Policy History

Date	Action
	Approved by President Mohammed Qayoumi
May 27, 2013	Reviews: IT Management Advisory Committee
April 9, 2013	Draft Policy Released

Table of Contents

Introduction and Purpose

The San José State Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of SJSU information assets.

In accordance with the California State University Information Security Policies, this Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of SJSU, violate individual privacy rights and possibly constitute a criminal act.

The intent of the Information Security Program is to:

- Document roles and responsibilities.
- 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).
- Document risk management strategies to identify and mitigate threats and vulnerabilities to level 1 and level 2 information assets as defined in the SJSU Data Classification and Handling Standard.
- Document incident response strategies.
- Document strategies for ongoing security awareness and training.
- Comply with applicable laws, regulations, SJSU and CSU policies.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which SJSU must protect from unauthorized access.
- Integrity and availability of information stored on or processed by SJSU information systems.
- Compliance with applicable laws, regulations, CSU policies and SJSU policies governing information security and privacy protection.

The SJSU Information Security Program and security standards are not intended to prevent, prohibit or inhibit the sanctioned use of information assets as required to meet SJSU's core mission and campus academic and administrative goals.

Scope

Consistent with the CSU Information Security Policies, the SJSU Information Security Program shall apply to the following:

- Central and departmentally-managed campus information assets.
- All users employed by SJSU, its auxiliaries, contractors, vendors or any other person with access to SJSU's network resources or information assets. This includes non-SJSU-owned computing devices that may store protected information.
- 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 SJSU. This includes third party service providers' systems that access or store SJSU's protected information.

Auxiliary organizations, external businesses and organizations that use campus information assets must operate those assets in conformity with the SJSU Information Security Program.

SJSU retains ownership or stewardship of information assets owned (or managed) by, or entrusted to SJSU. SJSU 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 intended to protect the confidentiality, integrity and availability of information and are not intended to restrict, monitor or utilize the content of legitimate academic and organizational communications.

Information Security Policy

Consistent with CSU Information Security Policies, SJSU's Information Security Program, combined with the Information Technology Resource Responsible Use Policy, establishes policy and sets expectations for protecting university information assets. These are supported by related policies, standards, guidelines and practices to facilitate campus compliance:

- Policies are high-level statements of principle, equivalent to organizational law, that provide technology agnostic scope and direction to the campus community.
- Standards establish specific criteria and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and they provide a basis for verifying compliance through audits and assessments.
- Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.
- Practices consist of one or more series of interrelated steps to be taken to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to facilitate completing the process.

Policies should be written so as to require infrequent changes while standards, guidelines and practices are typically updated as needed to address specific changes in policy, technology or university practices.

The Information Security Officer (ISO) and Associate Vice President, Information Technology Services & Chief Information Officer (AVP/CIO) are responsible for coordinating the development and dissemination of information security and technology policies, standards, guidelines and procedures, respectively.

Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and university strategic planning and initiatives. Key campus stakeholders are consulted early on and research is conducted to find potential models from other universities.

Using a standard format, a draft policy is developed and shared broadly with campus constituents for review and comment. All input is considered, but is not necessarily incorporated. The Information Technology Management Advisory Committee is advisory and reports to the President on policies and plans related to management and use of information resources. The IT Management Advisory Committee reviews and forwards final draft recommendations to the President for formal campus adoptions. Standards, guidelines and practices do not require Presidential approval; campus constituents, including the IT Management Advisory Committee, may be asked to review and comment, but final approval rests with the ISO and AVP/CIO.

Only new and substantially altered policies, standards and practices are subject to this process; minor updates and changes can be made and documented without undergoing the full review process.

Approved policies, standards, guidelines and practices will be published on the web, incorporated into security training programs and disseminated through available campus communication methods. They will be reviewed annually to determine if any changes are required.

Information Security Policy Management

In accordance with CSU policies, the SJSU ISO oversees an annual review of this program and communicates any changes or additions to appropriate SJSU stakeholders. The SJSU Information Security Program shall be updated as necessary to reflect changes in CSU policies, SJSU's academic, administrative or technical environments, or applicable laws and regulations.

