evaluations*
  - *Pre-employment background investigations*
  - *Mother's maiden name*
  - *Race and ethnicity*
  - *Parents' and other family members' names*
  - *Birthplace (City, State, Country)*
  - *Gender*
  - *Marital Status*
  - *Physical description*
  - *Other*

Classification Description: Level 3 - General

Information which may be designated by your campus as publically available and/or intended to be provided to the public.

Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the campus in order to mitigate potential risks.

Disclosure of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets.

REVISION CONTROL

Last Revised:

FINAL: 09/28/11

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	6/16/2011	Macklin	Draft Standard	All
1.1	6/17/2011	Moske	Format draft.	All
1.2	9/23/2011	Macklin	Reformat, updates to definitions	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
9/28/11	Washington	Approved

8070.00 | Information Systems Acquisition, Development and Maintenance

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for managing the acquisition, development and maintenance of CSU information systems.

POLICY STATEMENT

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.

8070.S000 Application Security

Last Revised: **02/26/15**

Final **02/26/15**

REVISION CONTROL

Document Title: Application Security
Author: Information Security
File Reference: 8070.S000_Application_Security.docx

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
8/8/12	Alex Harwood	Copied text from the Sac State Application Standard and made adjustments to make it CSU generic verses Sac State specific.	
2/15/13	Alex Harwood	Major changes done with the team	All
3/1/13	Alex Harwood	Minor changes to the document for final draft	All
6/11/13	Macklin	Updates based on team comments	All
7/2/13	Macklin	Updates based on team comments	All
2/26/15	Leslie DeCato	Corrected references to other standards in document	1.5.2, 1.3

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
2/15/13	Dustin DeBrum	Reviewed
3/1/13	Felecia Vlahos	Approved for submission to Policy/Standard/Guideline
3/1/13	Alex Harwood	Approved for submission to Policy/Standard/Guideline
7/18/2013	ISAC	Reviewed, approved and recommended for CISO review
02/26/15	CISO	CISO Approved. Posted

8070.S000 Application Security

Implements:	CSU Policy 8070.0
Policy Reference:	https://csyou.calstate.edu/Policies/icsuam/Pages/8070-00.aspx

1.1 Application Security Standards

This standard applies to all CSU applications and web environments which:

- Are considered mission critical systems,
- Access protected level 1 information,
- Access protected level 2 information and are accessible from the Internet, or
- Provide an official public campus service or presence.

Application and web development environments must comply with CSU and campus standards and procedures. Contracts for services involving application, web development or hosting must incorporate appropriate language (see *8040S000 Third Party Contract Language*).

Campuses must develop and maintain information security criteria for application development. These criteria must apply both to internally developed applications and those developed by contractors or vendors. Criteria must include a process for ensuring that the campus Information Security Office is made aware of applications which access or provide protected level 1 data.

1.2 Application and Web Development Environment Assessment

Campus procedures for local development must ensure that before development begins:

- The planned application and supporting environment have been documented. Documentation must:
  - Adequately describe the purpose and behavior of the application
  - Identify the type and configuration of the supporting systems and networks.
- Risk analysis verifies that:
  - The application and supporting environment will comply with all applicable policies, standards, and procedures
  - Deploying the application will not introduce any unacceptable risks.

1.3 Application Development and Production Architecture

Development and testing must be performed in a non-production environment.

- Production environments for applications with high risk should run on stand-alone dedicated servers or VM server containers.
- Production servers and development servers which store, process or transmit protected data must be housed in a data center that meets physical and logical security control requirements as per CSU Information Security *Policy 8080 Physical Security*.
- Servers must be placed in the appropriate network zone based on the campus approved network architecture plan as per *8045S4301 Boundary Protection and Isolation Standard § 2.2*.
- Servers should be “hardened” according to the campus configuration procedures in order to ensure that they are secure.

1.4 Application Coding

Applications must be reviewed, tested, and documented as determined by a risk assessment, before being placed into a production environment to ensure vulnerabilities are addressed, including but not limited to:

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

The integrity and availability of source code and/or critical files/folders must be ensured by use of a source code control system and scheduled backups.

1.5 Application Development

1.5.1 Data Security

Within the development environment:

- Application developers must remove all test data and test accounts before deploying an application into a production environment.
- Protected data should be redacted where possible in the development environment.

Within the production environment:

- Sample or example scripts must be removed from production servers.
- Protected data may not be displayed in any documentation.
- Developers must check system, test and development tools and processes to be sure that protected data is not copied or created accidentally. Refer to *CSU Policy 8065 Information Asset Management* along with associate standards.

1.5.2 Logging

Applications should log information as *per 8045S600*.

All log data should be written to an external log server or solution as determined by risk.

Logging should be enabled for operating system, database, network, application server, web server and other components of the application system in order to provide sufficient information for incident or problem analysis. See *8045S600 Logging Elements* for more information about logging requirements.

1.5.3 Applications Collecting Personally-Identifiable Data

CSU Policy 8025.0, Privacy of Personal Information, governs the collection and storage of personal information. Respondents should be informed in advance of the use of "web bugs," URL keywords, or other methods to track respondents' identities. Applications collecting personally identifiable information should, and ecommerce sites must post a web privacy statement describing the type of information collected, how it is to be used, and how it may be disclosed.

1.5.4 Encrypt Protected Information

Applications must encrypt Protected Level 1 information as it is transmitted over the network, including login credentials and session identifiers as *per 8065S000 § 12.3 The SSL/TLS (Secure Sockets Layer)* protocol is the CSU standard for protecting web-based network traffic. Certificates must be used to provide positive identification of applications to users. Servers must have valid certificates, signed by a recognized Certificate Authority.

1.5.5 Application Authentication

Applications that authenticate users must establish sessions using a randomized session identifier that expires after a specified total time or user inactivity.

1.5.6 Access Control

Applications shall implement the philosophy of "default deny". Access application content and environments should be denied except for those users and conditions under which access is specifically permitted.

- Developer access privilege should be limited to the least privilege necessary for development.
- If an application needs a system account, an approved and secure service level account must be created and incorporated into the development of the application.
- Users of applications should be prevented from accessing data to which they have not been granted authorization.

Refer to *8060 – Access Control* and related standards for more information.

1.5.7 Application Management

Each application process should execute with the least set of privileges necessary to complete the job

Any elevated permission (system admin account, dba, etc.) should be protected (on a need to know basis), documented and approved through Access Control Processes. Refer to *8060 – Access Control* and related standards for more information on granting permissions.

1.6 Web and Application Testing and Change Management

The security of applications and information systems must be appropriately documented prior to production deployment.

Developers must test the information system's security controls. These tests must verify that controls are working properly.

Tests should be done from a hacker's point of view, and must be conducted prior to production deployment.

The rigor of the test plan must reflect the risk associated with the application along with the classification of the data being stored or accessed. **NOTE**: The *CSU Data Classification Schedule* is located at http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf .

Developers must document the test plan(s) and test results.

Previously deployed systems must be tested as part of any significant upgrade or as determined by a risk assessment.

1.6.1 Code Reviews

A code review of application code to locate potential security flaws and functionality problems should be performed before production deployment. Any security flaws found should be documented and tracked to resolution.

1.6.2 Web Application Vulnerability Scanning

Web applications should be scanned with an approved web application scanner prior to production deployment and periodically at a frequency determined by risk.

Security vulnerabilities must be remediated or mitigated based on a risk assessment.

1.6.3 Web and Application Change Management

Change management procedures should be in place for all production application implementations.

