Standard: Physical Security

Contents

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-PSS		strevena@csustan.edu	1.0	Stan Trevena	209.667.3137

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.

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 Stanislaus State, Self-Funded, 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 Stanislaus State 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 Stanislaus State 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 Stanislaus State 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 Stanislaus State, all access rights to Stanislaus State restricted areas must be immediately revoked. It is the responsibility of the employee's manager to inform the Information Security Officer and Facilities Services of the separation and ensure completion of the employee clearance form.

Escorts Required for all Visitors

Visitors must be escorted by an employee authorized by a department manager whenever they are in Stanislaus State data centers, offices, or facilities.

Third-Party Supervision

Individuals who are neither Stanislaus State 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 Stanislaus State 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 Stanislaus State 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 Stanislaus State information handling activities must take place in areas which are physically secured and protected against unauthorized access, interference, and damage.

Server Room Access

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

Server Room 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 Information Security Officer on an annual 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 Stanislaus State secure areas.

Secure Areas - Bulk Supplies

Bulk supplies such as paper forms must not be stored within any Stanislaus State secure area.

Secure Areas - Fire Equipment

Appropriate firefighting equipment must be provided and suitably placed in all Stanislaus State secure areas. Combustible materials shall not be stored in Halon and/or 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

Network equipment 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 protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Eating and Drinking

Workers and visitors must not eat or drink in any network equipment or server room.

Production Computer System Location

All multi-user production computer systems containing level 1 data, firewalls, and telephone systems must be physically located within a secure data center approved by the Information Security Officer.

Server Room 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 Office of Information Technology offices and equipment rooms.

Water Damage Precautions

All new Stanislaus State 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 Officer. 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 electrical power filters, or surge suppressors.

Supporting Utilities - Adequate Levels

All utilities that support Stanislaus State 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 Stanislaus State 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 Stanislaus State 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 Stanislaus State 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 Stanislaus State 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 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 Stanislaus State archives must be kept on-hand, properly configured, and maintained in operational condition.

Equipment Repairs Require Onsite Maintenance

All Stanislaus State equipment that contains sensitive data must be repaired within the Stanislaus State physical campus. Machines must not be sent outside of the Stanislaus State campus unless all sensitive data has been removed or the vendor has been specifically approved by the Information Security Officer, 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 Stanislaus State 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 Officer, including the irreversible removal of sensitive information and licensed software.

Mobile Devices Must Be Returned for Decommission

All Stanislaus State issued mobile devices, including laptops, tablets, or cell phones must be returned to Stanislaus State when no longer in use by employees or contractors.

Devices Holding Confidential Data Must Not be Resold

Stanislaus State storage devices such as hard-drives, Embedded Solid State Storage, electronic cameras and cell phones which store confidential data must not be resold or recycled. These devices must be destroyed using sensitive information destruction procedures established by the Information Security Officer.

Removal of Property

Equipment, information or software not assigned to the individual should not be taken off-site without prior authorization.

Conditions for Lending Stanislaus State Equipment to Employees

Before equipment is removed from Stanislaus State 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 form.

References

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