Status Active PolicyStat ID 15698973

Origination	4/19/2010	Owner	Josh Callahan: Chief Info Security Officer
Effective	4/30/2024	Area	Business and Finance
Reviewed	4/30/2024		
Next Review	4/30/2025		

CSU Information Security Policy and Standards

I. Policy

The California State University (CSU) manages and protects the confidentiality, integrity, and availability of CSU information assets and establishes procedures that define the organizational scope of the CSU information security program. This policy is 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.

II. Scope

This 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 this 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.

III. Roles and Responsibilities

The roles and responsibilities for the protection of CSU Information Assets are set forth below.

A. The Board of Trustees of the California State University

The Board of Trustees of the California State University (CSU) is responsible for protecting the confidentiality, integrity, and availability of CSU Information Assets.

B. Systemwide Chief Information Officer (CIO)

The Systemwide Chief Information Officer (or the designee of the Chancellor) is responsible for the systemwide Information Security Program and may organize the responsibilities as appropriate.

C. Systemwide Chief Information Security Officer (CISO)

The Systemwide Chief Information Security Officer must:

- Provide leadership for the overall CSU Information Security Program.
- Provide leadership for the CSU Information Security Advisory Committee.
- Conduct a periodic review and update of the CSU security policy and standards.
- Advise the Chancellor and CSU senior management on matters regarding information security.
- Provide support to information security staff at each campus.
- Develop systemwide information security strategies and metrics.

D. Campus President

In addition to other duties as defined within the CSU, each 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.
- The President (or President's designee) must identify the specific duties and responsibilities for the Campus Information Security Officer (ISO), which, at a minimum, include those items in the CSU Information Security Policy and other items as identified below. While the role of the ISO may be an additional duty, the President must ensure the appointee has sufficient time to carry out the assigned duties and responsibilities.
- The President may assign additional information security roles and responsibilities appropriate to

the campus.

- Each President must review information security risks at least annually.
- Each campus President (or President-designee) and the Systemwide CIO (or the Systemwide CIO's designee) must appoint a campus information security officer (ISO).
- Each campus President and the Systemwide CIO 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.

E. Campus Chief Information Officer (CIO)

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

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

F. Campus Information Security Officer (ISO)

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

- Oversee campus information security risk assessment activities.
- Inform the campus President (or President-designee) of significant information security risks as they are identified.
- Oversee the campus information security incident response program in coordination with appropriate campus personnel.
- Oversee the campus information security awareness and training program.
- Provide 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.
- Respond to information security related requests during an audit.
- Avoid conflicts of interest by not having direct responsibility for information processing or technology operations for campus programs that employ Level 1 or Level 2 Data.
- Ensure adherence to information security policies and standards by all parties that use or access campus information assets including auxiliaries, external businesses and decentralized

Information Technology departments.

G. Campus Managers

In addition to other duties as defined within the CSU, technical and program (e.g., human resources, registrars, privacy officers, etc.,) managers must:

- Ensure that Information Assets under their control are managed in compliance with CSU and campus information security policies and standards.
- Ensure 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.

H. Campus Data Owners

In addition to other duties as defined within the CSU, the data authority/owner must:

- 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.
- Work with the campus 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.
- Authorize access to the Information Asset in accordance with the classification of the asset and the need for access to the information.
- 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.
- Work with the ISO to monitor and ensure compliance with CSU/campus security policies and procedures affecting the Information Asset.
- Work with the ISO to identify an acceptable level of risk for the Information Asset.
- 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.

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.

I. Campus Data Custodian/Steward

In addition to other duties as defined within the CSU, Information Asset custodians must:

- Comply with applicable law and administrative policy.
- Comply with any additional security policies and procedures established by the owner of the Information Asset and the campus ISO.

- Advise 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.
- Notify the owner of the Information Asset and the campus ISO of any actual or attempted violations of security policies, practices, and procedures.

J. CSU Information Security Advisory Committee (ISAC)

The Information Security Advisory Committee (ISAC) advises the Systemwide CISO, campus ISOs, and campus constituents on standards, policies and practices related to the selection, funding, deployment, management, and assessment of information security in support of system-wide and campus-based academic and administrative programs.

K. Campus Data Users

Campus data users must:

- Work 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.
- Perform as appropriate other information security duties as required by other CSU and campus policies/standards, the data owner, or the campus ISO.

L. Users

It is the collective responsibility of all users of CSU Information Assets to ensure:

- That he or she does not put any Information Asset for which he or she has been given access at risk through his or her own actions.
- 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 or campus policies governing information security and privacy protection.

Additional user responsibilities are specified in the CSU Information Security Responsible Use Policy.

IV. ISO Policies

A. ISO Domain 5: Information Security Policy

The CSU Systemwide CISO shall be responsible for overseeing a documented annual review of this policy and communicating any changes or additions to appropriate CSU stakeholders. This policy shall be updated as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations. This policy, and CSU Information Security Program activities, will be guided by ISO 27002:2013 (*Information technology — Security techniques — Code of Practice for Information Security Controls*).

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

Policies, standards, and implementation procedures referenced in this policy must be developed by each campus through consultation with campus officials and key stakeholders.

B. ISO Domain 6: Organization of Information Security Policy

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.

Campuses must develop risk management processes that identify, assess, and monitor risks to Information Assets containing Level 1 or 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.

related standards: ISO Domain 6: Organization of Information Security Standard
Standards Enforcement, Exceptions
Risk Assessment Process

C. ISO Domain 7: Human Resource Security Policy

This section provides direction and support for managing personnel information security and information security training and awareness programs.

1. Personnel Information Security Activities

Campuses must develop procedures to:

- Conduct background checks on positions involving access to Level 1 Data and Information Assets containing Level 1 Data as defined in the CSU Data Classification Standard.
- Revoke access to Information Assets 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.
- 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.

- 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 their personal electronic information resulting from incidental personal use of campus Information Assets as appropriate.

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

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 agreement.

2. Information Security Training and Awareness Activities

All employees with access to Information Assets containing Data must participate in an annual information security awareness training with assignments and completions tracked and recorded. An online Data Security and FERPA course is available for assignment on the systemwide Learning Management System.

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.

All employees with access to Information Assets containing Level 1 or Level 2 Data 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. 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.

related standards: ISO Domain 7: Human Resource Security Standard
Employment Separations and Position Change
Campus Security Awareness and Training Program

D. ISO Domain 8: Asset Management Policy

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 Level 1 and Level 2 Data is responsible for:

- Classifying the Information Asset according to the CSU 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 CSU Asset Management Standard.

Level 1 and Level 2 Data must not be transferred to another individual or system without approval of the data owner. Before Level 1 or Level 2 Data is transferred to another individual or system, the data owner should establish agreements to ensure that authorized users implement appropriate security measures.

related standards: ISO Domain 8: Asset Management Standard
Data Classification Levels
Cloud Storage and Services

E. ISO Domain 9: Access Control Policy

This section provides direction and support for managing access to CSU Information Assets.

1. 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. Access to Level 1 data must use authentication methods that meet or exceed NIST 800-63-3 AAL2 by requiring multi-factor authentication, including both a secure password and the use of an authenticator. An authenticator can be software based (push technology or software token) or hardware based (physical token.) Appropriate controls must be in place to prevent unauthorized access to these Information Assets. 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 Information Assets containing Level 1 or Level 2 Data 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 or campus policy.

Authentication controls must be implemented for access to campus Information Assets that access or store Level 1 or Level 2 Data. Authentication credentials 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.

2. Separation of Duties

Separation of duties principles must be followed when assigning job responsibilities relating to restricted or essential resources. Campuses must maintain an appropriate level of separation of duties when issuing credentials or granting permissions to individuals who have access to Information Assets containing Level 1 or Level 2 Data. Campuses must avoid granting a user greater access or more authority over Information Assets than is required by the employee's job duties.

3. Access Review

Campuses must develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate campus managers and data owners must review, at least annually, user access rights to Information Assets containing Level 1 or Level 2 Data. The results of the review must be documented.

4. Modifying Access

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

related standards: ISO Domain 9: Access Control Standard

F. ISO Domain 10: Cryptography Policy

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 the campus or the Chancellor's Office provided the local policies and procedures conform to the terms set forth in this policy.

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

1. 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.

Electronic Signatures may be used for bilateral contractual and legal documents, unilateral contracts and other University controlled documents, internal campus and Chancellor's Office forms and approvals, and external forms and approvals.

2. 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.