1.7 Web and Application Periodic Review

Periodic risk assessment reviews should be performed on the application and supporting infrastructure to ensure no new security risks have been introduced.

8075.00 | Information Security Incident Management

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing an information security incident management program.

POLICY STATEMENT

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 and investigate 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 reviewed and documented 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 Systemwide Information Security Management.
- If a breach of level 2 data has occurred, the campus ISO must notify the Senior Director of Systemwide 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.

8075.S000 Information Security Incident Management

Implements:	CSU Policy #8075.0
Policy Reference:	8075.00 Information Security Incident Management

Introduction

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

1.0 Campus Incident Management Plans

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

1.1 ***Identification of a Computer Security Incident Response Team (CSIRT)***. Each campus shall identify the positions responsible for responding to an incident.

1.2 ***Protocol for escalation and internal reporting***. Campus procedures shall outline the method, manner, and progression of internal reporting, so as to ensure that:

a) Appropriate campus officials are informed about appropriate security incidents.

b) The CSIRT is assembled.

c) The incident is addressed in the most expeditious and efficient manner.

d) Any actual or suspected breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is reported immediately to the CSU Chief Information Security Offer.

1.3 ***Procedures for investigating an incident***. Each campus must document and develop appropriate procedures and processes for investigating information security events and incidents. These procedures must include minimal investigative requirements required to determine if protected information was stored on or accessible by a potentially compromised system. Campuses must document the mitigation process after identifying vulnerabilities on previously deployed systems.

1.4 ***Post incident analysis.*** Campuses shall review each incident to identify and apply lessons learned.

2.0 Investigating

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

2.1 Data (includes electronic, paper, or any other medium):

a) Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any Level 1 or Level 2 data.

b) Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29, HIPAA regulations or other legal or contractual obligation.

c) Deliberate or accidental distribution or release of personal information by a campus, its employee(s), or its contractor(s) in a manner not in accordance with law or CSU/campus policy.

d) Data handling compliance failures that constitute information security risk potential.

2.2 ***Inappropriate Use and Unauthorized Access*** – This includes tampering, interference, damage, or unauthorized access to campus information assets. This also includes, but is not limited to: successful virus attacks, web site defacements, server compromises, and denial of service attacks.

2.3 ***Equipment*** – Theft, damage, destruction, or loss of campus IT equipment, including laptops, tablets, integrated phones, personal digital assistants (PDAs), or any electronic devices containing or storing confidential, sensitive, or personal data.

2.4 ***Computer Crime*** – Use of a campus information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

2.5 Any other incidents that violate campus information security policy or conditions that provide substantial information security risk.

3.0 Evidence Collection and Handling

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

3.2 If a campus chooses to maintain its own forensic capability, the campus must maintain procedures and processes for ensuring that evidence and/or information collected under circumstances such as a litigation hold, or Public Information Act request is collected, documented and stored in a manner consistent with legal requirements as appropriate.

4.0 Incident Reporting

4.1 Each campus must identify a point of contact (POC) for information security incident reporting. A campus POC can be an individual (e.g., ISO) or an organization [e.g., IT Help Desk or Computer Security Incident Response Team (CSIRT)].

4.2 A formal, centralized method (i.e., email or phone number) for reporting information security incidents to campus POCs must be provided to users. Each campus must identify and communicate means for users and third parties to report suspected incidents. This information must be part of routine security awareness activities. Any user who observes or suspects that an information security incident is occurring with a campus' information assets must promptly report the incident to the campus' POC. Third parties who observe or suspect that an information security incident is occurring with a campus's information asset must promptly report the incident to their campus business contact. A user must not prevent or obstruct another user from reporting an information security incident in the above manner.

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

5.0 Internal Notifications

5.1 Each campus must inform the CSU CISO of any security incident resulting in exposure of protected information. The notification process must include the following steps:

a) Initial notification informing the CSU CISO that the campus is investigating a potential breach. This notification must be made immediately. If notice is made via voice, the campus must provide an email message confirming that the notice has been made and providing the required elements of § 5.1(b).

b) The initial notification must include the nature of the potential breach, an estimate of the severity – i.e. number of records and types of information at risk of exposure.

c) On completion of the incident risk assessment, the campus ISO must immediately notify the CSU CISO and the campus whether or not the campus has determined that there is a low probability that protected information has exposed.

d) If protected data has been exposed:

a. The CSU CISO will then:

i. Notify CSU Risk Management

ii. Notify the CSU HIPAA Privacy Officer if appropriate (HIPAA related incidents

iii. Notify the CSU OGC

iv. Notify the CSU CIO

v. Notify the CSU CFO if appropriate (PII or HIPAA related incidents)

b. The ISO shall

i. Notify the campus President and CIO as appropriate.

ii. Notify the campus OGC liaison.

c. The campus President shall contact the Chancellor.

6.0 External Notifications

6.1 In the case that external notifications are to be made to impacted party(ies), the notification process must include the following steps:

a) A DRAFT copy of the notification must be sent to the CSU CISO for review.

a. The CSU CISO will then:

i. Review DRAFT and provide input

ii. Send the DRAFT to CSU OGC for review and input

iii. Send updated DRAFT to campus ISO / POC

6.2 In the case that the exposed data contains HIPAA or PII and the impacted group is 500 records or greater, the following steps must occur

a) The ISO will send a DRAFT copy of the notice intended for the appropriate organization (AG, HHS, DOE, Media, etc.) to the CSU CISO.

a. The CSU CISO will then:

i. Review DRAFT and provide input

ii. Send the DRAFT to CSU OGC for review and input

iii. Send the updated DRAFT to campus ISO / POC for external organization

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	3/7/2011	Macklin	Incorporates campus and ISAC comments. TBD Clarification on evidence/forensics	14.X
1.0	3/22/2011	Washington	Formerly known as standard "14". Reformatted and re-arranged text. Add a statement regarding post-event reviews.	All
1.1	1/23/14	Macklin	Updated notification, HIPAA updates	§1, 2, 5
1.2	2/20/14	Perry	Updated notifications	5.1.d, 6

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
3/21/12	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	~~Approved for posting~~
2/20/14	CISO	Reviewed Approved for posting

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	3/7/2011	Macklin	Incorporates campus and ISAC comments. TBD Clarification on evidence/forensics	14.X
1.0	3/22/2011	Washington	Formerly known as standard "14". Reformatted and re-arranged text. Add a statement regarding post-event reviews.	All
1.1	1/23/14	Macklin	Updated notification, HIPAA updates	§1, 2, 5
1.2	2/20/14	Perry	Updated notifications	5.1.d, 6

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
3/21/12	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	~~Approved for posting~~
2/20/14	CISO	Reviewed Approved for posting

8080.00 | Physical Security

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU information Security policy provides direction and support for protecting limited access areas from unauthorized physical access.

POLICY STATEMENT

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 limited-access 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 review and document physical access rights to campus limited-access areas annually.

8080.S01 Physical and Environmental Security

Implements: CSU Policy #8080.00
Policy Reference: 8080.00 Physical Security

1.0 Introduction

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

a. Manage control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by campus staff and outsiders.

b. Prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

2.0 Security Zones

Campuses must assign an appropriate security zone designation to their physical areas. Appropriate physical controls must be implemented in shared and limited access security zones to manage access. Campuses must review these controls regularly.