The program may be augmented, but neither supplanted nor diminished by additional policies and standards.

Information Security Organization and Governance

In accordance with CSU policy, SJSU's president has designated an ISO to coordinate and oversee campus compliance with the Information Security Program and related laws, policies, standards and practices. The ISO, with the AVP/CIO, reports annually to the university President's Cabinet on the current state of campus security relative to protecting university information assets.

SJSU's ISO reports to the AVP/CIO and works to develop, implement and ensure compliance with policies, standards and practices related to the security of information technology resources.

The AVP/CIO reports directly to the Vice President for Finance and Administration/Chief Financial Officer (VP/CFO). The VP/CFO is a member of the senior management team that provides advice and counsel to the president. The AVP/CIO regularly briefs the Academic Senate, deans, department heads/chairs, campus techs and other campus constituents on information security issues.

Security policies, standards and practices are reviewed with campus constituents through various committees and other governance bodies. The AVP/CIO chairs, and the ISO is a standing member of, the IT Management Advisory Committee. This committee is advisory and reports to the President's Cabinet on policies and plans related to IT management and use of information resources.

The ISO chairs the Campus Information Security Committee (CISC) which reviews policies, standards and practices from a university-wide operational perspective. The CISC meets every 3rd Wednesday with campus information authorities and reviews application data requests, IT acquisitions and other transactions from an information security perspective.

The Information Security Management Team (which includes the ISO, Identity and Information Security Manager, and AVP/CIO) meets regularly to review security policies and issues, discuss specific incidents, identify areas of concern, clarify and interpret policies and develop communication and implementation strategies and plans. The team works with designated university officials, managers, technical staff and others to manage security incidents.

Administrators across the university are responsible for ensuring information security policies, standards and practices are followed by employees in their respective areas. An information security coordinator in each college and major administrative unit will provide necessary operational oversight to assist the responsible administrators.

Technical support staff and individual users are expected to follow established standards and practices and to report potential security violations.

Appendix A includes a detailed description of campus roles and responsibilities for information security.

Risk Management, Assessment and Planning

The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Understanding risk, especially the magnitude of the risk, allows organizations to prioritize resources.

Information security risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact for each risk to information security assets. Once a risk has been identified, strategies are developed to reduce the risk to acceptable levels, share or shift the risk to another party or assume the identified risk. Risks are monitored with the ongoing collection of information about the risk.

In accordance with CSU Information Security Policies, SJSU's risk management processes to identify information assets containing level 1 and level 2 data are defined in the SJSU Data Classification and Handling Standard.

Risk Assessment

SJSU performs periodic assessments of its information security risks and vulnerabilities. Risk assessments may be aimed at particular types of information, areas of the organization or technologies. Risk assessments are part of an ongoing risk management process. They provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls. The SJSU Security Risk Self-Assessment and Inventory Standard contains processes to perform annual self-assessments and inventory reporting.

The Security Risk Self-Assessments and Inventories are requested, collected, reviewed and evaluated by the ISO and the AVP/CIO. The results are shared with executive management and campus computing committees. The outcomes are produced in a Risk Assessment Report, updated annually, identifying control objectives, risk exposures, mitigation strategies and action plans for addressing each risk with timelines.

Risk Planning

Security must be a consideration from the very beginning of any project at the university, rather than something that is added later. In addition, a control review should be performed before implementation of computer systems which store or handle protected information. This may include:

- A technical security evaluation to ensure appropriate safeguards are in place and operational.
- A risk assessment, including a review for regulatory, legal and policy compliance.
- A contingency plan, including the data recovery strategy.
- A review of on-going production procedures, including change controls and integrity checks.

Privacy of Personal Information

Consistent with CSU Information Security Policies, all users of campus information systems or network resources are advised to consider the open nature of information disseminated electronically, and must not assume any degree of privacy or restricted access to information they create or store on campus systems.

SJSU is a public university and information stored on campus information systems may be subject to disclosure under state law. No campus information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, SJSU acknowledges its obligation to respect and protect private information about individuals stored on campus information systems and network resources.