Digital Signatures may be used for any record or document when permitted and unless a handwritten signature is explicitly required. Digital signatures must be used in lieu of a simple electronic signature when legally required. 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:

- It is unique to the person using it,
- It is capable of verification,
- It is under the sole control of the person using it,

- It is linked to data in such a manner that if the data are changed, the digital signature is invalidated, and
- It conforms to Title 2, Division 7, Chapter 10, of the California Code of Regulations.

3. Procedures

Campuses must develop policies and procedures to identify, evaluate, and document who may use simple electronic and digital signatures and where simple electronic signatures are permitted and digital signatures are required.

Campus policies and procedures for electronic signatures must meet the electronic and digital signature standards as outlined in the Standards below, 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.

Campus and Chancellor's Office procedures must document the person by CSU position who is authorized to sign, approve, and/or prevent unauthorized actions from being taken as a result of an electronic signature.

related standards: ISO Domain 10: Cryptography Standard
Acceptable Use of Electronic and Digital Signatures

G. ISO Domain 11: Physical and Environmental Security Policy

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 Level 1 or Level 2 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 Level 1 or Level 2 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.

related standards: ISO Domain 11: Physical and Environmental Security Standard

H. ISO Domain 12: Operations Security Policy

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 Level 1 or Level 2 Data from threats.

1. Configuration Management

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.

2. 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 Level 1 or Level 2 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 campus Information Assets containing Level 1 or Level 2 Data 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.

a. *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.

3. 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.

4. Mobile Devices

Campuses must develop and implement controls for securing Level 1 or Level 2 Data stored on mobile devices. Level 1 or Level 2 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 Level 1 or Level 2 Data.

5. 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

Information Security 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 time frame. 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).

related standards: ISO Domain 12: Operations Security Standard
Protections Against Malicious Software Programs
Remote Access to CSU Resources
Mobile Device Management
Logging Elements
Common Workstation Minimum Configuration Requirements
High Risk/Critical Workstation Standard
Change Control

I. ISO Domain 13: Communications Security Policy

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 Level 1 or Level 2 Data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and Level 1 or Level 2 Data must ensure confidentiality, integrity, and availability.

related standards: ISO Domain 13: Communications Security Standard
Network Information Requirements
Boundary Protection and Isolation

J. ISO Domain 14: Systems Acquisition, Development and Maintenance Policy

Campuses must integrate information security requirements into the software life cycle of information systems that contain Level 1 or Level 2 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 Level 1 or Level 2 Data.

related standards: ISO Domain 14: Systems Acquisition Standard
Application Security Standards

K. ISO Domain 15: Supplier Relationships Policy

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.

Third party service providers may be granted access to campus Information Assets containing Level 1 or Level 2 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 Information Assets containing Level 1 or Level 2 Data 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.

related standards: ISO Domain 15: Supplier Relationships Standard

L. ISO Domain 16: Information Security Incident Management Policy

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 Level 1 or Level 2 Data, or improper dissemination of Level 1 or Level 2 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.

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 Systemwide CISO.
- If a breach of Level 2 Data has occurred, the campus ISO must notify the Systemwide CISO. The Systemwide CISO will provide the Chancellor with quarterly status reports on Level 2 Data breaches that have occurred in the CSU.

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

related standards: ISO Domain 16: Incident Management Standard

M. ISO Domain 17: Information Security Aspects of Business Continuity Management Policy

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.

related standards: ISO Domain 17: Business Continuity Management Standard

N. ISO Domain 18: Compliance Policy

The CSU Systemwide CISO 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 Systemwide CISO 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.

related standards: ISO Domain 18: Compliance Standard

V. ISO Standards

A. ISO Domain 6: Organization of Information Security Standard

To implement the ISO Domain 6: Organization of Information Security Policy, a campus Information Security 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 Data 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.

1. Risk Management Strategies

Campus risk assessments must be based on established severity and likelihood criteria set forth below and managed through ongoing evaluation and review activities. The campus must not alter the severity or likelihood classifications listed below, but the campus may add criteria and/or numeric weighting based on its unique environment or circumstance.

2. Formal Risk Assessment Process

a. Establish Criteria

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

A. Criteria for situations in which a formal risk assessment must be performed (i.e. HIPAA, PCI, Level 1 Data, etc.).

B. 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.

b. Identify Formal Risk Assessment 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.

c. 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 3 years.

B. **Risk Exposure**: Each formal risk assessment must use the established risk assessment criteria outlined below 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.

d. Risk Severity and Likelihood

Each campus must use the severity and likelihood criteria set forth below.

Severity Scale

Critical - Events that, if realized, 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 - Events that, if realized, 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 - Events that, if realized, 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 - Events that, if realized, 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

This table maps the likelihood and severity of a risk to the overall risk level.

		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**

3. 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.

B. ISO Domain 7: Human Resource Security Standard

To implement the ISO Domain 7: Human Resource Security Policy, this section provides direction and support for managing personnel information security and information security training and awareness programs.

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.

2. Information Security Training and Awareness Activities

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.

a. Campus Security Awareness and Training Program

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

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 Level 1 Data.

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 3years.

E. Annual information security training for privileged users (e.g., system and security administrators) who interact with Information Systems containing Level 1 or Level 2 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.

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

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.

C. ISO Domain 8: Asset Management Standard

To implement the ISO Domain 8: Asset Management Policy, 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.

1. Data Ownership

Campuses must complete an inventory identifying Level 1 Data. Campuses must assign ownership of each Information Asset containing Level 1 Data. Normally, responsibility for Level 1 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.

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 Classification levels.

3. Data Classification Levels

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.

a. Classification Description: Level 1 - Confidential

Access, storage, and transmissions of Level 1 - Confidential information are subject to restrictions as described in this document. Information may be classified as confidential based on criteria including but not limited to:

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

b. Classification Description: Level 2 – Internal Use

Access, storage, and transmissions of Level 2 - Internal Use information are subject to restrictions as described in this document. Information may be classified as "internal use" based on criteria including but not limited to:

- Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.
- 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 assets
- Location of Level 1 or Level 2 Data
- 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

c. Classification Description: Level 3 - General

Information which may be designated by your campus as publicly 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.

d. Use and Maintenance of Data Classification Levels

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 Classification 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.

C. The CSU's Systemwide Chief Information Security Officer (CISO) must determine what data will be designated Level 1 Data and must identify appropriate minimum controls.

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

4. 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 Level 1 Data is transmitted electronically, it must be sent via a method that uses strong encryption.

C. When Level 2 Data is transmitted electronically, it must be protected using approved campus processes.

5. Data Storage

A. Each campus must develop and implement appropriate controls for securing Level 1 or Level 2 Data. These controls must ensure the confidentiality, integrity, and availability of the asset.

B. Campus electronic media and hardware on which Level 1 or Level 2 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 Level 1 or Level 2 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, Level 1 Data stored electronically must be encrypted using strong encryption methods.

6. Data Retention and Disposition

All data on campus hardware and electronic and non-electronic media must be retained and disposed of in accordance with the Systemwide Records Information Retention and Disposition Schedules Implementation Policy (EO 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.

7. Data Backup

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

B. Transportation procedures for backup media containing Level 1 or Level 2 Data must be documented and reviewed annually.

C. Backup media containing Level 1 Data must be encrypted using strong encryption methods.

D. 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.

8. Cloud Storage and Services

Cloud computing services are application and infrastructure resources that users access via the Internet. These services enable customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide services, platforms, and infrastructure to support a wide range of business activities.

Employees must not store or transmit Level 1 or Level 2 University data using services hosted by third parties which do not have a contract in place with the campus or its Auxiliaries, such as personal cloud accounts.

There are a number of information security and data privacy concerns about use of cloud computing services by University Personnel, departments, auxiliaries, and centers. They include but are not limited to:

- University no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers
- University dependency on a third party for critical infrastructure and data handling processes
- Potential security and technological defects in the infrastructure provided by a cloud vendor
- University has limited service level agreements for a vendor's services and the third parties that a cloud vendor might contract with
- University is reliant on vendor's services for the security of some academic and administrative computing infrastructure

Note that all requirements from all other relevant CSU policies and standards remain in full effect when cloud services are used.

a. Acquisition

Campuses must establish a process and assign responsibility for ensuring that contracts and renewals for cloud services are reviewed in order to identify appropriate supplemental contract language.

A risk assessment may be necessary where 3rd party contract terms substantially deviate from CSU supplemental or general IT terms in such manner as to pose a risk to the confidentiality, integrity, or availability of CSU Level 1 or Level 2 Data.

To assist campuses in responsibly assessing the risk of contemplated cloud purchases, cloud vendors who will be storing or accessing Level 1, 2, or 3 Data, or using central authentication must provide the campus with a security plan and/or policy and at least one of the following before the acquisition of any cloud services:

A. The Higher Education Cloud Vendor Assessment Tool. This questionnaire is designed specifically to help higher education institutions evaluate the security of cloud vendors.