Zone	Brief Description	Necessary Controls
Public	No information assets containing protected data or critical systems are located in the area. (Example: Student Union, Library open areas)	None. Access to this area can be unrestricted.
Shared Access	An area containing one or more protected information assets or critical systems. Persons in the area include those who do not have authorization to protected information assets or critical systems stored in the area. (Example: Administrative Offices)	Appropriate physical access controls and construction must be implemented to restrict access to protected information assets or critical systems that reside in the area.
Campus Limited Access Area	An area containing one or more protected information assets or critical systems. Persons in the area are authorized to access the	Appropriate physical access controls and construction must be implemented that limit access to the area to only persons having a need for specific access in order to accomplish a legitimate task. The controls must enforce the principles of need to know and least possible privilege.

Zone	Brief Description	Necessary Controls
	protected information assets or critical systems. (Example: Data Center)	All physical access to such areas must be controlled by mechanisms such as tracking and logging. Access records must retain information such as: • Records identifying persons with keys (credentials, etc) • Where possible, systems must provide o Date and time of access o User ID performing access

3.0 Work Area Security

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

a. Ensuring that protected data is not left unattended.

b. Limiting the viewing of protected data from unauthorized users.

4.0 Viewing Controls

Information systems accessing protected data must not be left unattended or unsecured. Activation of automatic locking software or log off from the systems must occur when information systems are unattended.

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

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
3/11/2011	Lisa Moske	Document Revision: Draft Standards Template	Click here to enter Revision Date
3/17/2011	Washington	Reformatted document. Updated the “Security Zones” and “Data Center Access” sections.	
3/22/2011	Washington	Replaced bullets with letters. Deleted “Data Center Access” section.	

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
9/28/11	Washington	Approved

8085.00 | Business Continuity and Disaster Recovery

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing a business continuity and disaster recovery program.

POLICY STATEMENT

An information security program needs to support the maintenance and potential restoration of operations through and after 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 campus program must be in compliance with the CSU Business Continuity Program.

8090.00 | Compliance

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for establishing a system-wide information security compliance program.

POLICY STATEMENT

The CSU Information Security Management Office 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 Information Security Management Office 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. The campus policies and standards must include monitoring controls that ensure ongoing compliance with applicable laws, regulations, and CSU policies.

8095.00 | Policy Enforcement

Effective Date: 4/19/2010 | **Revised Date**: 4/19/2010

POLICY OBJECTIVE

The CSU Information Security policy provides direction and support for enforcing the CSU Information Security Policy.

POLICY STATEMENT

The CSU respects the rights of its employees and students. In support of the CSU Information Security policy, campuses must establish procedures that ensure investigations involving employees and students suspected of violating the CSU Information Security policy are conducted in compliance with appropriate laws, 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 and the California Education code. Student infractions of the CSU Information Security policy must be handled in accordance with the established student conduct process. Auxiliary employees who violate the requirements of the policy may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the CSU.

The CSU may also refer suspected violations to appropriate law enforcement agencies.

8100.00 | Electronic and Digital Signatures

Effective Date: 4/1/2011 | **Revised Date**: 12/5/2012

POLICY OBJECTIVE

It is the policy of the CSU to permit the use of electronic or digital signatures in lieu of handwritten signatures. Usage of electronic or digital signatures is at the option of an individual campus or the Chancellor's Office provided they conform to the terms set forth in this policy.

This policy does not pertain to facsimile signatures printed on checks issued by the CSU.

POLICY STATEMENT

100 Electronic Signatures
An electronic signature is an electronic sound (e.g., audio files of a person's voice), symbol (e.g., a graphic representation of a person in JPEG file), or process (e.g., a procedure that conveys assent), attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record.

200 Digital Signatures
A digital signature is a specific type of electronic signature that uses cryptographic transformation of data to provide authenticity, message integrity, and non-repudiation.

For a digital signature to be valid, it must be created by a technology accepted for use by the State of California and conform to technologies capable of creating digital signatures as set forth in California Government Code Section 16.5:

(1) It is unique to the person using it;

(2) It is capable of verification;

(3) It is under the sole control of the person using it;

(4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated;

(5) It conforms to Title 2, Division 7, Chapter 10, of the California Code of Regulations.

300 Electronic and Digital Signature Implementation
Campuses must develop procedures to identify, evaluate, and document where electronic signatures are permitted and digital signatures are required. Procedures should follow a risk assessment methodology defined in the Electronic and Digital Signature Standard and must be approved by the Vice President for Administration/CFO.

Campus and Chancellor's Office standards and procedures for electronic signatures must meet CSU electronic and digital signature standards and may be used for transactions between the CSU and outside parties only when approved by the campus Vice President for Administration/CFO and when both parties have agreed to conduct transactions by digital means.

400 Acceptable Use
Simple Electronic Signatures may convey intent of an individual to sign a record and are often easier to implement. Simple electronic signatures may be acceptable and authorized for internal campus or Chancellor's Office uses involving low risk.

Digital Signatures may be used where simple electronic signatures are acceptable and authorized for use. They may be permitted or required for any record or document where a signature is required by Federal law, California law, or by CSU policy unless a handwritten signature is explicitly required. Digital signatures must be used instead of a simple electronic signature when legally required or when greater risk exists.

The presence of an electronic signature does not mean that a record was properly signed or that the signatory was authorized. Campus and Chancellor's Office procedures must identify the person by position who is authorized to sign, approve, and/or prevent unauthorized actions from being taken as a result of an electronic signature.

CSU Electronic and Digital Signature Standards and Procedures, 8100.S01

Last Revised: **05/21/2012**

REVISION CONTROL

Document Title: CSU Digital Signature Standards and Procedures
Author: Information Security and Identity Access Management
File Reference: CSU Electronic and Digital Signature Standards.docx

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
N/A	Sheryl Okuno	Original Document - LA	N/A
08/16/2011	Michael Trullinger	Release of New Document	Multiple
09/26/2011	Javier Torner		Multiple
09/27/2011	Mark Hendricks		Multiple
09/29/2011	Michael Trullinger	Review – No Significant Additions	Multiple
11/04/2011	Mark Hendricks		Multiple
11/09/2011	Working Group		Multiple
11/09/2011	Michael Trullinger		Multiple
11/10/2011	Michael Trullinger & Mark Hendricks	Corrections and Revision	Multiple
12/14/2011	Michael Trullinger	Included feedback from ISAC	Multiple
04/27/2012	Michael Trullinger	Feedback from OGC, Risk Management, HRM, Audit	Multiple
05/21/2012	Michael Trullinger	Minor Corrections – 1.0 Release	Multiple

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
Click here to enter Review Date	Click here to enter Reviewer	Click here to enter Reviewed, Recommended or Approved

Table of Contents

Page

Introduction

As organizations move away from paper documents with ink signatures, the ability to sign electronic transactions and documents for business, financial, or other reasons is important, if not essential. There is a considerable amount of confusion surrounding signature technologies, and how they might be used for purposes such as signing an electronic document, signing or encrypting an email, or indicating approval in an electronic workflow process.

These standards and procedures are meant to be referenced by anyone requesting, using, or accepting a CSU approved electronic signature and their intent is to:

- Provide the framework for evaluating the appropriateness of an electronic signature technology for an intended purpose
- Establish a CSU System-wide standard for the management and issuance of "key material" used for digital signatures
- Enable greater adoption of digital signature technology across the CSU to streamline business processes, improve identity proofing processes, and increase information security

The legal definition for electronic signatures has been established in the US Federal Electronic Signatures in Global and National Commerce (ESIGN) Act of 2000 and is very broad. A risk based evaluation using OMB 04, 04 "E-Authentication Guidance for Federal Agencies" and NIST SP800-63 must be performed by an organization to determine risks associated with using an electronic signature method and the quality as well as security of the electronic signature method required.

