C L A Y T O N S T A T E U N I V E R S I T Y

ITS Physical Security Policy

Executive Summary

The Physical Security Policy 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		Email:	**jameshunter@clayton.edu**
Version #	**1.0**	Contact	**James Hunter**	Phone:	**678-466-4390**

Revision History

Date	Action
11/3/2017	Draft sent to Bill Gruszka and Jason Berry
1/30/2018	Updated
1/31/2018	Sent to ITC Policy Committee for review

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 CLAYTON STATE UNIVERSITY, datacenter and MDF/IDF closets which house servers, switches, and telephony.

Standard

Third-Party Physical Access

Visitor or other third-party access to CLAYTON STATE UNIVERSITY offices, datacenter, and other work areas containing sensitive information must be controlled by staff or appropriate physical controls.

Datacenter and MDF/IDF closet 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.

Datacenter and MDF/IDF Door Strength

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

entry.

Computer Facility Door Closing

Datacenter, and MDF/IDF closets 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 CLAYTON STATE UNIVERSITY 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

Datacenter, and MDF/IDF closets should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access and all access is logged.

Key and Fob 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 CLAYTON STATE UNIVERSITY 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 CLAYTON STATE UNIVERSITY, all access rights to CLAYTON STATE UNIVERSITY restricted areas must be immediately revoked. It is the responsibility of the employee's manager to inform the Information Security Officer, HR, of the separation and ensure completion of the employee clearance form.

Visitor Identification

All non-ITS personnel gaining access to CLAYTON STATE UNIVERSITY datacenter and MDF closet 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.

Escorts Required For All After-Hour Visitors

Visitors must be escorted by an employee authorized by a department manager whenever they

are in CLAYTON STATE UNIVERSITY offices or facilities outside of normal business hours.

Third-Party Supervision

Individuals who are neither CLAYTON STATE UNIVERSITY employees, nor authorized contractors, nor authorized consultants, must be supervised whenever they are in restricted areas containing sensitive

information by authorized personnel.

Unescorted Visitors

Whenever a worker notices an unescorted visitor inside CLAYTON STATE UNIVERSITY 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 Datacenter and MDF/IDF Closets

Buildings that house CLAYTON STATE UNIVERSITY Datacenter and MDF/IDF Closets must be protected with physical security measures that prevent unauthorized persons from gaining access.

Securing Propped-Open Datacenter and MDF/IDF closet Doors

Whenever doors to the datacenter and MDF/IDF closets are propped-open by non-ITS personnel, 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 CLAYTON STATE UNIVERSITY secure areas.

Secure Areas - Fire Equipment

Appropriate firefighting equipment must be provided and suitably placed in all CLAYTON STATE UNIVERSITY secure areas.

Working in secure areas

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

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 MDF/IDF closets or datacenter.

Datacenter Environmental Controls

Management must provide and adequately maintain fire detection and suppression,

power conditioning, air conditioning, and humidity controls in CLAYTON STATE UNIVERSITY MDF/IDF closets and datacenter.

Water Damage Precautions

All MDF/IDF closets and datacenter must meet minimum water damage prevention requirements and minimum water damage. 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.

Supporting utilities

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

supporting utilities.

Power Conditioning Equipment

All MDF/IDF closets and datacenter must be outfitted either with a generator, uninterruptible power supply UPS) systems, electrical power filters, or surge suppressors.

Electrical Supplies – Compliance

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

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 and networking systems processing or storing confidential level 1 data.

Emergency Lighting

Emergency lighting must be provided in the CLAYTON STATE UNIVERSITY datacenter 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.

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.

Cabling Security – Segregation

Power cables must be segregated from communications cables to prevent interference.