B. A current SSAE-16 SOC 2 Type II (or equivalent third party audited security standard). This is a questionnaire that demonstrates the SOC compliance status in the following areas: Security, Availability, Processing Integrity, Confidentiality and Privacy. Each provider must demonstrate adherence to these principles to produce a qualified opinion.

C. A current Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CSA CAIQ). This is a questionnaire of about 300 questions used to assist both cloud providers, by providing principles of cloud security standards, and clients looking for appropriate cloud providers to suit their business needs and meet their security standards. Campuses can tailor the CSA CAIQ or questionnaire, and the risk assigned to each portion of the CSA CAIQ or questionnaire, as appropriate for each purchase. See the following for examples:

D. The Survey Analytics's Standardized Information Gathering Questionnaire. This questionnaire is used by outsourcers to obtain required documentation on a service provider and establish a profile on operations and controls for each control area.

The vendor provided information must be referenced in the contract.

The requester must provide a complete description of how they will deploy the product, including the type of data that will be involved and the type of authentication that will be used. See the Sample Security Data Requirements Checklist for an example of how this description can be provided.

Acquisition of cloud services which store, or access, or provided access to Level 1 or Level 2 Data must comply with the Supplier Relationships (ISO Domain 15) Standard. Campus must publish a guideline indicating what types of data may be stored on each cloud storage solution and how each cloud storage solution may be used, and must inform all users of cloud storage of this guideline.

b. Access to Data Stored in the Cloud

Campus Information Assets stored in the cloud shall be protected with no less control than that used for on-premises systems, as per the entirety of the Asset Management (ISO Domain 8) section of the CSU Information Security Standards.

c. Level 1 Data Stored in the Cloud

Campuses shall not use cloud services to store level 1 data (i.e. storage hosting solutions such as box.com, Dropbox.com, Google docs, etc.) unless such access can be limited by technical or procedural controls in order to reduce inadvertent exposure. Examples of adequate controls include but are not limited to:

- Configuration options which limit user ability to share documents or folders outside the organization
- Training and awareness for users who store level one data
- Periodic reports showing user permissions/access, including:
    - Reports of all access
    - Reports of all access granted to off campus entities
- Periodic assessment of level one data stored off campus
- Procedures for the management of encryption keys must protect the keys from unauthorized disclosure.

d. Synchronization of Stored Content

Level 1 Data stored in a cloud provider may only be automatically synchronized with compliant assets, computers, and devices that are university owned and managed.

D. ISO Domain 9: Access Control Standard

To implement the ISO Domain 9: Access Control Policy, access to campus Information Assets containing Level 1 or Level 2 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. 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

a. Granting Access

Authentication controls must be implemented for campus Information Assets which store or access Level 1 or Level 2 Data, and for systems the campus considers critical to operations. Campus-defined controls must take into consideration:

1. The need to validate user identity prior to granting access to Level 1 or Level 2 Data.
2. The requirement for unique user accounts and corresponding access privileges.
3. The requirement to deny all access rights until rights are formally approved and assigned.
4. The ability to report repeated failed access attempts.
5. The ability for access rights to be promptly modified or revoked.
6. The need for authentication credentials to be regularly changed.

b. User Account Management

1. 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).
2. 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 Level 1 or Level 2 Data. The period of acceptable inactivity must be based upon the nature of the data and/or the criticality of the system.
3. "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.
4. 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.
5. 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).
6. Campuses must establish criteria for creating application or system-level access accounts. These accounts must be assigned appropriate stewards and reviewed at least annually.

2. Identity Verification

For a campus to make the linkage between a claimed identity and real-life existence of a person, it needs valid forms of identity evidence, and to verify that the individual to be identified matches that identity evidence. There are three main steps to the identity verification process:

A. acceptability of the identity evidence,
B. validation of the identity, and
C. verification of identity.

"Acceptability of the identity evidence" addresses with what form of identity evidence is allowed, how much information is required, and the required strength level of that evidence.

"Validation of the identity" is the process of confirming that the provided identity evidence is not fraudulent.

"Verification of identity" is the process of confirming that the individual identified by the evidence is the individual who is offering the evidence.

Determination of the "identity assurance level" necessary to protect the assets to be accessed will inform the strength of the acceptability, validation and verification processes. The CSU requires that identity verification processes for Open University students, applicants, and alumni must meet NIST Identity Assurance Level 1 requirements and identity verification processes for all other users must meet NIST Identity Assurance Level 2 requirements, as defined by NIST Special Publication 800-63-3.

a. Definitions

Authenticator Assurance Level (AAL)

Identity Assurance Level (IAL)

b. Scope (Identity Verification)

This section applies whenever a password, token, or identity authenticator is bound to a user's identity record, issued, or otherwise provided to that user, or when a user-provided authenticator is bound to their identity record. Examples include but are not limited to issuing and resetting passwords or multi-factor authentication tokens.

c. Identity Verification Criteria

Verification requirements

1. Verification processes must be designed to limit the exposure of the PII to the minimum necessary to establish the unique identity characteristics of the user.
2. A password, token, identity authenticator or other element of identity evidence for authenticating a user must not be issued or otherwise provided to that user without first verifying their identity.
3. The identity verification process must protect against fraud from people associated with the user requesting verification (e.g., family members, roommates, employers, etc.), as these people may know the answers to verification questions.
4. The identity verification process must require that only the minimum amount of info necessary to verify identity is revealed to the verifier. For example, use of a superior piece of evidence of identity such as in-person presentation of an official photo ID card is adequate, without requiring the user to also provide other identity elements such as phone number, address, etc.
5. When using "information known by the requestor" to validate identity, the campus must rely only on previously known data, and may not on use info provided by the user during the validation process.
6. Caller ID, along with email addresses which incorporate the users' first and/or last name may not

be used as evidence of identity.

Campuses must develop and maintain a method for establishing identity at NIST Identity Assurance Level 2 (IAL2), which:

i. requires verification of identity with a photo ID or other equivalent effective method,
ii. may include taking a photograph for the purposes of later establishing the identity of the user,
iii. may include collecting answers to identity validation questions for the purposes of later establishing the identity of the user, and
iv. may result in an identity card and/or electronic copy of the campus identity information.

d. Evidence of Identity

Validation of Identity Evidence

Evidence used to prove identity must be able to be used by the identity verifier in that it must be:

1. comprehensible by the verifier
2. in such condition for writing to be legible, or photos suitable for visual verification
3. current and unexpired

Acceptable Forms of Identity Evidence

Verification Options	
Option 1	One **Superior** piece of identity (defined below)
Option 2	Two **Strong** pieces of identity (defined below)
Option 3	One **Strong** and two **Fair** pieces of identity (defined below)

Evidence Type	**Definition**
Superior	In-person presentation of government issued photo ID such as driver's license or passport, or campus identification card issued after otherwise establishing Identity Assurance Level 2 (IAL2).
Strong	Each of the following constitute one strong piece of identity: 1. Verification of appearance from video chat with photo on file previously taken by the university for identification purposes, such as in 2.c.2 above. 2. Verification of appearance from video chat with government or University issued photo ID displayed in video chat. Multiple forms of valid identification may be used as separate pieces of evidence.
Fair	1. Confirmation via recovery email.

	2. Answers to identity validation questions previously collected by the university for identification purposes, such as in 2.c.3 above. Examples include but are not limited to: - Mother’s maiden name - Name of first pet - High school nickname - Favorite Elementary School teacher - Make/model of first vehicle 3. Answers to academic record or employment questions verifiable by the identity verifier.

e. Disabling Automated Recovery Methods

To secure accounts that are threatened by individuals with detailed personal knowledge about the account owner, campuses must implement a method to allow users to disable automated online credential recovery methods for their individual accounts.

f. Identity Verification Activity Records

All identity verification activities must be recorded. These records must be maintained for a minimum of three years.

Identity verification activity records must contain:

1. Date/time
2. Identity being verified
3. Type(s) of identity evidence verified
4. Resulting action, e.g., “password reset” or “record updated” or “denied – unable to verify”
5. Organization or office performing the validation, e.g., “HelpDesk” or “System Administrator”
6. Identity of verifier
7. Purpose of verification, e.g., “Password change” or “MFA reset”

3. Authentication

a. Assurance Criteria

Access to capabilities or to services that increase the risk to campus infrastructure, such as but not limited to VPN access, remote computer access (RDP), virtual desktop infrastructure (VDI), remote admin access, or directing the movement of funds, must use authentication methods that meet NIST 800-63-3 AAL2 by requiring multi-factor authentication, including both a secure password and use of an authenticator. An authenticator can be software-based (push technology or software token) or hardware-based (physical token). Due to the fundamental insecurity of the Signaling System 7 protocol used in the cellular networks, SMS and voice calls as a second factor are explicitly prohibited.