For many day-to-day cases, a simple electronic signature (generated through an authentication or "click to accept" process) is adequate to indicate that an individual has demonstrated intent to sign or approve a transaction. Others cases will require or prefer use of a digital signature.

A digital signature is a very specific form of an electronic signature which uses cryptography to establish the authenticity and validity of the signature with much greater certainty. A digital signature may be utilized where an electronic signature is required. For transactions where there is a greater risk to the CSU, or where a "wet" signature is typically required, digital signatures must be used instead of a simple electronic signature.

Entities Affected

These standards and procedures apply to all members of the CSU community and govern all applications of digital signatures used to conduct official University business. They also apply to transactions between the CSU and other parties.

1.0 Electronic and Digital Signature Definition

An ***electronic signature*** is an electronic sound (e.g., audio files of a person's voice), symbol (e.g., a graphic representation of a person in JPEG file), or process (e.g., a procedure that conveys assent), attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record (ESIGN Act of 2000). A digitally reproduced (e.g. scanned) physical signature is a common example.

A ***digital signature*** is the cryptographic transformation of data, which when added to a message, allows the recipient to verify the signer and whether the initial message has been altered or the signature forged since the

transformation was made. A digital signature is an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a handwritten signature.

Electronic signatures issued by the CSU are considered property of the CSU and are for University business only. Private keys used for digital signatures are considered 'Level 1' confidential data whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damages to the CSU, its students, its employees, or its customers.

2.0 Electronic and Digital Signature Legality

Under California law, a digital signature has the same force and effect as a manual signature. A digital signature may be affixed to any written communication with the University in which a signature is required so long as it complies with the requirements of California Government Code section 16.5 and these Standards and Procedures.

The legality and enforceability of a signature are typically evaluated based on the answer to the following questions:

- Does a signature represent the intent of the signatory?
- Could the statement have been altered?
- How certain is the signatory's identity?

Simple Electronic Signatures may convey the intent of an individual to sign and are often easier to implement, but usually cannot provide satisfactory assurance if authentication, non-repudiation, and integrity are legally required. Determining appropriateness of an electronic signature type (e.g. digital signatures using PKI or a simpler electronic signature) is based on level of risk. A higher assurance level signature may be required for enforceability.

3.0 Reasons for Applying a Digital Signature

The most common reasons for applying a digital signature are authentication, integrity, and non-repudiation.

Authentication

Digital signatures can be used to authenticate the source of messages, documents, and digital content. When ownership of a digital signature secret is known to a specific person only, the digital signature created by that secret can be used to validate authenticity of a person's digital signature.

Integrity

A recipient may need confidence that content they have received has not been altered during transmission. Although encryption technology can be used to secure transmissions, it does not guarantee that the content being protected has not been changed without the author's knowledge. The integrity of authorship of digitally signed content is maintained with or without encryption, as long as the process used to create, store, or retrieve the digitally signed content does not permit content to be changed without invalidating (and where appropriate removing) the signature.

Non-repudiation

Digital signatures can provide non-repudiation. Non-repudiation means that signatories cannot successfully claim they did not sign a message while concurrently claiming that the secret part remained solely in their possession. Some non-repudiation practices include a time stamp for the digital signature that can be used to determine signature validity when the date and time of a compromised secret can be determined.

4.0 General Standards and Requirements

A digital signature is based on an asymmetric cryptosystem that uses a mathematical formula to scramble content. With use of appropriate technology, signatories can encrypt (scramble) content, and recipients can decrypt (unscramble) and verify it. To affix a digital signature or scramble electronic content, a signatory must obtain a digital signature from an accepted authority which typically consists of an electronic asymmetric key-pair (includes a private (secret) key and publicly distributable key).

For a digital signature to be considered valid, it must be:

- Capable of verification
- Linked to content in such a manner that if the content is changed, the digital signature is invalidated (and where appropriate and necessary, removed).
- In conformity with Title 2, Division 7, Chapter 10, of the California Code of Regulations
- Issued by an authority

5.0 Acceptable Use

Electronic and digital signatures are permissible for many record types and activities. Digital Certificates, specifically, can be issued for the purposes of authentication, signing and securing e-mail messages or electronic documents, and encrypting content. Procedures used for issuing certificates that will be used to encrypt sensitive documents and data, including S/MIME email messages, should be carefully developed after assessing retention requirements since key backup and/or escrowing may be necessary to decrypt the source content. If a Digital Certificate is issued for authentication and signing only, key backup and escrow may be unnecessary.

5.1 Agreement to Conduct Electronic Transactions

Digital signatures may be used for transactions between the campus, the Chancellor's Office, and outside parties only when the parties have agreed to conduct transactions by electronic means. The party's agreement to conduct transactions electronically may be informal or recognized through a contract, including cases where a party's action indicates agreement.

5.2 Signature Required by University Policy

When a CSU or campus policy requires that a record have the signature of a responsible person, that requirement can be met if the associated digital signature was issued and is maintained using an approved digital signature method and procedure.

5.3 Signature Required by Law

When an authorized representative of a CSU campus uses an approved digital signature method for a signing required by a third party, the CSU will consider the valid digital signature as having met the requirement.

6.0 Risk-based Approach for Determining Appropriate Electronic Signature Type

Individuals and organizations within the CSU wanting to use electronic signatures must conduct a thorough review of associated risks and must select the appropriate, approved technology. OMB 04-04, FIPS 199, and NIST 800-64 provide mechanisms to establish risk and consequences for business processes.

6.1 Level of Assurance for Authentication Definitions

Electronic authentication is the process of establishing confidence in user identities electronically presented to an information system (NIST SP800-63). "Level of Assurance" is the structure used by the CSU to define the technical and procedural practices to determine authentication certainty.

6.2 Determining Risk

OMB 04-04 "E-Authentication Guidance for Federal Agencies" defines four levels of identity authentication, their associated technical requirements, and risk assessment criteria for determining the impact of authentication errors. In their simplest terms, they are:

- **Level 1**: Little or no confidence in the asserted identity's validity.
- **Level 2**: Some confidence in the asserted identity's validity.
- **Level 3**: High confidence in the asserted identity's validity.
- **Level 4**: Very high confidence in the asserted identity's validity.

OMB 04-04 also identifies six potential impact categories for authentication errors:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Impact values assigned by OMB for these categories of harm are defined in Federal Information Processing Standard 199, "Standard for Security Categorization of Federal Information and Information Systems."

Impact Values (FIPS 199)

- **Low**: The loss of confidentiality, integrity and availability could be expected to have a limited adverse effect on organizational operations, organization assets or individuals.
- **Moderate**: The loss of confidentiality, integrity and availability could be expected to have a serious adverse effect on organizational operations, organization assets or individuals.

- **High**: The loss of confidentiality, integrity and availability could be expected to have a severe or catastrophic adverse affect on organizational operations, organization assets or individuals.

Potential Impact of Financial Loss

- **Low**: at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- **Moderate**: at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- **High**: severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

***Table 1** – Maximum Potential Impacts for Each Assurance Level*

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	L	M	M	H
Financial loss or agency liability	L	M	M	H
Harm to agency programs or public interests		L	M	H
Unauthorized release of sensitive information		L	M	H
Personal Safety			L	M-H
Civil or criminal violations		L	M	H

NIST 800-63 Electronic Authentication Guideline provides technical requirements for each of the authentication levels of assurance defined in OMB 04-04. Each assurance level has defined controls for identity proofing, token (secret) requirements, and authentication/assertion protection mechanisms as published in NIST 800-63.