Collection of Personal Information

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

Where such information is collected:

- The Information Authority and individual user collecting the information will use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.
- The Information Authority and individual user collecting the information shall store personally identifiable information only when it is appropriate and relevant to the purpose for which it has been collected.

Access to Personal Information

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

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

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

- To comply with applicable laws or regulations.
- To comply with or enforce applicable SJSU or CSU policy.
- To ensure the confidentiality, integrity or availability of campus information.
- To respond to valid legal requests or demands for access to campus information.

If SJSU personnel accesses, modifies and/or discloses information about an individual and/or the individual's activities on campus information systems or network resources, staff will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by SJSU policy or applicable laws.

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

Access to Electronic Data Containing Personal Information

Individuals who access or store protected data must use due diligence to prevent unauthorized access and disclosure of such assets.

Browsing, altering or accessing electronic messages or stored files in another user's account, computer or storage device is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for SJSU business reasons. This prohibition does not affect:

- Authorized access to shared files and/or resources based on assigned roles and responsibilities.
- Authorized access by a network administrator, computer support technician or departmental manager where such access is within the scope of that individual's job duties.

- Access to implicitly publicly accessible resources such as university websites.
- Campus response to subpoenas or other court orders.
- Campus response to a request pursuant to public record disclosure laws.

Personnel Information Security

In accordance with CSU Information Security Policies, the following are the information security pre-employment requirements and guidelines for managing separations or changes in employment status.

Employment Requirements

Hiring managers must conduct background checks on people hired into positions involving access to level 1 information assets, as defined in the SJSU Information Classification and Handling Standard.

Separation or Change of Employment

Access rights must be promptly revoked from information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy or by the Information Authority. Unless otherwise authorized in writing, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical and remote access, must be promptly revoked.

Procedures must be implemented to ensure proper disposition of information assets upon termination. Electronic and paper files must be promptly reviewed by an appropriate manager to determine who will become the data steward of such files, and identify appropriate methods to be used for handling the files. If the separating employee is holding resources subject to a litigation hold, the Information Authority 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.

Procedures must be implemented to 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.

Procedures must be established to allow for separated employees to obtain such incidental personal electronic information, as appropriate.

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

Information Security Awareness and Training

Consistent with CSU Information Security Policies, all employees with access to the SJSU network and information assets must participate in information security awareness training.

The Information Security Awareness Training Program is designed to help individuals protect and respond appropriately to threats to campus information assets containing level 1 or level 2 data, as defined in the SJSU Data Classification and Handling Standard.

The Program promotes awareness of:

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

- CSU and campus notification procedures in the event protected data is compromised.

Within about one month of employment, new employees are provided individual access to the Information Security Awareness Training Program.

Employees are expected to complete the training within 90 days of receiving their access to the program.

Department heads and campus executive management are responsible for, and will be provided status of training compliance.

Managing Third Parties

The CSU Information Security Policies require third parties who access SJSU information assets to adhere to appropriate CSU and SJSU 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.

Granting Access to Third Parties

Third party service providers may be granted access to campus information assets containing protected data, as defined in the SJSU Data Classification and Handling 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 Information Authority list and based on the principles of business need and least privilege.

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

Information Technology Security

The CSU Information Security Policies require SJSU to appropriately secure its information technology resources to protect the confidentiality, integrity and availability of university information. This includes, but is not limited to computer systems, network resources and software applications.

Each member of the campus community and third party providers are responsible for the security and protection of information technology resources over which they have control. The physical and logical integrity of these resources must be protected against potential threats such as unauthorized access, malicious or criminal action, inadvertent compromise and inappropriate use.

Protection of information technology assets must be commensurate with the criticality of the function performed, the nature and level of access provided, information classification associated with the asset, exposure of the asset to potential risks, and the liability to the university if the asset is compromised. In general, a combination of administrative, operational and technical security safeguards will be required.

Combined with SJSU's Responsible Use Policy, said policies and related standards and practices set expectations and define minimum requirements for securing SJSU's information technology infrastructure and resources.

Protections Against Malicious Software Programs

Each device with the effective capability must have controls 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 of a campus network or information system.

