Standard: Data Center Security

June 27, 2024

Executive Summary

The university data centers provide for the reliable operation of SJSU's computing systems, computing infrastructure, and communication systems. Per ICSUAM 8000, California SAM, local, State, and Federal law, this standard defines the requirements for security controls of machines hosted in SJSU data centers to safeguard the confidentiality, integrity, and availability of information stored, processed and transmitted by SJSU.

Table of Contents

Introduction and Purpose

This standard defines the requirements for security controls of machines hosted in SJSU data centers. This standard is composed to explicitly comply with ICSUAM 8000, California SAM, local, State, and Federal law.

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 employees and partners. This standard applies to any machine storing unencrypted Level 1 data at rest, any machine providing internet-facing services outside the campus border firewall (i.e. Web Servers), and campus "core" network aggregation points.

Standard

Storage of Unencrypted Level 1 Information is prohibited on servers

For any machine on the campus, storing level 1 unencrypted data at rest is prohibited unless an exception has been approved by the Information Security Office. For information classification and handling of Level 1 sensitive data, refer to the Information Classification and Handling Standard.

Physical and Environmental Security

Additional physical security controls are included in the Physical Security Standard.

Background Check of Employees

All new employees with entry access to data centers must pass a background check (Livescan) at time of hire.

Electronic Lock Required

Electronic locks are required on all entry doors to data centers storing level 1 data. Entry logs must be properly maintained showing who entered, time, and date. Entry logs must be maintained for at least 90 days.

Networking Equipment Locked

Networking equipment, including lab equipment, must be enclosed and locked in a secured room protected by a lock with logging capabilities..

Management Control of Access

Management needs to have control over access to assets.

Physical Need to Access

Physical access to locked data center rooms is based on the physical need to access principal. Physical access is limited to individuals required to have access. Service employees, including custodians, should not have electronic access to data center locked rooms. University Police personnel are authorized to access the data center in emergency situations only via electronic lock, if functional, or physical access if necessary.

Removal of Permissions upon Employee separation

Upon separation of employees, key cards and keys should be immediately revoked. Alarm codes should be changed upon employee separation.

Audit of Key Cards

Key cards and physical keys must be audited annually and approved by Data Center management (MPP).

Master Keys

Physical locks must not accept master keys.

Moisture Detectors

Moisture Detectors should be in use and placed in data centers, in accordance with the Physical Security Standard.

Smoke Detectors

Smoke Detectors should be in use and placed in data centers, in accordance with the Physical Security Standard.

Environmental Reporting

Environmental alerting, such as temperature and moisture is required for server rooms storing level 1 data.

Fire Suppression

Fire extinguishers or fire suppression for electronic equipment, must be located in each Data Center. Data Centers must not be protected by water-based fire suppression systems.

Uninterruptible Power Supply (UPS)

UPS power in the data center should be capable of handling backup power in room for a minimum of 5 minutes to provide ample time for generator startup.

Glass Windows

Glass windows to public areas allowing viewing of server rooms are prohibited.

Power Generators

Power generators capable of sustaining computer operations during a power outage are required for servers storing level 1 data.

Earthquake Protection

Full-Height server racks which are in excess of three times as tall as they are wide must be affixed to the structure on at least 2 faces to prevent damage in the event of a minor earthquake.

Firewalls between data centers and core networks

Firewalls are required between SJSU data centers and the core networks, as specified in the Network Security Standard.

Emergency Preparedness and Training

All personnel with access to data center rooms must undergo emergency preparedness training on an annual basis, including learning how to operate fire extinguishers, suppression, and emergency alarms.

Test Data Center Emergency Procedures

All data center owners need to develop and test data center emergency procedures annually. Procedures must specify due care for safety and life preservation measures.

IT Disaster Recovery Plan

Data Centers must have an IT Disaster Recovery Plan identifying the critical systems in the data center, the assets necessary for those applications, and the plans for resuming services after an unplanned disruption.

Backup Tapes

Data center room sensitive servers must use backup tapes sent to an offsite location, in accordance with the Data Retention Standard. Tapes containing level 1 data must be encrypted. Data center backup tapes must be in compliance with CSU Executive Order 1031: Records Retention & Disposition Schedules

Food, Drink, Hazardous Materials

Food, drink, and hazardous materials are prohibited in Data Centers.

Labels on Doors

Labels on doors that list “data center” or “telecom” closet are prohibited.

Data Center Owner Training

Data center owners must maintain procedures for training, including the following areas: gaining physical access, removing physical access, visitor access (including logging), stop tailgating, alarm arm/disarm procedures, cleanliness (dust removal), facility services, development access to data center (including logging), and change control (including documentation).

Information Security Standards

Data Center Security

Standard #	IS-DCS	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	5.1	Contact	Information Security Team	Phone	408-924-1530

Revision History

Date	Action
4/25/2014	Draft sent to Mike
5/13/2014	Reviewed with comments and sent to Mike
12/1/2014	Reviewed. Content suggestions. Added comments. Hien Huynh
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
11/18/2020	Reviewed. Nikhil Mistry
10/19/2021	Reviewed & Grammar Corrections. Cole Gunter
11/30/2022	Reviewed. Cole Gunter
6/27/2024	Reviewed - Noel McCormick