Standard: Risk Assessment Program

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 with, which must be upheld by all members of the university. The Risk Assessment Program Standard defines the requirements for the identification and classification of the appropriate security controls for all campus sensitive information resources, for not only adhering to these published security standards, but identifying risk exposure areas of sensitive data, and applying appropriate mitigations in order to manage the risks across all campus information assets. The Information Stewards will work with SJSU and Information Security Officer (ISO) to perform a risk assessment with the assigned assets. Once risks have been identified, the Information Stewards will implement security controls as documented in the risk mitigation plan to acceptable levels that were approved by management. Lastly, risks are validated, monitored and audited with the ongoing collection of information about the risk. These standards of due care will help manage the risk of loss of confidentiality, integrity, and availability of SJSU sensitive information.

Table of Contents

Introduction and Purpose

This standard defines the risk management program requirements for the identification of the appropriate security controls for all campus sensitive information, for not only adhering to these published security standards, but identifying risk exposure areas of sensitive data, and applying appropriate mitigations in order to manage the risks across all campus information assets. These standards of due care will help manage the risk of loss of confidentiality, integrity, and availability of SJSU sensitive information.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of SJSU Information Technology Information Owners and Administrators.

Standard

This standard establishes and documents Risk Assessment Program requirements based on SJSU business requirements for protection of sensitive level 1 and level 2 information. For more information on data classification, refer to the SJSU "Information Classification and Handling Standard" [1]. Each campus department is responsible, through its Information Owner, for documenting an inventory of sensitive resources along with a Risk Assessment Questionnaire for each sensitive resource.

Risk Assessment

Each year the Information Security Officer (ISO) in conjunction with each campus IT Unit who is operating desktops, laptops, tablets, network or servers with unique configuration must conduct a security risk assessment. The analysis resulting from this project must include a description of the information security risks currently facing the campus unit, and specific recommendations for preventing or mitigating these risks. Each critical unit within the campus that manages its own computers, networks, or applications must perform this Risk Assessment of three asset categories:

1. Servers storing or processing sensitive data
2. Web applications processing sensitive data
3. Users and Administrators who access sensitive data

The ISO will provide guidance for specific procedures and timelines. After analysis of the security risk exposure areas, coordinated through the ISO, a mitigation plan will develop and then certify that adequate security measures have been implemented to mitigate the risks.

The risk categories are as follows:

0	Not Performed	There are **no security controls or plans in place**. The controls are nonexistent.

1	Performed Informally	Base practices of the control area are generally performed on an **ad hoc** basis. There is general agreement within the organization that identified actions should be performed, and they are performed when required. The practices are not formally adopted, tracked, and reported on.
2	Planned	The base requirements for the control area are planned, implemented, and **repeatable**.
3	Well Defined	The primary distinction from Level 2, Planned and Tracked, is that in addition to being **repeatable** the processes used are more mature: **documented**, **approved, and implemented organization-wide**.
4	Quantitatively Controlled	The primary distinction from Level 3, Well Defined, is that the process is **measured and verified** (e.g., auditable).
5	Continuously Improving	The primary distinction from Level 4, Quantitatively Controlled, is that the defined, standard processes are **regularly reviewed and updated**. Improvements reflect an understanding of, and response to, a vulnerability's impact.

Risk Assessment Questionnaire

Each campus department is responsible for completing a Risk Assessment questionnaire for each application and server storing, processing, and transmitting sensitive data. For more information, refer to the SJSU “Risk Assessment Questionnaire” [2].The procedure for submission of the Risk Assessment questionnaire will be provided by the ISO.

Risk Assessment Resource Inventory

Each campus department is responsible for completing a Resource Inventory worksheet for each group of servers and each application that is processing, storing, or transmitting sensitive level 1 or level 2 information. For more information, refer to the SJSU "Risk Assessment Resource Inventory Application/Server" [3].

