Standard: Physical Security

Executive Summary

The Physical Security Standard defines the standards of due care for security physical access to information resources. Physical security describes measures that are designed to prevent access to unauthorized personnel from physically accessing, damaging, and interrupting a building, facility, resource, or stored information assets. According to International Information Systems Security Certification Consortium (ISC)², the Physical (Environmental) Security addresses design, implementation, maintenance, threats, and vulnerabilities controls that can be utilized to physically protect an enterprise's resources and sensitive information of an organization. These resources include but not limited to people, the facility which they work, and the data, equipment, support systems, media, and supplies they utilize.

Information Security Standards

Physical Security

Standard #	IS-PS	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	3.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
5/31/2014	Draft sent to Michael Cook
7/10/2014	QA review
3/5/2015	Revisions – Michael Cook
3/6/2015	Reviewed. Added suggestions and comments. (Hien)
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.

Table of Contents

Introduction and Purpose

This Physical Security standard defines the standards of due care for security physical access to information resources.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary computer facilities which house servers or switches supporting PCI or HIPAA compliant transactions, this standard does not apply to standard university telecommunications closets.

Standard

Physical security perimeter

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

Third-Party Physical Access

Visitor or other third-party access to SJSU offices, computer facilities, and other work areas containing sensitive information must be controlled by staff or appropriate physical controls.

Computer and Communications Facility Location

Multi-user computers and communications facilities must be located in University controlled buildings with no public facing windows.

Computer Facility Fire Resistance

The walls surrounding computer facilities and must be constructed of non-combustible material and resistant to fire for at least one hour, and all openings to these walls, such as doors and ventilation ducts, must be self-closing and resistant to fire for at least one hour. Facilities shall be equipped either with appropriate type handheld fire extinguisher or automated fire suppression systems.

Computer Facility Door Strength

Computer facility rooms must be equipped with fire doors, and other doors resistant to forcible entry.

Computer Facility Door Closing

Computer facility equipment rooms must have doors that automatically close immediately after they have been opened.

Video Cameras and Recording of Security Parameters

CCTV cameras, camcorders, webcams, and other video cameras used on SJSU premises must be placed so that they do not capture fixed passwords, credit card numbers, encryption keys, or any other fixed security parameters.

Physical entry controls

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access and all access is logged.

Physical Access Control to Sensitive Information
Access to every office, computer room, and work area containing sensitive Level 1 information must be physically restricted to limit access to those with a need to know.

Badge Access Sharing
Workers must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances.

Unauthorized Physical Access Attempts
Workers must not attempt to enter restricted areas in SJSU buildings for which they have not received access authorization.

Separated Worker Access to Restricted Areas
Whenever a worker terminates his or her working relationship with SJSU, all access rights to SJSU restricted areas must be immediately revoked. It is the responsibility of the employee's manager to inform the Information Security Office and Facilities Development and Operations of the separation and ensure completion of the employee clearance form.

Visitor Identification
All visitors to SJSU data centers must sign a log prior to gaining access to restricted areas to document the date, time, and purpose of their visit. They also must sign out log when leaving.

Escorting Visitors
Visitors to SJSU spaces containing confidential level 1 data including, but not limited to, customers, former employees, worker family members, vendors, equipment repair contractors, and package delivery company staff must be escorted at all times by an authorized employee.

Escorts Required For All After-Hour Visitors
Visitors must be escorted by an employee authorized by a department manager whenever they are in SJSU offices or facilities outside of normal business hours.

Third-Party Supervision
Individuals who are neither SJSU employees, nor authorized contractors, nor authorized consultants, must be supervised whenever they are in restricted areas containing sensitive information by an authorized personnel.

Unescorted Visitors
Whenever a worker notices an unescorted visitor inside SJSU restricted areas, the visitor must be questioned about the purpose for being in restricted areas, then be accompanied to a reception desk, a guard station, or the person they came to see.

Access to Computers and Communications Systems
Buildings that house SJSU computers or communications systems must be protected with physical security measures that prevent unauthorized persons from gaining access.

Securing Critical or Sensitive Information Handling Activities
All critical, valuable, or sensitive SJSU information handling activities must take place in areas which are physically secured and protected against unauthorized access, interference, and damage.

Computer Center Access
Programmers, users, and others without a legitimate business need for such access must not enter or be inside computer machine rooms.

Computer Center Staff Access
A complete list of all workers who are currently authorized to access the computer center must be maintained, reviewed, and updated by the Computing Services Director on a quarterly basis.

Securing offices, rooms, and facilities
Physical security for offices, rooms, and facilities should be designed and applied (i.e Locked or Manned doors during business hours) as necessary.

Securing Computer or Communications Systems
All multi-user computer and communications equipment must be located in locked rooms.

Securing Propped-Open Computer Center Doors
Whenever doors to the computer center are propped-open, the entrance must be continuously monitored by an employee.

Protecting against external and environmental threats
Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

Secure Areas - Hazardous Materials
Hazardous or combustible materials must be stored at a safe distance from all SJSU secure areas.

Secure Areas - Bulk Supplies
Bulk supplies such as paper forms must not be stored within any SJSU secure area.