Access to Level 1 data must use authentication methods that meet NIST 800-63-3 AAL2 by requiring multi-factor authentication, including both a secure password and use of an authenticator. An authenticator can be software-based (push technology or software token) or hardware-based (physical token).

Access to Level 2 data requires authentication methods that either meet NIST 800-63-3 AAL2 or both:

1. meet NIST 800-63-3 AAL1 and
2. limit access to people who are physically present or connections that originate from on-campus IP addresses.

b. Password Criteria Example

The below table provides an example of acceptable authentication requirements. Compared with previous NIST standards, 800-63-3 relies less on complex passwords and more on multi-factor authentication. Campuses may choose to implement different requirements, based on risk.

This table applies to credentials that can only be used to authenticate to systems that require multi-factor authentication:

Model NIST 800-63-3 Example Complexity Rule Set	
Example Complexity	Minimum password length of 10 characters On creation, password must not contain: • Password obtained from previous breaches • Dictionary words • Repetitive or sequential characters • Context-specific terms (username, campus, etc)
Example Failed Attempts	After 10 failed attempts since the last successful attempt: • Account is locked for 5 minutes; or • User is required to complete a CAPTCHA before attempting authentication again.
Example Aging	None
Example Multi-factor authentication	Requires use of approved authenticator to achieve AAL2

This table applies to credentials that can be used to authenticate to any systems without requiring multi-factor authentication:

Model NIST 800-63-3 Example Complexity Rule Set	
Example Complexity	Minimum password length of 10 characters On creation, passwords must contain: • A combination of letters, numbers and special characters, containing at least three of the following character types:

	◦ Lowercase alphabetic character (a-z) ◦ Uppercase alphabetic character (A-Z) ◦ Special character (punctuation, spaces, *, %, $, etc.) ◦ Number (0-9) On creation, password must not contain: • Password obtained from previous breaches • Passwords recently set for the account • Dictionary words • Repetitive or sequential characters • Context-specific terms (username, campus, etc)
Example Failed Attempts	After 10 failed attempts since the last successful attempt: • Account is locked for 5 minutes; or • User is required to complete a CAPTCHA before attempting authentication again.
Example Aging	One year expiration

c. Authentication Methodology Implementation

1. Critical information systems and those with Level 1 and/or Level 2 data must use a campus central authentication method approved by the campus Information Security Officer.
    a. Where authentication by campus central authentication is not possible, (i.e. cloud-based application which does not integrate with campus authentication methods), the campus must ensure that the accounts used are adequately provisioned, deprovisioned, and access follows the philosophy of least privilege. Refer to ISO Domain 9: Access Control Standard - Authentication to Cloud Services for cloud authentication specifics.
    b. The assurance and password criteria from § 3.a and 3.b still apply.
2. When passwords are issued they must be One-Time Passwords/Keys. One-Time passwords (e.g., passwords assigned during account creation, password resets), must be set to a unique value per user and changed immediately after first use.
3. The campus multi-factor authentication methodology implemented must:
    a. Logins to a system from a credential requires a re-authentication with MFA every 12 hours; other applications that leverage the active session of that credential on that system that would otherwise require MFA do not require a re-authentication
    b. Authentication to systems that grant access to protected data may require re-authentication more frequently, based on risk OR as determined by the campus Information Security Officer.
    c. NIST 800-63b 4.2.3 (Session connection control) – Require re-authentication after a 30 min period of inactivity

d. Password Storage and Transmission

1. Passwords or credentials 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.
2. Strong encryption must be used to protect passwords stored in a collection of passwords (database)(See NIST 800-63-3-B § 5.1.1.2).
3. Campuses must identify and inventory service accounts where password storage in clear text is necessary. The risk associated with these accounts must be mitigated by compensating controls as per risk assessment.
4. Campuses must identify and inventory applications where password transmission in clear text is necessary. The risk associated with these accounts must be mitigated by compensating controls as per risk assessment.

e. Detecting and Mitigating Account Compromise

1. Campuses must protect against employee account compromise with a combination of controls which may include methods such as:
    a. Restrictions on access based on geographical locale, host posture check or other technical solution
    b. Monitoring for access from multiple locations within a specified amount of time
    c. Awareness training designed to prevent phishing and/or other methods of credential compromise
    d. Behavioral analytics designed to detect and mitigate account compromise

4. Access Modification

At least annually, appropriate campus managers, data stewards, and/or their designated delegates must review, verify, and revise as necessary user access rights to campus Information Assets which store or access Level 1 or Level 2 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

5. Authentication to Cloud Services

Authentication to campus Information Assets hosted in the cloud shall be subject to no less control than those hosted on campus and must comply with the CSU Information Security Policy and Standards, particularly this section addressing Access Control (ISO Domain 9).

a. Central Authentication

Web-based Software as a Service (SaaS) cloud services must use a campus central authentication method in order to ensure that campuses may appropriately provision and deprovision identities and authorization for campus personnel. Examples of this include but are not limited to Shibboleth, SAML, ADFS, and CAS.

Campus authentication services must be configured in such a manner that the cloud provider does not have access to passwords in either text or encrypted format. Examples of protocols that expose user passwords to the service providers include but are not limited to LDAP and Radius.

b. When Central Authentication is Unavailable

The campus must establish a procedure for approving web-based SaaS cloud services that do not use central authentication.

This procedure must include a documented risk assessment and periodic review of the service.

Where campus authentication is not used, the campus must have a way to recover any account when the community member separates, such as using a campus email address as the contact for password resets, maintaining an appropriately protected list of passwords, or having the campus administer the accounts.

Additionally, the cloud host may not store passwords in clear text.

c. Multi-Factor Authentication

To mitigate the risk of a data breach occurring as a result of compromised credentials (such as through a successful phishing attack), multi-factor authentication is required for access from off campus to Level 1 Data belonging to someone else.

E. ISO Domain 10: Cryptography Standard

To implement the ISO Domain 10: Cryptography Policy, use of electronic or digital signatures within the CSU must follow the standards listed below.

This section is 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

1. Acceptable Use of Electronic and Digital Signatures

A. 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.

B. 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.

C. 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.

2. Risk Based Approach for Determining Appropriate Digital or Electronic Signature

A. 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. If the decision to use digital signature certificates is made, the appropriate validation type must also be selected.

B. 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.

a. Evaluation Process for Use of Electronic Signature

A. 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.

B. 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.

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

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

b. Acceptable Forms of Digital Signatures

A. 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.

B. 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".

C. 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.

3. Digital Certificates

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

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

B. 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".

4. Storage and Protection

A. Campuses must develop procedures for retrieval of escrowed materials, such as private keys. Campus Key recovery procedures should include the following:

1. Formal process for logging key recovery and approval
2. 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.

B. 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.

C. Digital signatures, digital certificates, and escrowed materials must be retained for a period at least as long as the longest retention period for any documents that are signed or encrypted using those certificates and escrowed materials.

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

5. Entities Affected

A. These standards and related guidance 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.

B. 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 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.

C. Each campus 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.

F. ISO Domain 11: Physical and Environmental Security Standard

To implement the ISO Domain 11: Physical and Environmental Security Policy, campuses must implement physical and environmental security controls to prevent unauthorized physical access, damage, and interruption to campus' Information Assets.

Campus controls must be adequate to protect critical systems, Level 1, and Level 2 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.

1. 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 Level 1 Data, Level 2 Data, or critical systems are located in the area.	None. Access to this area can be unrestricted.

	(Example: Student Union, Library open areas)	
Shared Access	An area containing Level 1 Data, Level 2 Data, or critical systems. Persons in the area include those who do not have authorization to access the data or systems. (Example: Administrative Offices)	Appropriate physical access controls and construction must be implemented that limit access to the data 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.
Campus Limited Access Area	An area containing Level 1 Data, Level 2 Data, or critical systems. Persons in the area are authorized to access the data or systems. (Example: Data Center)	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. 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: -Date and time of access -User ID performing access

2. Work Area Security

Campuses must establish and communicate user guidelines for securing Level 1 or Level 2 Data in work areas. This includes data in electronic and non-electronic form. The guidelines must address:

A. Ensuring that Level 1 or Level 2 Data is not left unattended.

B. Limiting the viewing of Level 1 or Level 2 Data from unauthorized users.

3. Viewing Controls

Information systems accessing Level 1 or Level 2 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 Level 1 or Level 2 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.