7.0 Evaluation Process for Use of Electronic Signature

7.1 Evaluation of Risk

An evaluation must first be performed by the authoritative Operational Unit to determine risks associated with using an electronic signature, including the quality, security, and method required for a given type of content or document. This evaluation process should use the E-Authentication Guidance for Federal Agencies, OMB 04-04 for reference and guidance. The results of that assessment must be documented and included with the official record of approval and any proposals submitted to the record custodian.

7.2 Determination of Electonic Signature Methodology

The electronic signature type selected for a document, content, method, or business process should be commensurate to the assurances needed to mitigate the identified risks. Additionally, specifications for recording, documenting, and/or auditing the electronic signature as required for non-repudiation and other legal requirements shall also be determined by the authoritative operational unit. The lowest cost and least complex method for mitigating risk are generally acceptable. The *National Institute of Standards and Technology (NIST) Electronic Authentication Guidelines* publication (referenced in this document) should be consulted when making this determination.

7.3 Use of "Lower Assurance" Electronic Signature Methods

Operational Units that propose electronic signature methods that are at a lower level of assurance than indicated in the risk assessment process shall:

- Describe the reason for variance
- Identify the potential risk of using a tool from a lower assurance level than the risk assessment identifies
- Justify why a lower assurance level method is appropriate
- Identify the steps that will be taken to mitigate the risk
- Obtain the signed approval of the operational unit director and include it with the official record approving use of an electronic signature method

8.0 Acceptable Forms of Electronic Signatures

8.1 Electronic Forms

The selection of an option (e.g. tick box or button) on an electronic form to indicate agreement can be used as a replacement for written signatures when the appropriate functional requirements are met and the technology used records:

- Intent of agreement
- Information that clearly identifies (e.g. by recording the login username) the individual who has 'signed' the agreement
- Within an auditable trail that the form was signed

Furthermore, the signatory's identity must be accessible for the length of the retention period required for the form, as set out in the CSU or Campus Records Retention Schedule. The technology used should also restrict the form once 'signed' such that the contents of the form cannot be changed without the signature being invalidated.

8.2 Scanned Image of a Handwritten Signature

A scanned image of a handwritten signature can be used as an equivalent to a written signature if signing internal CSU data when the appropriate security requirements have been met. Scanned images of a signature must only be used where express permission has been granted by the author and is considered acceptable for high volume processes such as mass mailings. Given the ease with which images may be manipulated, images without other forms of authenticity should be used for **low risk transactions only.**

8.3 Authorization by Email

Acceptance or agreement of intent through an official, controlled Email system (e.g. receipt of an email through the University email system) may be used when the appropriate functional requirements, risk, and security have been carefully considered. Given the ease with which emails may be manipulated, email receipts without other forms of authenticity should only be used for **low risk transactions** and may not be accepted from "generic or shared" email accounts unless the appropriate controls are in place to establish the actual sender.

9.0 Acceptable Forms of Digital Signatures

For a digital signature to be valid it must be created by a technology accepted for use by the State of California and that has been adopted by the CSU. Acceptable California State technologies currently include public key cryptography and signature dynamics. The most common technology used is public key cryptography. It has a greater degree of verifiability than signature dynamics, does not require the additional handwriting analysis steps of signature dynamics, and is *the only technology accepted by the CSU.*

9.1 Public Key Cryptography

Public Key Cryptography

Public Key Cryptography (PKC) signatures allow for third party verification of a signature and are affixed to electronic content using software enhancements to existing applications and web browsers. PKC signatures accepted by the CSU must be issued through a Public Key Infrastructure (PKI) scheme and which results in an asymmetrical digital certificate.

9.2 Encryption

Custodians or users of institutional administrative data who deploy personal digital certificates for encryption must establish procedures ensuring that the CSU has access to all such records and data. Each major operating unit deploying personal digital certificates for encryption is required to implement procedures to archive, secure, and utilize "master recovery keys".

Any custodian or user of institutional administrative data who deploys software or algorithmic programs to encrypt data is required to inform his or her supervisor prior to deployment and disclose, in a comprehensible form, the keys or other means to access the data.

10.0 Digital Certificates

10.1 Minimum Requirements

For a digital certificate to be considered valid, it must follow California State requirements and:

- Identify the issuing Certificate Authority (CA) that has been authorized by the California Secretary of State.
- Uniquely identify its subscriber
- Include its subscriber's public key
- Identify its operational period
- Be comparable against a well-known Certificate Revocation List (CRL) to confirm its validity
- Be digitally signed by the issuing CA

10.2 Approved Authorities

A *Certificate Authority* is commonly a well-known, third party entity that is entrusted to issue digital certificates, verify matching of pubic keys to identity information, and provide a current revocation list. A Certificate Authority, or their delegates, has the responsibility to verify the identity of a subscriber before issuing a certificate.

California State

The list of approved California State authorities is currently available at:

http//www.sos.ca.gov/digsig/

California State University System

The CSU has adopted the InCommon Client Certificate Service as a preferred vendor for PKI digital signature certificates. The California Secretary of State has approved and included this CA in their list under their root name, "COMODO Ltd".

11.0 Issuance and Maintenance

Individuals and organizations within the CSU that want to use electronic signatures must conduct a thorough review of associated risks and must select the appropriate approved technology. OMB 04-04, FIPS 199, and NIST 800-64 provide mechanisms to establish risk and consequences for business processes. If the decision to use digital signature certificates is made, the appropriate validation type must also be selected.

InCommon Digital Certificate Validation Types

A **Standard Validation** type certificate may be issued to an individual whose campus identity meet both Federal NIST Level 1 requirements and these additional requirements:

- Has a valid I-9 Employment Eligibility Verification form or comparable form on record with the issuing campus.
- Has an electronic credential* provided by the campus that can be uniquely matched to the individual's valid I-9 record or comparable form
- Was issued in such a way that ensures and maintains:
  - Single ownership and use of the credential
  - Distribution which ties the unique electronic credential to the individual who submitted the associated I-9 record or comparable form

When met, a digital certificate may be issued through automated processes using that electronic credential*. Standard validation certificates are currently available for employees only.

A **High Validation** type certificate may be issued to an individual whose campus identity verification processes meet Federal NIST Level 3 requirements as well as requirements for issuance of a Standard Validation type certificate. High Validation certificates may not be issued through an automated process.

12.0 Registration

Registration is the process by which an individual or server identifies and authenticates itself before a digital certificate can be obtained. Applications and servers that require the ability to electronically sign a transaction may be issued a certificate through a designated data steward. Data stewards must submit documentation that includes a description of ongoing system administration and maintenance practices, system access controls procedures, event logging configurations, and security incident response procedures prior to issuance.

12.1 Duration and Expiration

All digital signatures must contain an expiration date. It is recommended that the expiration date not exceed one year from the date of original issue or date of last renewal and may not exceed 3 years.