Network Security

Storing protected information assets or transmitting protected data over the campus network must ensure confidentiality, integrity and availability.

Mobile Devices

Protected data must not be stored on mobile devices unless effective security controls have been implemented to protect the data. Individuals must use encryption, or equally effective measures, on all mobile devices that store level 1 data as defined in the SJSU Data Classification and Handling Standard. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the ISO. Other effective measures include physical protection that ensures only authorized access to protected data.

Information Asset Event Monitoring

Event monitoring must not be conducted for the purpose of gaining unauthorized access, 'snooping,' or for other activities that violate the CSU Responsible Use Policy or SJSU Acceptable Use Policy. Records created by monitoring controls (e.g., event logging) must be protected from unauthorized access and reviewed regularly. Access to the data generated by the monitoring controls (e.g., logging) must be restricted to those who have a business need.

Data generated by event monitoring must be retained for a period of time that is consistent with effective use, SJSU records retention schedules, regulatory and legal requirements such as compliance with litigation holds, or with IT Security Standards.

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 each month. 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).

Configuration Management

Configuration standards to ensure that information technology systems, network resources and applications are appropriately secured to protect confidentiality, integrity and availability are provided in the IT Security Standards.

Change Control

Consistent with CSU Information Security Policies, the following provides direction and support for managing changes to information assets and provides guidance for implementing emergency changes to information assets.

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. Change control processes are documented in the IT Security Standards.

Emergency Changes

Only authorized persons may make emergency changes to campus information assets containing level 1 data, as defined in the SJSU Data Classification and Handling 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.

Access Control

The CSU Information Security Policies require controlled access to SJSU information assets and guidance for: granting access to SJSU information assets; separating duties of individuals who have access to an SJSU information asset; conducting reviews of access rights to SJSU information assets; and modifying user access rights to SJSU information assets.

On-campus or remote access to information assets containing level 1 or level 2 data, as defined in the SJSU Data Classification and Handling Standard, must be based on operational and security requirements. Appropriate controls must be in place to prevent unauthorized access to protected information assets. This includes not only the primary operational copy of the protected information assets, but also data extracts and backup copies. IT Security Standards define requirements for provisioning approved additions, changes and terminations of access rights and reviewing access of existing account holders. Access to campus protected information assets must be denied until specifically authorized.

Access to public and shared resources may be excluded from this requirement. Information Authorities 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 Information Authority, unless otherwise defined by CSU or SJSU policy.

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

Authentication controls must be implemented for access to campus information assets that access or store protected data, must be unique to each individual, and may not be shared unless authorized with the below criteria. 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 in writing at least annually.

Separation of Duties

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

Access Review

Information Authorities and others, as appropriate, must review, at least annually, user access rights to information assets containing protected data. The results of the review must be documented.

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.

Information Asset Management

In accordance with the CSU Information Security Policies, the SJSU Property Office maintains an inventory of information assets. These assets are categorized and protected throughout their entire life cycle, from origination to destruction.

- Property Office Procedure Manual [pdf]

  (http://www.sjsu.edu/finance/docs/property_manual.pdf)

Information Systems Acquisition, Development and Maintenance

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

- Contracting and Procurement Guidelines [pdf]

  (http://www.sjsu.edu/finance/docs/Purchasing%20Guideline_Final_11.7.12.pdf)

Information Security Incident Management

In accordance with CSU Information Security Policies, security incidents involving loss, damage or misuse of information assets or improper dissemination of protected data, regardless of medium, must be properly reported and investigated to mitigate adverse impacts, protect the university from similar incidents, and comply with existing policies and laws.

Security incidents will be managed by the Information Security Management Team. The Security Incident Reporting Procedures contain processes for reporting security incidents internally and externally, and the process to respond to inquiries from notified users, their spouse, vendors or the media.

Physical Information Security

Consistent with CSU Information Security Policies, the physical areas where information assets containing protected data are located must be protected from unauthorized physical access. These physical areas include data centers, office areas and other locations. Information assets which access protected data that are located in public and non-public access areas must be physically secured to prevent theft, tampering or damage. Information Authorities must review and document physical access rights to campus limited-access areas annually.