G. ISO Domain 12: Operations Security Standard

To implement the ISO Domain 12: Operations Security Policy, this section provides standards and guidance for appropriate technical controls to minimize risks to CSU information technology infrastructure.

1. Configuration Management

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.

a. Common Workstation Minimum Configuration Requirements

A. **Password Management -** State owned desktop and laptop computers must comply with the campus password complexity and aging policies as outlined in this document, Access Control (ISO Domain 9) Standard.

B. **Inventory -** Campus methods for managing computer inventory must have capability of maintaining inventory records for any campus computing devices, such as workstations, laptops, etc.

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

    2. 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.

    3. All devices, including workstations, peripherals, external drives, and memory sticks, which store Level 1 Data must:

        a. Be encrypted using campus approved encryption methods.

        b. Be tracked and managed via the campus inventory process as outlined in this document.

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

D. **Software Updates -** Workstation computers must be configured to allow automatic application of software updates through a patch management system.

E. **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.

F. **Enterprise Management -** The workstation must be managed by an appropriate configuration management system, such as a campus enterprise desktop management system, that ensures:

1. The workstation is subject to periodic vulnerability reporting.
2. The success and/or failure of critical patches is reported.

G. **Inactivity Screen Lock -** Workstations must be configured with screen locking features to prevent unauthorized access to a machine while not in use.

1. Campuses must identify screen lock time limits appropriate to the purpose of the workstation and the environment in which it is located.

b. High Risk/Critical Workstation Standard

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 large quantities of Level 1 Data are protected from unauthorized access.

A. **Definitions -** The following definitions apply to this section:

1. High Risk Workstation: any workstation that is used for elevated access to critical systems or stores or accesses 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.
2. Critical systems: systems which are necessary to conduct University business.

B. **High Risk Workstation Governance**

1. **Incorporating Common Workstation Standards -** All High Risk Workstations must meet Common Workstation Minimum Configuration Requirements.
2. **High Risk Workstation Designation -** Campuses must implement a process for designating and reviewing the designation of critical or High Risk Workstations.
3. **Change Control -** The configuration of a High Risk Workstation may not be altered except as approved via the campus Change Control Process.
4. **Physical Security -** High Risk workstations must be physically protected as per the Physical Security Standard.

C. **High Risk Workstation Configuration**

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.

2. **Protection Against "Zero Day" Malware -** For High Risk Workstations with operating systems commonly vulnerable to malware, either restricted outbound network egress (see A.1 above) or application whitelisting must be used in order to protect against "zero-day" malware.

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.

4. **Security Event Logging -** The High Risk Workstation must be configured to log security events.

    a. 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 at a minimum of 30 days

    b. Log activity must comply with the Information Asset Monitoring (Logging Elements) Standard.

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.

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

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

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. See here for example.

9. **Vulnerability Scanning -** Periodic vulnerability scans must be completed and assessed in order to verify that operating systems and application are adequately updated.

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.

2. Change Control

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 Level 1 Data, Level 2 Data, and critical systems. Significant changes made to a common or shared CSU Information Asset (e.g., CMS) must be appropriately reviewed and approved by a centralized CSU change control oversight group. Significant changes made to a campus-specific Information Asset must be appropriately reviewed and approved by the designated change control authority.

a. Change Management Methodology

The change control review process must include:

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

B. Identification and documentation of changes.

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

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

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

I. Ability to terminate and recover from unsuccessful changes.

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

b. 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 Chances**
Change Type Criteria	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	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

		requirement. Such changes can include either the hardware or software components of Information Systems and network resources.	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 backout 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.

3. Protections Against Malicious Software Programs

A. All campus Information Systems must be secured with current versions of campus approved anti-malware software unless otherwise authorized by the campus.

B. Campus approved anti-malware software must:

1. Be capable of detecting, removing, and protecting against malicious software, including viruses, spyware, and adware
2. 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

3. Be capable of tracking and reporting significant actions taken by the software (e.g., deleted or quarantined malware)
4. Check for and install updates and signatures at least daily

C. Unless appropriately authorized, users must not bypass or turn-off anti-malware software installed on campus Information Systems.

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

4. Mobile Devices

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

a. 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:

- Access control
- Encryption
- Strong passwords
- Anti-virus software
- Personal firewall

b. Storage of Level 1 Data

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

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

c. User Practices for Mobile Devices

A. 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.

B. Campuses must maintain and publish 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.

5. Remote Access to CSU Resources

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.

a. 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.

b. 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.

A. All remote access (wired or wireless) to non-public campus Information Assets must:

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

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

c. Non-Public CSU-Shared Resources

A. 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.

B. Campuses must identify and communicate approved user practices for remote connections.

6. Information Asset Monitoring (Logging Elements)

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.

a. Logging Elements

A. At a minimum and as appropriate, considering the capabilities of the device or application creating the log entries, such controls must track and log the following events:

   1. Actions taken by any individual with root or administrative privileges
   2. Changes to system configuration

   3. Access to audit trails
   4. Invalid access attempts (failed login)
   5. Use of identification and authentication mechanisms (logins)
   6. Notifications and alerts
   7. Activation and de-activation of controls, such as anti-virus software or intrusion detection system
   8. Changes to, or attempts to change, system security settings or control.

B. For each of the above events, the following must be recorded, as appropriate:
   1. User identification
   2. Type of event
   3. Date and time
   4. Success or failure indication
   5. Data accessed
   6. Program or utility used
   7. Origination of event (e.g., network address)
   8. Protocol
   9. Identity or name of affected data, information system or network resource.

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

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

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

H. ISO Domain 13: Communications Security Standard

To implement the ISO Domain 13: Communications Security Policy, campuses must establish a method for documenting the campus network topology, equipment configuration and network address assignments. Campuses must also implement controls designed to provide or limit access to networked CSU assets.

1. 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:

A. Network topology information containing:
   1. The locations and IP addresses of all segments, subnets, and VLANs.

2. Identification of any established security zones on the network and devices that control access between them.
3. The locations of every network drop and the associated switch and port on the switch supplying that connection.
4. A summary representation (e.g., drawing) of the logical design appropriate for managerial discussions.
5. A summary security model appropriate for managerial discussion.

B. IP address management

1. Static IP address assignments information sufficient to identify host, contact and device location (for wired ports)
2. Dynamic address server (i.e., DHCP) settings showing:
    a. Range of IP addresses assigned
    b. Subnet mask, default gateway, DNS server settings, WINS server settings assigned

C. Configuration information network devices such as:

1. Switches
2. Routers
3. Firewalls
4. Any other device critical to the functioning of the network

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

1. Net masks
2. Default gateway
3. DNS server IP addresses for primary and secondary DNS servers
4. Any relevant WINS server information
5. Responsible administrator contact information

2. Network Documentation Management

A. 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.

B. 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 3 years, and designated critical system information at least annually.

3. Boundary Protection and Isolation

A. 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.

B. The campuses must appropriately separate network access to public information system resources from those that do not provide services to external networks. (For example, a private file server that is only accessible from on campus must be in a private campus server farm subnet instead of in a DMZ.)

C. Campuses must establish zoning or separation within internal networks based on established trust relationships, authorized services, and data classification in order to ensure that Level 1 and Level 2 Data are not made available to unauthorized persons.

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

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

F. Each campus must maintain documentation as follows:

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

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

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

   4. 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.

I. ISO Domain 14: Systems Acquisition Standard

To implement the ISO Domain 14: Systems Acquisition Policy, this section applies to all CSU applications and web environments which:

A. Are considered mission critical systems,

B. Access Level 1 Data,

C. Access Level 2 Data and are accessible from the Internet, or

D. Provide an official public campus service or presence.

1. Application Security Standards

Application and web development environments must comply with CSU and campus standards and procedures. Contracts for services involving application and web development or hosting must incorporate appropriate language as set forth in Supplier Relationships (ISO Domain 15) Standard.

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 Level 1 Data.

a. Application and Web Development Environment Assessment

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

A. The planned application and supporting environment have been documented. Documentation must:

   1. Adequately describe the purpose and behavior of the application; and

   2. Identify the type and configuration of the supporting systems and networks.

B. Risk analysis verifies that:

   1. The application and supporting environment will comply with all applicable policies, standards, and procedures; and

   2. Deploying the application will not introduce any unacceptable risks.

b. Application Development and Production Architecture

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

B. Production environments for applications with high risk should run on stand-alone dedicated servers or VM server containers.

C. Production servers and development servers which store, process or transmit Level 1 or Level 2 Data must be housed in a data center that meets physical and logical security control requirements as per the CSU Information Security Policy, Physical and Environmental Security section.