Scheduling once a year

Risk Assessments for sensitive information will run once per calendar year, in accordance with the schedule determined by ISO and Information Owner. For more information, refer to the SJSU "Risk Assessment Scheduler" [4].

3rd Party Applications Complete Cloud Security Questionnaire

Any application processing sensitive information that is hosted by a 3rd party provider, including web applications, must complete the Cloud Security Questionnaire. For more information, refer to the SJSU "Cloud Security Questionnaire" [5].

Definitions

Availability

The state that exists when information resources are accessible and usable upon demand by an authorized user.

Confidentiality

The state that exists when data is held in confidence and is protected from unauthorized disclosure to unauthorized individuals, entities, or processes. Misuse of data beyond the scope of their duties by those authorized to use it is also considered to be a violation of data confidentiality.

Compensating Controls

Controls currently in place that reduce the exploitability of a risk exposure. They can be preventative, detective, and responsive.

Control

Security mechanisms implemented to prevent, detect, reduce or eliminate risks. In doing so, controls maintain the properties of availability, integrity, and confidentiality.

Integrity

The state that exists when data is the same as that in the source documents, or has been correctly computed from source data, and has not been exposed to accidental alteration or destruction. Incomplete data, unauthorized changes, or additions to the data, and erroneous source data are all considered violations of data integrity.

Information Asset

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, student, employee, partner, and other campus information.

Partner

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

Risk
The result of a threat acting on a vulnerability, expressed as a product of likelihood (probability) and severity (of impact.)

Risk Assessment
The determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat or hazard. The result of a risk assessment is typically a report that shows assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible defensive measures and their costs and estimated probable savings from better protection.

Residual Risk
The risk that remains after a control is applied to an identified risk, and that control does not eliminate the risk.

Risk Cost\Benefit\Impact Evaluation
The process of evaluating risk compared to value of information-related assets and amount of damage done to system or owner should the system or data be compromised or damaged.

Risk Mitigation
The process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process.

Risk Exposure
Describes the outcome of a successful exploit of the vulnerability by a threat. The rating of low/medium/high rates the impact or consequence of a risk exposure.

Risk Sensitivity
A value relative to the resource's tolerance for risk exposure. The importance or criticality of the resource to the organization. The higher the risk sensitivity, the more valuable it is to the organization, and the lower the risk tolerance it will have.

Risk Severity
Measures the magnitude of consequences from a threat/vulnerability pair being exploited. The magnitude of the vulnerability or weakness, independent of any details about the threat source or the resource sensitivity. Severity rating is meant to describe the extent or scope of the exposure, not list all of the consequences. Severity is asset agnostic. Think of severity as measuring the degree of damages or how pervasive the exploit is.

Threat
Any person, object or event that, if realized, could potentially cause damage to an information resource or the data processed on those resources. This includes damage to the availability, integrity, and/or confidentiality of resources or information.

Vulnerability
Weaknesses in an information resource that can be exploited by a threat.

More Information

References

[1] San Jose State University: “Information Classification and Handling Standard”
[2] San Jose State University: “Risk_Assessment_Questionnaire”
[3] San Jose State University: “Risk Assessment Resource Inventory Application/Server”
[4] San Jose State University: “Risk_Assessment_Scheduler”
[5] San Jose State University: “Cloud Security Questionnaire”
ISO Domain 6: Organization of Information Security Standard
NIST SP 800-30 – Risk Assessment Guide

Information Security Standards

Risk Assessment Program

Standard #	IS-RAP	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	4.0	Contact	Information Security Team	Phone	408-924-1530

Revision History

Date	Action
5/21/2014	Initial draft sent to Mike
01/6/2014	Reviewed. Content suggestions. Added comments. Hien Huynh
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
11/18/2020	Reviewed. Nikhil Mistry
10/20/2021	Reviewed & Grammar. Cole Gunter
10/3/2022	Reviewed. Cole Gunter
7/17/2024	Reviewed and updated