Business Continuity Planning (BCP)

In accordance with CSU policies, SJSU must ensure that our information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to user.

BCP is the methodology for restarting the university after a hypothetical severe disaster, assuming that a large percentage of resources will have been lost. The end-product of BCP is a logistical digest for all identified Essential Units addressing the issue of how to bring back their operations.

The SJSU Business Continuity Steering Committee (BCSC) is designated by the President's Cabinet to be responsible for oversight of BCP. Committee members of BCSC will get input from, and oversee the preparedness work by the managers of the Essential Units in their respective areas. Being prepared for business continuity is integral to campus managers' responsibility.

The SJSU BCP is designed to cover all campus activities that are identified as essential to the restarting of all key university businesses on campus. It does not cover auxiliary organizations.

As an on-going function, BCP is an iterative process that goes through periodic review and update cycles.

Each cycle has the following components:

1. Identify all essential units (i.e., 'Business Impact Analysis').
2. Identify critical processes and services within essential units.
3. Identify priority of critical processes.
4. Resiliency assessment (i.e., analysis of vulnerabilities).
5. Solution design.
6. Communication of business continuity issues to managers of essential units; and training.
7. Implementation of solutions for vulnerabilities.
8. Testing, 'lesson learned,' and remedial actions.
9. End of one BCP cycle, start of a new BCP cycle.

IT Business Continuity Plan

Information technology service areas are responsible for developing and maintaining a plan for the restoration of services in the event of a disaster, in accordance with campus BCP. The plan should outline priorities, recovery time estimates, objectives and procedures for all IT functions. In the case of a catastrophic event that disrupts campus IT services, the plan should provide priorities and strategies for the restoration of hardware, applications and data.

The IT Business Continuity Plans is an iterative process that goes through periodic review and update cycles. Departments who administer their own hardware, applications and data are responsible for the development and maintenance of their own BCP based on their department's needs, taking into account the recovery time estimates outlined in the BCP and IT BCP.

Compliance

SJSU information security practices must comply with a variety of federal and state laws and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information, including personally identifiable information (e.g., social security number, driver's license number), personal financial information (e.g., credit card numbers), medical information and confidential student information.

There are many individual laws, regulations and policies that establish our information security requirements. Some of the most notable include:

CALIFORNIA CODE OF REGULATIONS, TITLE V, SECTIONS 42396 - 42396.5

Title V of the California Code of Regulations, specifically sections 42396 - 42396.5 addresses privacy and principles of personal information management applicable to the CSU.

CALIFORNIA INFORMATION PRIVACY ACT

The California Security Breach Information Act (SB-1386) is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is acquired by an unauthorized person. The Act, which went into effect July 1, 2003, was

created to help stem the increasing incidence of identity theft. Found in the California Civil Code (Sections 1798.29).

CALIFORNIA PUBLIC RECORDS ACT

The California Public Records Act addresses exclusions to the disclosure of public information of personally identifying information that may be a violation of personal privacy.

CALIFORNIA SENATE BILL 25 (SB 25)

SB 25 extends those social security number restrictions to all government agencies, including public colleges and universities. Under SB 25, public entities will have to ensure that social security numbers don't get posted or displayed on any printed material, or used on identification cards.

FAIR AND ACCURATE CREDIT TRANSACTIONS ACT (FACTA)

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act of 2003, which required 'creditors' to adopt policies and procedures to prevent identity theft. These requirements are described in section 114 of FACTA and are known as the 'Red Flags Rule.'

The Red Flags Rule applies to financial institutions and 'creditors' that offer or maintain accounts that provide for multiple transactions primarily for personal, family or household purposes. Institutions are considered creditors if they provide goods or services that are not fully paid for in advance or allow individuals to defer payment for goods or services.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

Enacted in 1974, FERPA protects the privacy of student education records and affords students certain rights with respect to the student's 'education records.' More information about the SJSU FERPA program can be found at:

- SJSU Bulletin: Privacy Rights of Students [pdf]

  (http://www.sjsu.edu/studentconduct/docs/FERPA.pdf)

GRAMM-LEACH-BLILEY ACT (GLBA)

Enacted in 1999, the GLBA requires financial institutions to carefully protect customers' financial information. Universities are 'financial institutions' by virtue of their loan servicing, and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) 'safeguarding' rules and (2) privacy rules. All personally identifiable financial information from students, parents and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure.