D. Servers must be placed in the appropriate network zone based on the campus approved network architecture plan as per the Communications Security (ISO Domain 13) Standard.

E. Servers should be "hardened" according to the campus configuration procedures in order to ensure that they are secure.

c. 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
- Injection flaws
- Inadequate access control
- Improper error handling

- Inadequate authentication and session management
- Insecure storage
- Cross-site scripting (XSS) attacks
- Denial of service
- Buffer overflows
- 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.

d. Data Security

Level 1 or Level 2 Data may not be displayed in any documentation.

Within the development environment:

A. Application developers must remove all test data and test accounts before deploying an application into a production environment.

B. Level 1 or Level 2 Data should be redacted where possible in the development environment.

Within the production environment:

A. Sample or example scripts must be removed from production servers.

B. Developers must check system, test and development tools and processes to be sure that Level 1 or Level 2 Data is not copied or created accidentally. Refer to the Asset Management (ISO Domain 8) Standard.

e. Logging

A. Applications should log information as per the Operational Security (ISO Domain 12) Standard.

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

C. 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.

f. Applications Collecting Personally-Identifiable Data

The CSU Information Security Privacy of Personal Information Policy, 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.

g. Encrypt Level 1 Data

Applications must encrypt Level 1 Data as it is transmitted over the network, including login credentials and session identifiers as per the Asset Management (ISO Domain 8) Standard.

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.

2. 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.

A. Tests should be done from an attacker's point of view, and must be conducted prior to production deployment.

B. 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.

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

D. Previously deployed systems must be tested as part of any significant upgrade or as determined by a risk assessment. See the Operational Security (ISO Domain 12) Standard for more information about change control requirements.

a. 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 must be documented and tracked to resolution.

b. 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.

c. Web and Application Change Management

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

d. 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.

3. Application Authentication

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

a. 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.

A. Developer access privilege should be limited to the least privilege necessary for development.

B. 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.

C. Users of applications should be prevented from accessing data to which they have not been granted authorization.

Refer to the Access Control section of the CSU Information Security Policy, and the Access Control (ISO Domain 9) Standard.

b. 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 documented and approved through formal access control processes. Refer to the Access Control section of the CSU Information Security Policy, and the Access Control (ISO Domain 9) Standard.

J. ISO Domain 15: Supplier Relationships Standard

To implement the ISO Domain 15: Supplier Relationships Policy, when Critical, Level 1, or Level 2 Data is shared with third parties, campuses must ensure that it is either specifically permitted or required by law. Campuses must also ensure 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. 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 Level 1 or Level 2 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 Data.

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.

K. ISO Domain 16: Incident Management Standard

To implement the ISO Domain 16: Incident Management Policy,

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 notification about, and successful recovery from a variety of information security 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. Campus Incident Management

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

A. ***Incident Categorization***

1. Malicious Code
2. Denial of Service
3. Unauthorized Access
4. Improper Usage
5. Breach of Confidential Data

B. ***Incident Impact***

1. Classification of any data affected
2. Criticality of systems affected
3. Number of people affected

a. *Identification of a Computer Security Incident Response Team (CSIRT)*

Each campus must identify the positions responsible for responding to an incident.

b. *Protocol for escalation and internal notification*

Campus procedures must outline the method, manner, and progression of internal notification to ensure that:

A. Appropriate campus officials are notified about relevant security incidents including Campus Counsel.

B. The CSIRT is assembled.

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

D. Any actual or suspected incident involving personal information (notice-triggering and non-notice triggering data elements) in any type of media (e.g., electronic, paper) is reported immediately to the Systemwide Chief Information Security Officer (SCISO).

c. *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.

d. *Post incident analysis*

Campuses must review each incident to identify and apply lessons learned, including remediation strategies.

2. *Covered Incidents*

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

a. *Data Loss or Compromise (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 by legal or contractual obligations.

C. Deliberate or accidental distribution or release of personal information by a campus, its employees, auxiliaries, affiliates or contractors in a manner not in accordance with law or CSU/campus policy.

b. *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 malware attacks, web site defacements, server compromises, and denial of service attacks.

c. *Equipment Loss or Damage*

Theft, damage, destruction, or loss of campus IT equipment, including laptops, tablets, mobile devices, or any electronic devices containing or storing confidential, sensitive, or personal data.

d. *Computer Crime*

Use of a campus information asset in commission of a crime including but not limited to activities as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

e. *Other incidents*

Any other violations of campus information security policy or conditions that present substantial information security risk.

3. Evidence Collection and Handling

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.

The campus must establish 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. Mitigation

Mitigation steps must be chosen with due care to preserve security, follow CSU standards and policies, and preserve evidence.

Any emergency changes made during the incident must be either rolled back or approved via the normal change control process as per the CSU Information Security Change Control Policy and Standard.

5. Incident Reporting

Each campus must identify a point of contact (POC) and process 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)]. Campus process must include feedback processes to ensure reports of incidents are acknowledged.

In accordance with the Information Security Responsible Use Policy, campuses must provide users with a formal, centralized method (i.e., email or phone number) for notifying campus points of contact about information security incidents or events. This information must be part of routine security awareness activities. Any user or third party who observes or suspects that a campus information security incident is occurring must promptly notify the campus' point of contact about the incident.

6. Notification

The campus must determine (as stated below) the nature and scope of what, if any, external notifications are required.

When a campus has a reasonable suspicion that Level 1 data has been exposed or the campus begins to consider notifying any individual or external entity regarding exposure of data (of any data, including Level 2), the campus must immediately inform the Systemwide CISO. The notification process must include the following steps:

A. Initial notification informing the Systemwide CISO that the campus is investigating a potential incident.
B. Notification must include the nature of the potential incident and an estimate of the severity – i.e. number of records and types of information at risk of exposure.

If Level 2 data was breached (no Level 1):

A. Campus ISO activates Campus CSIRT

B. The campus decides whether to notify affected parties. If the campus chooses to do so:

   1. The campus ISO must immediately notify the SCISO in accordance with section 6.2 above

   2. Notifications must be sent out in accordance with section 6.5 below

If Level 1 data was breached:

A. Campus ISO activates Campus CSIRT

B. Campus must follow Campus Incident Response procedures to notify Campus President, SCISO, and Campus Counsel in accordance with section 6.2 above

C. Campus President contacts Chancellor

D. The Systemwide CISO will then notify the CSU Chief Financial Officer (CFO), CSU Chief Information Officer (CIO), CSU Office of General Counsel (OGC), CSU Risk Management, Public Affairs (PA), and HIPAA Privacy Officer (as needed)

E. Notifications must be sent out in accordance with section 6.5 below

F. If there is a HIPAA Impact:

   1. SCISO notifies OGC HIPAA Resource Attorney

   2. Notify Public Affairs

   3. Notify Health and Human Services (HHS) / Office of Civil Rights (OCR) in accordance with section 6.6 below

   4. If more than 500 records have been breached, then the campus notifies the State Attorney General and the Media in accordance with section 6.6 below

G. If there is not a HIPAA Impact:

   1. If more than 500 records have been breached, then the campus notifies the State Attorney General in accordance with section 6.6 below

a. Notification of impacted parties

In the case that external notifications are to be made to impacted parties, the notification process must include the following steps:

A. A DRAFT copy of the notification must be sent to the Systemwide CISO for review.

B. The Systemwide CISO will then:

   1. Review DRAFT and provide input.

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

   3. Send updated DRAFT to campus ISO/POC.

C. Campus notifies affected parties.

   1. However, if notification cost is more than $250,000 or more than 500,000 parties are affected, then the campus may employ substitute notice as allowed by law (per California Article 7 Section 1798.29 (i)(3)).

b. Notification of regulatory agencies

In certain situations (such as when the exposed data contains Level 1 Data and the impacted group is 500 HIPAA records or greater), it will be necessary to contact regulatory agencies. These include but are not limited to:

- Attorney General (https://oag.ca.gov/ecrime/databreach/report-a-breach)
- Health and Human Services (https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html?language=es)
- Department of Education (https://ed.gov)
- Office of Civil Rights

In these situations, the following steps must occur:

A. The ISO will send a DRAFT copy of the notice intended for the appropriate organization to the Systemwide CISO.

B. Public Affairs contacts Media as appropriate or required.

C. The Systemwide CISO will then:

    1. Review DRAFT and provide input.
    2. Send the DRAFT to CSU OGC for review and input.
    3. Send the updated DRAFT to campus ISO/POC for external organization.
    4. Campus notifies appropriate agency.