12.2 Revocation

When a signature is issued, it is expected to be in use for its entire validity period; however, circumstances may require it to be invalidated sooner. Revocation may be requested by the subscriber, a Data Steward, or Information Security under the following conditions:

- The individual who was issued the signature has undergone a name change
- There is a reason to believe that the secret portion of the signature or the storage of it has been compromised
- There is substantive reason to believe that misuse has occurred or is likely to occur
- There is reason to believe the signature is not being used in compliance with these standards
- Related security concerns were identified during an audit
- The subscriber's relationship with the issuing campus has been discontinued
- The minimum requirements for the issued signature are no longer met by the subscriber

13.0 Storage and Protection

13.1 Escrow

The purpose of escrowing electronic signatures or portions of them is to provide access to institutional administrative data by ensuring that access does not become dependent on a single individual or an obscure method of storing and/or protecting them. Signatures or portions of them used for encrypting content require escrowing. Escrowing of private keys for digital signatures must be maintained by the Certificate Authority (CA) issuing the keys.

13.2 Key Recovery

Campuses must develop procedures for retrieval of escrowed materials, such as private keys.

Campus Key recovery procedures should include the following:

- Formal process for logging key recovery and approval
- Key recovery authorization should include at least one campus official. For instance; Key recovery may be approved by the appropriate Data Steward and the campus Information Security Officer.

13.3 User Device Storage

Certificates issued for low to medium risk application may be installed in desktop applications such as email clients and web browsers. High Risk/Level of Assurance certificates must be stored in FIPS 140 approved trusted cryptographic devices such as a smartcard or e-Token device. Private keys are CSU Level 1 data and must be protected via encryption.

13.4 Retention

Record Retention

Electronic signature archives and system activity logs must be retained in accordance with CSU Records Retention policies. Record retention schedules should be updated to reflect the use of electronic and digital signatures, as well as encryption.

The minimum record retention period for registration data for digital certificates is seven years and six months beyond the expiration (or revocation, whichever is later). All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

13.5 Recovery, Including Disasters

Campuses and the Chancellor's Office must develop procedures for business continuity and disaster recovery of master recovery keys.

14.0 Roles and Responsibilities

14.1 Digital Signature Subscriber

A subscriber is the individual who has been provided a digital signature certificate for the purpose of signing. The subscriber is responsible for:

- Providing accurate information when applying for a digital certificate
- Taking reasonable precautions to protect and not share the secret portion of the digital certificate (e.g. storing a certificate private key in a password-protected container), ensuring that the digital certificate is under their sole control
- Using the digital certificate only for authorized, legal and University purposes
- Providing written notification to campus Information Security immediately if the secret portion of the signature is believed to have been compromised
- Using their digital certificate for authorized purposes
- Renewal of expired certificates

14.2 Certificate Administration

Certificate administrators are the parties responsible for management of certificate infrastructure, up to and including those responsible for issuance and distribution of digital certificates. The parties are responsible for:

Certificate Authority

- Adequately and safely storing backup copies of all files necessary to re-establish and operate the Certificate Authority
- Timely publication of certificates and revocation information

System

- Protection of escrowed materials, and institutional escrow keys required for certificate retrieval
- Delegation of authority to issue certificates

Issuance and Distribution

- Notification of issuance of a certificate to the subscriber who is the subject of the certificate
- Notification of issuance of a certificate to others than the subject of the certificate

14.3 Data Steward

Data stewards are the individual(s) responsible for a segment of institutional data. Data stewards are responsible for the following as it relates to digital signatures of content germane to their duties:

- Physical and electronic security of any signed data
- Evaluation of transactions enabled by digital signature
- Seeking approval for use of a digital signature from University Legal Counsel or Information Security
- Seeking technical advice from Information Technology Services
- Acknowledgement of applicable liability caps and warranties
- Digital signature verification

14.4 Campus and Chancellor's Office

CSU Campuses, and likewise the CSU Chancellor's Office, is responsible for maintaining operational and business practices in accordance with these standards and procedures.

14.5 University Legal Counsel

University Legal Counsel may be requested to review and potentially approved the proposed use of a digital signature to determine if it is legally permitted.

14.6 Information Security Office

The Information Security Office is responsible for providing security guidance and for assisting in the auditing process, where assigned. The responsibilities may include and are not limited to:

- Reviewing the digital signature uses and providing recommendations to Data Stewards and the campus Vice President for Administration, including evaluation of associated risks
- Assuring proper issuance and maintenance of campus procedures and subscriber credentials
- Notifying a Certificate Administration and Data Stewards within 24 hours of suspected compromises
- Reviewing digital signature implementations and conducting and documenting periodic audits of those implementations at least every three years
- Providing assistance to develop new (or refine existing) campus practices and procedures to ensure protection of digital signatures and their appropriate use
- Notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended
- Notification of revocation or suspension of a certificate to others than the subject whose certificate is being revoked or suspended

14.7 Campus Vice President for Administration

The Vice President for Administration is responsible for delegating campus electronic and digital signature review and audit responsibilities. Final approval or dismissal of campus use of a digital signature is at the Vice President

for Administration's discretion. Determination of approval or dismissal for specific uses may also be made after a review has been conducted by the appropriate data steward.

15.0 Appendix A: Definitions

#	Term	Definition
1.	**Approved Certification Authorities**	The list of certification authorities approved to issue certificates for digital signatures.
2.	**Asymmetric Cryptosystem**	A computer algorithm or series of algorithms which utilize two different keys with the following characteristics • one key signs or decrypts content; • one key verifies or encrypts content; and, • the keys have the property that, even when one key is known, it is computationally infeasible to discover the other key.
3.	**Asymmetric Key-Pair**	A private key and its corresponding public key in an asymmetric cryptosystem. Public keys can be used to verify a digital signature created with the corresponding private key and to encrypt content.
4.	**Certificate Authority**	A person or entity that issues a certificate and certifies amendments to an existing certificate.
5.	**Compromised**	
6.	**Digital Certificate**	Also known as a public key certificate or identity certificate, a digital certificate is an electronic document which uses a digital signature to bind a public key with an identity, such as the name of a person or an organization and address. The certificate can be used to verify that a public key belongs to a person.
7.	**Digital Signature**	A *digital signature* is the cryptographic transformation of data, which when added to content, allows the recipient to authenticate the signatory and whether the content has been altered or the signature forged since the transformation was made.
8.	**Data Steward**	An individual who is responsible for the maintenance and protection of data. The duties include but are not limited to performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in CSU/campus security policies and standards.
9.	**Electronic Credential**	Digital documents or identifiers that are bound to a natural person's identity for the purposes of authentication.
10.	**Electronic Signature**	Any electronic data that carries the intent of a signature (not all electronic signatures use digital signatures).
11.	**Level 1 Confidential Data**	Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.
12.	**Master Recovery Key**	
13.	**Private Key**	The secret key of a key pair used to create a digital signature or decrypt data.
14.	**Public Key**	The well-known key of a key pair used to verify a digital signature or to encrypt data.
15.	**Public Key Cryptography**	An encryption method that uses an asymmetric key-pair.
16.	**Signature Dynamics**	A measurement of the way a person writes his or her signature by hand on a flat surface, binding the measurements to a message through the use of cryptographic techniques.
17.	**Sole Control**	
18.	**Subscriber**	An individual or organization that has been provided one or more digital documents or

#	Term	Definition
		identifiers (username, certificate) from an issuing authority.

Appendix B: Contacts

For questions regarding this standard, contact:

CO Manager:
Mr. Mark Crase
Chief Technology Officer, Cyberinfrastructure Services
CSU Office of the Chancellor
mcrase@calstate.edu

Subject Matter Experts:

Mr. Michael Trullinger
Associate Director, Identity and Access Management
CSU Office of the Chancellor
mtrullinger@calstate.edu

Javier Torner, Ph.D.
Information Security Officer & Interim Associate Vice President, IRT
CSU San Bernardino
jtorner@csusb.edu