INFORMATION PRACTICES ACT OF 1977 (IPA)

Found in the California Civil Code (Sections 1798.14 - 1798.23), the IPA requires State agencies to record only personal information that is relevant and necessary to accomplish the purpose of the agency. Additionally, the agency should collect personal information directly from the individual who is the subject of the information, rather than from any other source.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. It applies to American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc. International.

Additional laws and regulations specify the disclosure of employee and student information and require the university to take specific actions in the event SJSU suspects protected information may have been disclosed, either accidentally or maliciously, to unauthorized parties. Individuals who handle protected information are encouraged to speak with their managers, Information Authorities or the ISO to familiarize themselves with relevant laws and regulations.

Policy Enforcement

Consistent with CSU policies, the ISO is authorized by the President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the university community.

Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the ISO. Approved requests will be reviewed annually to determine if an exception is still warranted.

SJSU reserves the right to temporarily or permanently suspend, block or restrict access to campus information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of SJSU information assets; to protect SJSU from liability; or to enforce this policy and its related standards and practices.

The ISO will work with the AVP/CIO to develop supplemental standards and practices to facilitate campus compliance with this policy; develop communication plans to inform users about the policy and its related standards and practices; advise departments on the interpretation and enforcement of this policy; and confer with university legal counsel and other university officials on matters involving potential violations.

Potential violations will be investigated in a manner consistent with applicable laws and regulations, collective bargaining agreements, CSU and campus policies, standards, guidelines and practices.

The ISO, or designee, will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate university officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Allegations against employees that are sustained may result in disciplinary action. Such actions will be handled by the appropriate Human Resources office using existing disciplinary processes consistent with the terms of the applicable collective bargaining agreement and the California Education Code. Student infractions will be handled by the Office of Student Rights and Responsibilities using established policies and practices. Auxiliary organization employees may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to SJSU.

Non-compliance may result in personal, criminal, civil or other administrative liability. Departments may be held accountable for remediation costs or other financial penalties incurred due to non-compliance.

Appeals of university actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for SJSU students and employees.

Appendix A—Information Security Roles and Responsibilities

ACADEMIC PERSONNEL OR JUDICIAL AFFAIRS

- Supports the Information Security Officer and the Associate Vice President/Chief Information Officer in the reporting, investigating, assessing and resolving potential security violations.

ASSOCIATE VICE PRESIDENT, IT SERVICES & CHIEF INFORMATION OFFICER (AVP/CIO)

- Provides policy and operational guidance to the university.
- Provides security standards and guides for protecting information assets.
- Ensures compliance to existing campus information security policies, standards and procedures.
- Coordinates with Information Security Officer to develop and implement information security policies, standards and procedures.
- Coordinates with the Information Security Officer, if needed, on the investigation, assessment, tracking, resolution and reporting of security issues involving information technology resources and reports potential criminal violations to the appropriate entities in a timely manner.
- Coordinates with the campus Information Security Officer to evaluate the risk introduced by any changes to campus operations and systems.
- Serves as the chairperson for the SJSU IT Management Advisory Committee.
- Notifies the Assistant Vice Chancellor for Information Technology Services if a breach of level 1 data has occurred.
- Reviews information security risks at least annually.
- Reviews the Information Security Annual Report provided by the Information Security Officer.

CAMPUS INFORMATION SECURITY COMMITTEE (CISC)

- Reviews, provides feedback, and recommends action to the Associate Vice President/Chief Information Officer to improve security policies and practices to protect SJSU's digital information assets, and the information technology resources used to access, transmit and store them.