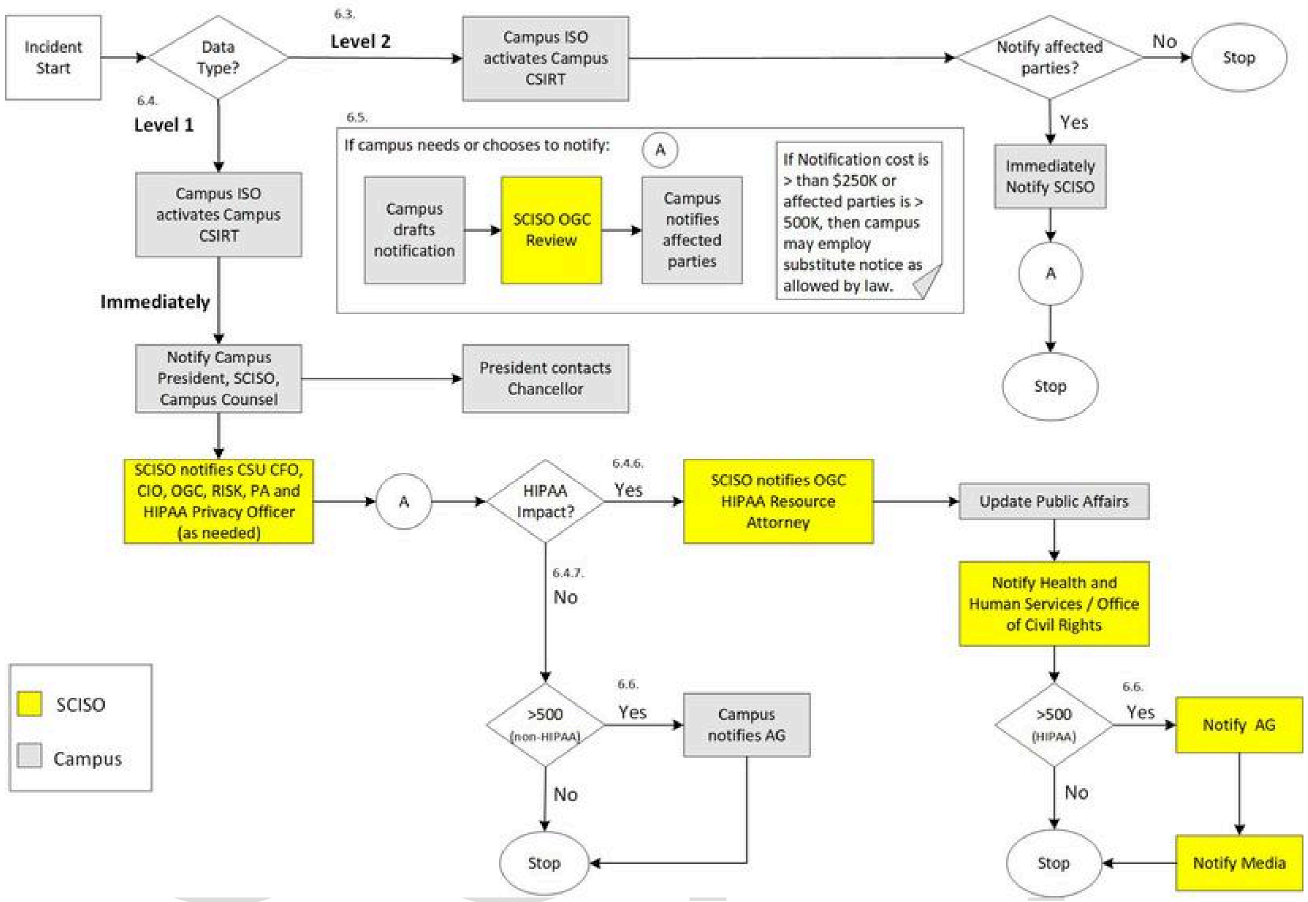
7. Remediation

After an incident, the campus must develop and implement corrective actions, where appropriate, directed at preventing or mitigating the risk of similar occurrences and applying lessons learned from incidents.

This Incident Communication Plan is intended to be a guide, not definitive.

Incident Notification Communication Plan

(Overview only)



Incident Start
Data Type?
6.3.
Level 2
Campus ISO activates Campus CSIRT
Notify affected parties?
No
Stop
Yes
Immediately Notify SCISO
A
Stop
6.4.
Level 1
Campus ISO activates Campus CSIRT
6.5.
If campus needs or chooses to notify:
A
Campus drafts notification
SCISO OGC Review
Campus notifies affected parties
If Notification cost is > than $250K or affected parties is > 500K, then campus may employ substitute notice as allowed by law.
Immediately
Notify Campus President, SCISO, Campus Counsel
President contacts Chancellor
SCISO notifies CSU CFO, CIO, OGC, RISK, PA and HIPAA Privacy Officer (as needed)
A
HIPAA Impact?
6.4.6.
Yes
SCISO notifies OGC HIPAA Resource Attorney
Update Public Affairs
Notify Health and Human Services / Office of Civil Rights
6.4.7.
No
>500 (non-HIPAA)
6.6.
Yes
Campus notifies AG
No
Stop
>500 (HIPAA)
6.6.
Yes
Notify AG
No
Stop
Notify Media
SCISO
Campus

L. ISO Domain 17: Business Continuity Management Standard

To implement the ISO Domain 17: Business Continuity Management Policy, during any disasters or other service interruptions, and during recovery and continuity activities, all CSU Information Security Policies and Standards are still fully in force and must be followed.

M. ISO Domain 18: Compliance Standard

To implement the ISO Domain 18: Compliance Policy, 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.

N. Standards Enforcement

Refer to the Enforcement section of the CSU Information Security Policy and Standards.

1. Exceptions

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 persons as 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 its risk management process to ensure that the exception is approved by an appropriate Vice-President or other campus administrator with fiscal responsibility for addressing the result of risk acceptance.

When a campus grants an exception or accepts a risk, it must monitor and periodically review the exception.

a. Exception Process

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 3 years.

D. A record documenting the exception process including:

   1. Contact information for individual and/or organization requesting the exception.
   2. The policy, standard or other requirement to which exception is being requested.
   3. Justification for the proposed exception.
   4. Description of any proposed compensating control or mitigating circumstance.
   5. Information security risk analysis using the campus risk assessment methodology.
   6. Designation (i.e. "high", "medium") of risk under the campus' risk assessment methodology.
   7. 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.

b. Periodic Review of Granted Exceptions

Exceptions must undergo periodic review and approval by appropriate administrators. The exception review process must include:

A. Periodic review as per the schedule established above.

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

C. Sufficient review 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:

- Updated approval from changed management or organization.
- Any changes in hardware, software, policy or standard relevant to this exception.

O. Enforcement

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

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. The CSU may refer suspected violations to appropriate law enforcement agencies. The CSU reserves the right to temporarily or permanently suspend, block, or restrict access to Information Assets, independent of campus investigation 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.

Student infractions of this policy must be handled in accordance with the established student conduct process.
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. Auxiliary employees who violate the requirements of this 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.

related section: Standards Enforcement

P. Exceptions

A campus may allow exceptions to CSU or campus policies, standards, or practices, so long as such exceptions are reviewed and approved in compliance with the exceptions process outlined in the CSU Information Security Standards.

Q. Contact and Related Documents

Questions about this document may be directed to CSU Information Security Management, infosec@calstate.edu

- CSU Information Security Privacy of Personal Information Policy
- CSU Information Security Responsible Use Policy
- ISO/IEC 27002:2013 Information technology --Security techniques --Code of practice for information security controls

VI. Definitions

Term	Definition
Anti-virus Software	Software that detects or prevents malicious software.
Application	A software program designed to perform a specific function for a user. Applications include, but are not limited to, word processors, database programs, development tools, image editing programs, and communication programs.
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.
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.
Authentication	The process of confirming that a known individual is correctly associated with a given electronic credential; for example, by use of passwords to confirm correct association with a user or account name (is a term that is also used to verify the identity of network nodes, programs, or messages).
Authenticator Assurance Level (AAL)	A term used by NIST 800-63-3 which indicates the extent to which a user controls the authenticator bound to their account. Example: AAL2 provides high confidence that that the user controls the authenticator.
Authorized	The process of determining whether or not an identified individual or class has been granted access rights to an information assets, determining what type of access is allowed; e.g., read-only, create, delete, and/or modify.
Availability	Ensuring that information assets are available and ready for use when they are needed.
Biometric Devices	An instrument intended to validate the identity of an individual through comparison of a demonstrated intrinsic physical or behavioral trait with a record of the same information previously captured. Examples: fingerprint, retina scan, voice recognition.
Business Continuity Planning	See CSU System Business Continuity Program.
Campus	Any CSU campus as defined in Section 89001 of the California Education Code to include satellite locations and the Chancellor's Office.
Campus Limited Access Area	Physical area such as a human resources office, data center, or Network Operations Center (NOC) that has a defined security perimeter such as a card controlled entry door or a staffed reception desk.