Appendix C: Applicable Federal and State Laws and Regulations

State	Title
California Civil Code, Division 3, Part 2, Title 2.5 §1633.1 – 1633.17	**California Uniform Electronic Transactions Act (UETA)** http//www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1633.1-1633.17 This Act facilitates electronic transactions consistent with other applicable law and specifies consistent practices concerning electronic transactions.
California Code of Regulations, Title 2, Division 7, Chapter 10	**Digital Signatures** http//www.sos.ca.gov/digsig/digital-signature-regulations.htm This regulation describes acceptable technology for digital signatures.
U.S.C. section 7001	**Electronic Signatures in Global and National Commerce Act of 2000** http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
California Government Code, Section 16.5	**Digital Signatures** http://www.sos.ca.gov/digsig/code-section-16-5.htm

Appendix D: Other Resources and Related Documentation

ID / Control #	Title
Integrated CSU Administrative Manual Section General Accounting 3701.01	**Digital Signatures** http//www.calstate.edu/icsuam/sections/3000/3701.01.shtml This document specifies the requirements for the use of digital signatures in lieu of handwritten signatures.
CSU Executive Order No. 1031	**Executive Order No. 1031:** System-wide Records/Information Retention and Disposition Schedules Implementation http//www.calstate.edu/EO/EO-1031.html This document ensures compliance with legal and regulatory requirements and best practices of records/information retention and disposition.
CSU Information Security Policy	**The California State University Information Security Policy** http//www.calstate.edu/icsuam/sections/8000/8000.0.shtml
Pending	**The California State University Information Security Standards** http://www.calstate.edu/ This document specifies CSU information security standards.
InCommon	**InCommon Client Certificate Service Overview** https://www.incommon.org/cert/clientcerts.html

8105.00 | Responsible Use Policy

Effective Date: 11/20/2013 | **Revised Date**: 11/20/2013

POLICY OBJECTIVE

The CSU Information Security policy provides defines user, including faculty, staff, students, third parties, and CSU responsibilities with respect to the use of CSU information assets.

POLICY STATEMENT

Introduction

The California State University (CSU) provides access to information assets for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students and staff. These resources are vital for the fulfillment of the academic, research and business needs of the CSU community. This policy defines user (e.g., faculty, staff, students, third parties, etc) and CSU responsibilities with respect to the use of CSU information assets in conjunction with the CSU Information Security Policy.

The CSU regards the principle of academic freedom to be a key factor in ensuring the effective application of this policy and related standards. Academic freedom is at the heart of a university's fundamental mission of discovery and advancement of knowledge and its dissemination to students and the public. The CSU is committed to upholding and preserving the principles of academic freedom: the rights of faculty to teach, conduct research or other scholarship, and publish free of external constraints other than those normally denoted by the scholarly standards of a discipline.

This policy is intended to define, promote, and encourage responsible use of CSU information assets among members of the CSU community. This policy is not intended to prevent, prohibit, or inhibit the sanctioned use of CSU information assets as required to meet the CSU's core mission and campus academic and administrative purposes.

The requirements stated within this policy must not be taken to supersede or conflict with applicable laws, regulations, collective bargaining agreements or other CSU and campus policies.

1.0 Scope

1.1 It is the collective responsibility of all users to ensure the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the CSU and to use CSU assets in an effective, efficient, ethical, and legal manner.

1.2 The CSU RESPONSIBLE USE POLICY shall apply to the following:

a) All campuses.

b) Central and departmentally managed campus information assets.

c) All users employed by campuses or any other person with access to campus information assets.

d) All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).

e) Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

1.3 Auxiliaries, external businesses and organizations that use CSU information assets must comply with the CSU RESPONSIBLE USE POLICY.

1.4 This policy establishes basic responsibilities for all users, the CSU and campuses, and describes expectations for responsible use in the following sections:

Section 3.0	General Principles	This section sets forth basic policy principles. Situations or behaviors not specifically mentioned in sections 5.0 - 7.0 may be addressed through application of these basic principles.
Section 4.0	User - Responsibilities	This section highlights policy specifics related to access, responsible use, network and information system integrity, trademarks and patents, and incidental use.

Section 5.0	CSU and Campus Responsibilities	This section highlights specific requirements for CSU and campus officials.
Section 6.0	Policy Enforcement	This section describes a process for addressing violations of the CSU RESPONSIBLE USE POLICY.

1.5 The development of this policy was expedited by reference to policies from:

a) CSU campuses: Bakersfield, East Bay, Fresno, Humboldt, Long Beach, Monterey Bay, Northridge, San Diego, San Luis Obispo, San Marcos, and Sacramento

b) Other institutions: Concordia College, Montana State University, University of Albany, University of Michigan, and Virginia Tech

2.0 Policy Management

2.1 The CSU RESPONSIBLE USE POLICY shall be updated as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations. The CSU Chief Information Security Officer shall be responsible for overseeing a periodic review of this policy and communicating any changes or additions to appropriate CSU stakeholders.

2.2 The policy may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by each campus.

2.3 Each campus through consultation with campus officials and key stakeholders must develop policies, standards, and implementation procedures referenced in the CSU RESPONSIBLE USE POLICY.

3.0 General Principles

3.1 The purpose of these principles is to provide a frame of reference for user responsibilities and to promote the ethical, legal, and secure use of CSU resources for the protection of all members of the CSU community.

3.2 Use of CSU information assets shall be consistent with the education, research, and public service mission of the CSU, applicable laws, regulations, and CSU/campus policies. Note: The term "information assets", along with many other important terms and concepts, is defined in the CSU ICSUAM Policy Glossary: https://csyou.calstate.edu/ICSUAM/Pages/Policy-Glossary.aspx.

3.3 All users (e.g., faculty, staff, students, third parties) are required to comply with CSU and campus policies and standards related to information security.

3.4 All users (e.g., faculty, staff, students, business partners) are required to help maintain a safe computing environment by notifying appropriate CSU officials of known vulnerabilities, risks, and breaches involving CSU information assets.

3.5 It is the policy of the CSU to make information assets and services accessible in order to meet the needs of CSU students, faculty, staff, and the general public. Information regarding the Accessible Technology Initiative can be found at: https://csyou.calstate.edu/Projects-Initiatives/ATI/Pages/default.aspx.

3.6 All users, including those with expanded privileges (e.g., system administrators and service providers), shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics, and video.

3.7 The CSU respects freedom of expression in electronic communications on its computing and networking systems. Although this electronic speech has broad protections, all University community members are expected to use the information technology facilities considerately with the understanding that the electronic dissemination of information may be available to a broad and diverse audience including those outside the university.

3.8 Other than publicly designated official CSU sites, the CSU does not generally monitor or restrict content residing on CSU systems or transported across its networks; however, the CSU reserves the right to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. These activities are not intended to restrict, monitor, or use the content of legitimate academic and organizational communications.

3.9 In the normal course of system and information security maintenance, both preventive and troubleshooting, system administrators and service providers may be required to view files and monitor content on the CSU and campus networks, equipment, or computing resources. These individuals shall maintain the confidentiality and privacy of information unless otherwise required by law or CSU/campus policy.

3.10 The CSU recognizes and acknowledges employee incidental use of its computing and network resources within the guidelines defined in the "Incidental Use" section of this policy, at paragraph 4.5 below.

3.11 All investigations of CSU or campus policy violations, non-compliance with applicable laws and regulations or contractual agreements will be conducted in accordance with appropriate CSU and campus procedures.