Secure Areas - Fire Equipment
Appropriate firefighting equipment must be provided and suitably placed in all SJSU secure areas. Combustible materials shall not be stored in FM-200 protected spaces.

Working in secure areas
Physical protection and guidelines for working in secure areas should be designed and applied.

Communications Equipment Areas
Telephone closets, network router and hub rooms, voice mail system rooms, and similar areas containing communications equipment must be kept locked at all times and not accessed by visitors without an authorized technical staff escort to monitor all work being performed.

Computer Room Deliveries
A secured intermediate holding area must be used for computer supplies, equipment, and other deliveries.

Equipment Security
To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities. Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. Special controls may be required to protect against physical threats, and to safeguard supporting

facilities, such as the electrical supply and cabling infrastructure. Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Smoking, Eating, and Drinking

Workers and visitors must not eat, or drink in the raised floor area in the computer machine room.

Production Computer System Location

All multi-user production computer systems containing level 1 data, firewalls, private branch exchange (PBX) systems, and voice mail systems must be physically located within a secure data center approved by the Information Security Officer.

Computer Center Environmental Controls

Local management must provide and adequately maintain fire detection and suppression, power conditioning, air conditioning, humidity control, and other computing environment protection systems in every SJSU computer center.

Water Damage Precautions

All new SJSU locations that house computer and communications equipment must meet minimum water damage prevention requirements and minimum water damage alarm precautions established by the Information Security Office. These include being above ground level and above flood levels of nearby rivers and sewers, having adequate drainage, and not being situated immediately below water tanks or water pipes. All facilities shall be equipped with moisture detection.

Supporting utilities

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Power Conditioning Equipment

All personal computers and workstations must be outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressors.

Supporting Utilities - Adequate Levels

All utilities that support SJSU information processing facilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning must be provided at a level that is adequate for the systems they are supporting.

Supporting Utilities - Inspection and Testing

All utilities that support SJSU information processing facilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning must be regularly inspected, tested, and documented.

Electrical Supplies – Compliance

All electrical supplies that support SJSU information processing facilities must conform to the equipment manufacturer's specifications.

Uninterruptible Power Supply – Implementation

An uninterruptible power supply (UPS) to support orderly close down or continuous running must be implemented for all information processing equipment that support critical SJSU business operations.

Back-up Generator – Implementation
A back-up generator with adequate fuel supplies must be installed if processing is required to continue in case of a prolonged power failure for all servers processing or storing confidential level 1 data.

Emergency Lighting
Emergency lighting must be provided in all SJSU information processing facilities in case of main power failure.

Cabling security
Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

Power and Telecommunications Cables
The installation and maintenance of power cables and telecommunication lines must be completed by a registered communications distribution designer who follows current Facilities Development & Operations standards.

Cabling Security – Underground
Power and telecommunications cabling carrying data or supporting information services must be underground, where possible, or subject to adequate alternative protection.

Cabling Security – Conduit
Network cabling must be protected from unauthorized interception or damage by using a conduit or by avoiding routes through public areas.

Cabling Security – Segregation
Power cables must be segregated from communications cables to prevent interference.

Equipment maintenance
Equipment should be correctly maintained to ensure its continued availability and integrity.

Equipment Maintenance
All information systems equipment used for production processing must be maintained in accordance with the supplier's recommended service intervals and specifications, with all repairs and servicing performed only by qualified and authorized maintenance personnel.

Retaining Hardware and Software
Hardware and software that is required to read data storage media held in the SJSU archives must be kept on-hand, properly configured, and maintained in operational condition.

Equipment Repairs Require Onsite Maintenance
All SJSU equipment that contains sensitive data must be repaired within the SJSU physical campus. Machines must not be sent outside of the SJSU campus unless all sensitive data has been removed or the vendor has been specifically approved by the Information Security Office, this includes copier/fax machines.

Security of equipment off-premises
Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.

Used Component Equipment Release
Before disposal the department is responsible for ensuring compliance with the SJSU Data Disposition Standard.

Information and Equipment Disposal
Department managers are responsible for the disposal of surplus property no longer needed for business activities in accordance with procedures established by the Information Security Office, including the irreversible removal of sensitive information and licensed software.

Mobile devices must be returned for decommission
All SJSU issued mobile devices, including laptops, PDAs or cell phones must be returned to SJSU when no longer in use by employees or contractors.

Devices Holding Secret Data Must Not be resold
SJSU storage devices such as hard-drives, Embedded Solid State Storage, PDA's, electronic cameras and cell phones which store Secret data must not be resold or recycled. These devices must be destroyed using sensitive information destruction procedures established by the Information Security Office.

Removal of property
Equipment, information or software should not be taken off-site without prior authorization.

Conditions for Lending SJSU Equipment to Employees
Before equipment is removed from SJSU premises, Departmental technicians must confirm that the equipment is properly configured with the necessary security software. All equipment on loan must be accompanied by a Property Checkout Authorization http://www.sjsu.edu/finance/docs/checkout_auth.pdf form.

References
CSU Policy Number: 8080.0 – Information Security Policy.
CSU Policy Number: 8080.S01 – Physical and Environmental Security