Standard: Information Classification and Handling

Executive Summary

San Jose State University (SJSU) is highly diversified in the information that it collects and maintains on its community members. It is the university's responsibility to be a good steward and custodian of the information that it has been entrusted, which must be upheld by all members of the university. In order to apply appropriate security measures for protecting university information resources, data must be evaluated and assigned the proper data classification level of protection that commensurate with the nature of the data and compliance requirements. The value of any data and the impact on the university if the data is exposed or lost must be taken into consideration when assigning a data classification level. Governed by the Institutional Data Management Counsel, the Information Classification and Handling Standard defines the requirements for assigning, maintaining classification settings, and handling sensitive information for all SJSU's computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU.

Information Security Standards

Information Classification and Handling

Standard #	IS-ICH	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	8.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
4/23/2014	Draft sent to Mike
5/13/2014	Revised draft sent to Mike
12/1/2014	Reviewed. Content suggestions. Added comments. Hien Huynh
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus
1/13/2016	Added information on encryption – Hien Huynh

Table of Contents

Introduction and Purpose

Governed by the Institutional Data Management Counsel, this standard defines the requirements for assigning, maintaining classification settings, and handling sensitive information for all San Jose State University's (SJSU) computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") electronic and hardcopy data, computer systems and facilities, with a target audience of all SJSU employees and partners.

Standard

Data Ownership

Refer to the SJSU Information Security Program for detailed roles and responsibilities.

Information Owner

All production information possessed or used by a campus department must have a designated Information Owner who is responsible for determining the appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information and ensuring that the appropriate controls are utilized in the storage, handling, distribution, and regular use of information.

Information Custodian

Each significant type of production information must have a designated Custodian who will properly protect campus department information in keeping with the designated Information Owner's access control, data sensitivity, and data criticality instructions.

IT Department Ownership Responsibility

With the exception of operational computing and network information, the IT Departments must not be the Owner of any production information.

Data Classification

3-Category Data Classification

All SJSU data must be broken into the following three sensitivity classifications: LEVEL 1: CONFIDENTIAL, LEVEL 2: INTERNAL USE ONLY, LEVEL 3: PUBLICLY AVAILABLE. Distinct handling, labeling, and review procedures must be established for each classification.

Data Classification Descriptions

The following descriptions are used for identifying and labeling each sensitivity classification for all SJSU information. For further information, refer to the Information Classification and Handling Cheat Sheet.

Level 1: Confidential (High Risk)

Confidential information can cause the most serious harm to individuals and the University as a result of unauthorized access. Much of this information is protected by statutes, regulation, other legal obligations and mandates including the Health Insurance Portability and

Accountability Act (HIPPA), the Family Educational rights and Privacy Act (FERPA), and information regulated by the Payment Card Industry (PCI). Confidential information is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws or classified as confidential by SJSU.

Information may be classified as confidential based on criteria including:

- Severe Risk: Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the University, its students, employees, or customers. Financial loss, damage to SJSU's reputation, and legal action could occur.
- Limited Use: Information intended solely for use within the University, its auxiliary employees, contractors, and vendors covered by a confidentially-security agreement and limited to those with a business "need-to know."
- Legal Obligations: Information for which disclosure to persons outside the University is governed by specific standards and controls designed to protect the information.

Level 2: Internal Use Only (Moderate Risk)

While possibly not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to SJSU's reputation, violate an individual's privacy rights or legal action could occur.

Information may be classified as internal use only based on criteria including:

- Sensitivity: Information protected due to proprietary, ethical, contractual, or privacy concerns.
- Limited Use: Information intended solely for use within the University, its auxiliary employees, contractors, and vendors covered by a confidentially-security agreement and limited to those with a business "need-to know."

Level 3: Publicly Available (Low Risk)

Publicly available information is information intended to be publicly available or provided to the public. Disclosure of this information does not expose SJSU to financial loss, diminish reputation, or jeopardize the security of information data.

Default Classification

Information without a label is by default classified as Internal Use Only.

Data Encryption and Handling

Security controls must specify how Level 1 information is protected as it is stored, processed, and transmitted on SJSU campus. Security controls must ensure that applications which decrypt Level 1 data have sufficient protection against malicious code or malware. All SJSU computers including desktops, laptops, tablets, mobile devices, storage on exchangeable media and server storing level one data must implement an ISO approved data encryption tool.