4.0 User Responsibilities
This section describes user responsibilities governing access, responsible use, network and information system integrity, and incidental use. These statements are not designed to prevent, prohibit, or inhibit faculty and staff from fulfilling the mission of the CSU. Rather, these statements are designed to support an environment for teaching and learning by ensuring that CSU resources are used appropriately.

4.1 Responsible Use of Information Assets
4.1.1 Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of CSU equipment, its data and software, and its access.

4.1.2 Users must not use or access CSU information assets in a manner that:

a) Conflicts with the CSU mission;

b) Violates applicable laws, regulations, contractual agreements, CSU/campus policies or standards; or

c) Causes damage to or impairs CSU information assets or the productivity of CSU users through intentional, negligent or reckless action.

4.1.3 Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into CSU computing and networking systems.

4.1.4 Unless appropriately authorized, users must not knowingly disable automated update services configured on CSU computers.

4.1.5 Users must take reasonable precautions to ensure their personal and/or CSU-provided devices (e.g., computers, tablets, smart phones) are secure before connecting to CSU information assets.

4.1.6 Users must close or secure connections to CSU information assets (e.g. remote desktop, virtual private network connections) once they have completed CSU-related activities or when the asset is left unattended.

4.1.7 Users must promptly report the loss or theft of any device, which grants physical access to a CSU facility (e.g., keys, access cards or tokens), or electronic access (passwords or other credentials) to CSU resources.

4.1.8 Users who publish or maintain information on CSU information assets are responsible for ensuring that information they post complies with applicable laws, regulations, and CSU/campus policies concerning copyrighted material and fair use of intellectual property.

4.1.9 Software must be used in a way that is consistent with the relevant license agreement. Unauthorized copies of licensed or copyrighted software may not be created or distributed.

4.1.10 Per Section 8314.5 of the California Government Code, it is unlawful for any state employee, or consultant, to knowingly use a state-owned or state-leased computer to access, view, download, or otherwise obtain obscene matter. "Obscene matter" as used in this section has the meaning specified in Section 311 of the California Penal Code. "State owned or state-leased computer" means a computer owned or leased by a state agency, as defined by Section 11000, including the California State University. This prohibition does not apply to accessing, viewing, downloading, or otherwise obtaining obscene matter for use consistent with legitimate law enforcement purposes, to permit a state agency to conduct an administrative investigation, or for legitimate medical, scientific, or academic purposes.

4.1.11 A user who has knowledge (or reasonable suspicion) of a violation of this policy must follow applicable CSU and campus procedures for reporting the violation. A user must not prevent or obstruct another user from reporting a security incident or policy violation. Refer to CSU Information Security Policy 8075 Information Security Incident Management.

4.2 Protection from Data Loss
4.2.1 Individuals who access, transmit, store, or delete Level 1 or Level 2 data as defined in the CSU Data Classification Standard1 must use all reasonable efforts to prevent unauthorized access and disclosure of confidential, private, or sensitive information.

[1] The CSU Data Classification Standard is located here.

a) Users must not provide access or transmit Level 1 or Level 2 data to another user without prior approval from the data owner or custodian.

b) Users must not access or transmit unencrypted Level 1 data over a public network.

4.3 Prohibition Against Unauthorized Browsing and Monitoring

4.3.1 The CSU supports and protects the concepts of privacy and protects the confidentiality and integrity of personal information maintained in educational, administrative, or medical records. Information stored in CSU information systems may be subject to privacy laws.

4.3.2 Users must not browse, monitor, alter, or access email messages or stored files in another user's account unless specifically authorized by the user. However, such activity may be permitted under the following conditions:

a) The activity is permitted under CSU or campus policy.

b) The activity is defined in the user's job description.

c) The activity is conducted under the authority and supervision of an approved CSU official acting within his or her job responsibilities.

d) The activity is part of a classroom exercise conducted under the supervision of a faculty member. In this case, the faculty member must ensure the exercise does not result in a breach of confidentiality, availability, and integrity of CSU information assets.

e) The activity is conducted to comply with an applicable law, regulation, or under the guidance of law enforcement or legal counsel.

4.4 Responsibility of Account Owners

4.4.1 The owner or custodian of credentials, such as a username and password, that permit access to a CSU information system or network resource is responsible for all activity initiated by the user and performed under his/her credentials. The user shall assist in the investigation and resolution of a security incident regardless of whether or not the activity occurred without the user's knowledge and as a result of circumstances outside his or her control.

4.4.2 Users must take reasonable steps to appropriately protect their credentials from becoming known by, or used by others.

a) Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining, and changing passwords.

Unless specific prior authorization has been granted, users are prohibited from:

b) Using or attempting to use the account to access, modify, or destroy CSU or non-CSU information assets for which a user is not normally authorized.

c) Disclosing passwords to any party or including passwords in documentation.

d) Embedding passwords in software code.

4.4.3 With the exception of publicly accessible CSU information assets, users must not transfer or provide access to CSU information assets to outside individuals or groups without proper authorization.

4.4.4 Users of CSU information assets must not purposefully misrepresent their identity, either directly or by implication, with the intent of using false identities for inappropriate purposes.

4.4.5 In the few instances where special circumstances or system requirements mandate that multiple users access the same account, extreme care must be used to protect the security of the account and its access password. Management of this account must conform to written or published CSU procedures designed to mitigate risk associated with shared access accounts.

4.5 Incidental Use

4.5.1 University-owned/managed information assets are provided to facilitate a person's essential work as an employee, student, or other role within the University. Use of university owned computer systems for University-related professional development or academic activities such as research or publication is permitted within the limits of system capacities.

4.5.2 Personal use of CSU information assets must be no more than "de minimis" (e.g. must have so little value that accounting for it would be unreasonable or impractical). Individuals may use CSU information assets for occasional incidental and minimal personal use provided such use:

a) Does not violate applicable laws

b) Is not in pursuit of the individual's private financial gain or advantage.

c) Does not interfere with the operation or maintenance of University information assets.

d) Does not interfere with the use of University information assets by others.

e) Does not interfere with the performance of the assigned duties of a university employee.

f) Does not result in a loss to the University.

5.0 CSU Responsibilities

5.1 The CSU has broad responsibilities with respect to protecting its information assets. These include but are not limited to controlling access to information, responding to and addressing information security incidents, complying with laws and regulations, and ensuring the logical and physical security of the underlying technology used to store and transmit information. CSU policies related to these activities are found in the Integrated CSU Administrative Manual and can be accessed at ICSUAM Section 8000.

5.2 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 network services; monitoring actions on information systems; checking information systems attached to the network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

6.0 Policy Enforcement

6.1 The CSU respects the rights of its employees and students. In support of the CSU Information Security policies, campuses must establish procedures that ensure investigations involving employees and students suspected of violating the CSU Information Security policy are conducted. These procedures must comply with appropriate laws, regulations, collective bargaining agreements, and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

6.2 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. Suspension, block or restriction to information assets in such a manner as to substantially affect the ability to complete assigned coursework or job duties shall be considered disciplinary actions subject to §6.3.

6.3 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 and the California Education code. Student infractions of CSU Information Security policies must be handled in accordance with the established student conduct process. Auxiliary employees who violate the CSU policies may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply with CSU policies may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the CSU.

6.4 The CSU may also refer suspected violations to appropriate law enforcement agencies.

Benjamin F. Quillian
Executive Vice-Chancellor / Chief Financial Officer

Approved: November 20, 2013