Term	Definition
Campus Managers	Responsible for (1) specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility and (2) ensuring that program staff and other users of the information asset are informed of and carry out information security and privacy responsibilities.
Catastrophic Event	An event that causes substantial harm or damage to significant CSU information assets. Examples: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.
Computer Security Incident Response Team (CSIRT)	The name given to the team that handles security incidents.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Control	Countermeasures (administrative, physical, and technical) used to manage risks.
Critical Asset	An asset that is so important to the campus that its loss or unavailability is unacceptable.
Critical Data	Data necessary to perform University operations.
Critical Systems	Systems which are necessary to conduct University business.
CSU Network	Any CSU administratively controlled communications network that is within the CSU managed physical space. Such networks may interconnect with other networks or contain sub networks.
Data	Individual facts, statistics, or items of information represented in either electronic or non-electronic forms.
Data Center	A facility used to house information processing or telecommunications equipment that handle protected or critical information assets.
Data Owner	Person identified by law, contract, or policy with responsibility for granting access to and ensuring appropriate controls are in place to protect information assets. The duties include but are not limited to classifying, defining controls, authorizing access, monitoring compliance with CSU/campus security policies and standards, and identifying the level of acceptable risk for the information asset. A Data Owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of information within that unit.
Data Steward	(also known as “Data Custodian”) An individual who is responsible for the maintenance and protection of the 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.
Digital Certificate	Also known as a public key certificate or identity certificate, a digital

Term	Definition
	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.
Digital Signature	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.
DMZ	DMZ (De-Militarized Zone) is a set of one or more information assets logically located outside of a protected network that is accessible from the Internet (open to the world) with limited controlled data exchanges with the protected environment.
Electronic Media	Electronic or optical data storage media or devices that include, but are not limited to, the following: magnetic disks, CDs, DVDs, flash drives, memory sticks, and tapes.
Electronic Signature	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.
Employee	Any person who is hired by the CSU to provide services to or on behalf of the CSU and who does not provide these services as part of an independent business.
Encrypted Protocol	An agreed-to secure means of data transmission over a network (wired or wireless).
Encryption	The process of encoding data so that it can be read only by the sender and the intended recipient.
Excessive Authority	Assignment of a single individual to overlapping administrative or management job functions for a critical information asset without appropriate compensating controls such as added reviews or logging.
Hardening	A defensive strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.
Hardware	Physical devices including, but is not limited to, portable and non-portable workstations, laptops, servers, copiers, printers, faxes, and PDAs.
High Risk Workstation	Any workstation that is used for elevated access to critical systems or stores or accesses level 1 information in such quantities as to require notification of a government entity (i.e. over 500 records

Term	Definition
	under HIPAA or CA 1798.29), or information classified as protected level 1 due to severe risk.
Identity Assurance Level (IAL)	A term used by NIST 800-63-3 which indicates the level of confidence provided by the identity proofing process in determining the identity of an individual. Example: IAL2 requires either remote or in-person identity proofing.
Information Assets	CSU information systems, network resources, and data (regardless of medium).
Information Security Program	An organizational effort that includes, but is not limited to: security policies, standards, procedures, and guidelines plus administrative, physical, and technical controls. The effort may be implemented in either a centralized or a decentralized manner.
Information Systems	A combination of hardware, network and other resources that are used to support applications and/or to process, transmit and store data
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]
Least Privilege	A concept of information security by which users and their associated applications execute with the minimum amount of access required to perform their assigned duty or task.
Level 1 Data	Data designated as *confidential* under the CSU Information Security Standards, Data Classification Standard. It must be protected due to its highly sensitive nature and/or legal obligation. Level 1 Data is subject to the most stringent restrictions on use and disclosure.
Level 2 Data	Data designated as internal use under the CSU Information Security Standards, Data Classification Standard. It must be protected due to its sensitive nature. Level 2 Data must be protected from unauthorized access and disclosure but is not subject to the same very high level of protection as Level 1 Data.
Level 3 Data	Data designated as general under the CSU Information Security Standards, Data Classification Standard. Level 3 Data is subject to few restrictions on use and disclosure.
Lockout Time	The amount of time for which logins to an account are disabled. Usually invoked once a threshold of invalid login attempts has been reached.

Term	Definition
Logical Access	The connection of one device or system to another through the use of software.
Malicious Software	Software designed to damage or disrupts information assets.
Mobile Devices	Devices containing electronic CSU data which are easily transported. Such devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), and “smart” phones.
Network Resources	Resources that include, but are not limited to: network devices (such as routers and switches), communication links, and network bandwidth.
Non-public	A service or information intended only for the internal use of the organization.
Notice-triggering Information	Specific items of personal information identified in California Civil Code Sections 1798.29 and 1798.3.
Operating System	Software that is primarily or entirely concerned with controlling a computer and its associated hardware, rather than with processing work for users
Patch (Patching)	The installation of a software update designed to fix problems, improve usability, or enhance performance.
Personal Electronic Information	Information resulting from incidental personal use of University resources.
Personally Identifiable Information	Any information that identifies or describes an individual, including, but not limited to name, Social Security number, physical description, address, phone number, financial matters, medical or employment history (California Information Practices Act).
Physical Access	Being able to physically touch, use, and interact with information systems and network devices.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Private IP Addresses	Defined by Request for Comment (RFC) 1918 as range of non-routable addresses.
Private Key	The secret key of a key pair used to create a digital signature or decrypt data.
Protected Asset	Information asset containing protected data.
Protected Data	Level 1 and Level 2 Data which are defined in the CSU Information Security Standards, Data Classification Standard. This data has been categorized according to its risk to loss or harm from disclosure.
Public Information	Any information prepared, owned, used or retained by a campus and

Term	Definition
	not specifically exempt from disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.
Public Key	The well-known key of a key pair used to verify a digital signature or to encrypt data.
Public Key Cryptography	An encryption method that uses an asymmetric key-pair.
Remote Access	Any connection from an external, non-campus network to any campus information system, data, or network resource.
Risk	The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.
Risk Assessment	A process by which quantitatively and/or qualitatively, risks are identified and the impacts of those risks are determined. The initial step of risk management.
Risk Management	A structured process which identifies risks, prioritizes them, and then manages them to appropriate and reasonable levels.
Risk Mitigation	Reduce the adverse effect of an event by reducing the probability of the event occurring and/or limiting the impact of the event if it does occur
Screen Filter	An item which can be used to limit the visibility of content displayed on a computer screen to those who are immediately in front of it.
Security Awareness	Awareness of security and controls, in non-technical terms, conveyed to motivate and educate users about important security protections that they can either directly control or be subjected to.
Security Incident	An event that results in any of the following: Unauthorized access or modification to the CSU information assets. An intentional denial of authorized access to the CSU information assets. Inappropriate use of the CSU's information systems or network resources. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.
Security Training	Specific technical understanding of how to secure the confidentiality, integrity and availability of applications, operating systems and information assets to prevent or detect security incidents
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.
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the

Term	Definition
	possible exception of limited user-specific application configuration settings.
System Administrator	(also known as “System Personnel” or “Service Providers”) Individuals, who manage, operate, support campus information systems; or manage networks.
Third Parties	For the purposes of the CSU Security Program, third parties include, but are not limited to, contractors, service providers, vendors, and those with special contractual agreements or proposals of understanding.
Threat	A person or agent that can cause harm to an organization or its resources. The agent may include other individuals or software (e.g. worms, viruses) acting on behalf of the original attacker.
User	Anyone or any system which accesses the CSU information assets. Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.
Vulnerability	A flaw within an environment which can be exploited to cause harm.

VII. References

Keywords: 8000

NIST Special Publication 800-63-3

VIII. Authority

This policy is issued pursuant to Section II of the Standing Orders of the Board of Trustees of the California State University, and as further delegated by the Standing Delegations of Administrative Authority. The president may delegate authority and responsibility described in this policy to other campus officials pursuant to Section VI of the Standing Orders of the Board of Trustees of the California State University.

All Revision Dates

4/30/2024, 5/20/2022, 5/12/2022

Approval Signatures

Step Description	Approver	Date

EVC	Steven Relyea: Executive Vice Chan & CFO	4/30/2024
Area Manager	Bradley Wells: Assoc VC, Business & Finance	4/30/2024
Owner	Josh Callahan: Chief Info Security Officer	4/25/2024