Machines that access encrypted data protected against Malicious Code

For any campus machine that decrypts sensitive Level 1 information: If the machine uses applications that decrypt Level 1 data in order to read, write, transmit, or otherwise process the data, then the machine must comply with the Patching and Malicious Code management Standard.

Level 1 Information must be stored encrypted
Level 1 information stored on workstation, laptop, tablet or server hard drives must be encrypted. Level 1 data stored on exchangeable media such as USB and CD/DVD must be encrypted. For further information, refer to the Information Classification and Handling Cheat Sheet and Data Center Security Standard.

Transmission of Level 1 Information
Level 1 information transmitted over public networks outside of SJSU Data Centers must be encrypted, using approved encryption guidelines authorized by the Information Security Office.

Level 1 Information on Cloud Storage and Personal Email prohibited
Storage of Level 1 Information on cloud based storage such as Google Drive, Dropbox, or any other cloud based solutions is prohibited. Transmission of Level 1 Information over personal email is prohibited. For further information, refer to the Information Classification and Handling Cheat Sheet.

User Awareness Training of Level 1 Information Handlers
Users who are accessing Level 1 data as a part of their job function for SJSU campuses must undergo user awareness training on the proper handling and encryption of Level 1 information, prior to allowing them access to applications that decrypt and process this information. For further Information refer to the Information Security Awareness Training Standard.

Authorized Encryption Application
Encryption of Level 1 data must use an encryption application approved by the Information Security Office. Users are prohibited from using other applications for encryption.

Data Labeling

Assigning Data Classification Labels
For all existing production information types, the Information Owner is responsible for choosing an appropriate data classification label to be used by all workers who create, compile, alter, or procure production information. The classification Level (1, 2, or 3) given for the campus department information must meet or exceed ICSUAM 8000 minimum specifications, in accordance with the Information Security Officer (ISO).

Multiple Classification Labeling
When information of various sensitivity classifications is combined, the resulting collection of information must be classified at the most restricted level found anywhere in the sources.

Data Classification Labeling
All Level 1 information must be labeled and handled according to guidelines issued by the Information Security Department, while information not falling into one or more of these categories need not be labeled.

Information Life Cycle Labeling
From the time when information is created until it is destroyed, it must be labeled with a sensitivity designation if it is Level 1.

Labels for Externally-Supplied Information
With the exception of general business correspondence and copyrighted software, all externally-provided information that is not clearly in the public domain must receive a SJSU data classification system label. The SJSU worker who receives this information is responsible for assigning an appropriate classification on behalf of the external party. When assigning a SJSU

classification label, this staff member must preserve copyright notices, author credits, guidelines for interpretation, and information about restricted dissemination

Downgrading Information

Dates for Reclassification

If known, the date that Level 1 information will no longer be sensitive must be indicated on all SJSU sensitive information. This will assist those in possession of the information with its proper handling, even if these people have not been in recent communication with the information's owner.

Expired Classification Labels

Those workers in possession of sensitive information that was slated to be downgraded on a date that has come and gone, but is not known definitively to have been downgraded, must check with the information Owner before they disclose the information to any third parties.

Notifications

The designated information owner may, at any time, downgrade the classification of information entrusted to his or her care as long as the downgrade operates within the confines of ICSUAM8065.S2. To achieve this, the owner must change the classification label appearing on the original document and notify all known recipients and Custodians.

Schedule for Review

To determine whether Level 1 or Level 2 information may be downgraded, at least once annually, information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be downgraded as soon as practical.

Disposition of Information

All Level 1 and Level 2 confidential Information data shall be disposed of in accordance with the Data Disposition Standard.

Definitions

Confidential Information (Sensitive Information)

Any SJSU information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by SJSU from a third party under a non-disclosure agreement.

Information Data

Any SJSU data in any form, and the equipment used to manage, process, or store SJSU data, that is used in the course of executing business. This includes, but is not limited to, corporate, student, customer, and partner data.

Partner
Any non-employee of SJSU who is contractually bound to provide some form of service to Company SJSU.

References

ISO/IEC 27002 - 7.2.1 Classification Guidelines
ISO/IEC 27002 - 7.2.2 Information Labeling and Handling