HUMAN RESOURCES/ACADEMIC PERSONNEL/JUDICIAL AFFAIRS

- Investigates alleged security violations by individual students, faculty and staff to determine if disciplinary action is appropriate.
- Interprets, recommends and imposes sanctions and discipline regarding security violations in accordance with existing policy and practice.

INFORMATION AUTHORITY/OWNER

The Information Authority is identified by law, contract or policy, with responsibility for granting access to and ensuring appropriate use of the information.

- Responsibilities are identified in the SJSU Information Classification, Handling, Retention, and Inventory Standards.

INFORMATION CUSTODIAN/STEWARD

The information custodian/steward has operational responsibility for the physical and electronic security of information.

- Responsibilities are identified in the SJSU Information Classification, Handling, Retention, and Inventory Standards.

INFORMATION SECURITY OFFICER (ISO)

- Coordinates, administers, communicates and maintains the Information Security Program on behalf of the President.

- Advises the President and campus leadership on information security matters.
- Consults with campus administrators to ensure campus information security policies and standards meet campus goals.
- Investigates, assesses, tracks, resolves and reports suspected violations of policies and procedures in coordination with appropriate entities.
- Confers with Associate Vice President/Chief Information Officer and Information Authorities on information security policies, standards, procedures, security violations, campus security risks and other security matters, as needed.
- Provides input to the campus budget process regarding prioritization and required resources for security risk mitigation.
- Responds to information security related requests during an audit and coordinates the CSU information security audits.
- Serves as the campus representative on the CSU Information Security Advisory Committee.
- Serves as chairperson for the SJSU CISC.
- Reviews and approves application data requests and authentication requests.
- Notifies the CSU Chief Information Security Officer if a breach of level 1 data has occurred.
- Oversees the campus incident response program, the information security awareness and training program, and annual self-assessment inventory processes.
- Reviews computing equipment loss reports and security incidents and determines action needed, if any.
- Provides annual Information Security Report, and Risk Assessment and Action Plan to the President, the Vice President of Administration and Finance and the Associate Vice President/Chief Information Officer.

INFORMATION SECURITY MANAGEMENT TEAM

Membership: AVP/CIO, ISO, Identity and Information Security Manager, Managing Sr. Director Infrastructure Services, and Sr. Director Information Services.

- Reviews information security policies, incidents, audit responses and recommendations from CISC.
- Determines need for information security product and service proposals.
- Makes information security recommendations for policies, products and service implementation.
- Provides information security training for campus staff (e.g., attendees at: information security forum, LAN coordinator meetings, etc.).
- Makes recommendations for information security training materials.

INFORMATION USERS

Individuals who need and use university information as part of their assigned duties, or in fulfillment of assigned roles, or functions within the university community.

- Responsibilities are identified in the SJSU Information Classification, Handling, Retention and Inventory Standards.

IT MANAGEMENT ADVISORY COMMITTEE

Reviews, provides feedback, and recommends action to the Associate Vice President/Chief Information Officer to improve security policies and practices to protect SJSU's digital information assets, and the information technology resources used to access, transmit and store them.

PRESIDENT

- Establishes an information security program, which is compliant and consistent with the CSU information security policy.
- Reviews information security risks at least annually.
- Reviews Information Security Annual Report provided by the Information Security Officer.
- Notifies the Chancellor if a breach of level 1 data has occurred.

PROPERTY OFFICE

- Provides a copy of the Computing Equipment Loss Report to the Information Security Officer that contains information about lost or stolen computing.

UNIVERSITY POLICE

- Receives and investigates all reports of potential criminal law violations involving any computing device containing university information and any university information resources.

USERS

- Observes all laws, regulations, policies and procedures related to security of information and systems.
- Protects the privacy rights of university faculty, staff and students.
- Protects the physical security of information and systems assigned to them.
- Reports suspected violations of security policies and procedures for university information to their supervisor, who will report it to the Information Security Officer and/or Information Technology Services, depending on the nature of the violation.

VICE PRESIDENT FOR ADMINISTRATION AND FINANCE

- Notifies the CSU Office of General Counsel of a breach of security to California residents whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.
- Reviews information security risks at least annually.
- Reviews Information Security Annual Report provided by the Information Security Officer.