|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Data Center Physical Security Policy | | | | | |
| Policy # | CPL-10-02 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888.641.0500 |

Table of Contents

[Purpose 1](#_Toc384701339)

[Scope 1](#_Toc384701340)

[Policy 1](#_Toc384701341)

[Location 1](#_Toc384701342)

[Access Control 2](#_Toc384701343)

[Facility Structure 2](#_Toc384701344)

[Intrusion Protection 2](#_Toc384701345)

[Environmental Controls 2](#_Toc384701346)

[Cable Security 3](#_Toc384701347)

[Equipment Maintenance 4](#_Toc384701348)

[Equipment Delivery and Removal 4](#_Toc384701349)

[Violations 4](#_Toc384701350)

[Definitions 4](#_Toc384701351)

[References 5](#_Toc384701352)

[Related Documents 5](#_Toc384701353)

[Approval and Ownership 5](#_Toc384701354)

[Revision History 5](#_Toc384701355)

Purpose

This policy defines the requirements for establishing physical location and protection controls at Company X information processing facilities to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Scope

This policy applies to all Company X facilities that store information systems, networking and telecommunications equipment, with a target audience of all employees and partners.

Policy

### Location

**Facility Location** - Multi-user computers and communications facilities must be located above the first floor in buildings, away from kitchens, away from bathrooms, in a location separated from the building’s exterior wall by an additional internal wall, as well as in a room without windows.

**Facility Location Address** - The physical address of every Company X computer center is confidential and must not be disclosed to those without a demonstrable need to know.

**Reducing Environmental Threats** - All new Company X computer or communications centers must be located in an area unlikely to experience natural disasters, serious man-made accidents, riots, and related problems.

### Access Control

**Facility Location Monitoring** - Video cameras or other access control mechanisms that monitor the entry and exit points to secure areas must be in place.

### Facility Structure

**Computer Room Wall Construction** - 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.

**Computer Room Walls** - There must be no external windows of multi-user computers and communications facilities. In cases where external windows cannot be avoided, they must be reinforced with impact-rated glass, or hurricane and projectile-rated protective film.

**Additional Walls** - Multi-user computers and communications facilities must be separated from the building`s exterior wall by an additional internal wall.

### Intrusion Protection

Security Perimeter - Access to every Company X secure area must be controlled by a clearly defined security perimeter.

Guarded Access - All third party access to Company X offices, computer facilities, and other work areas containing sensitive information must be controlled by guards, receptionists, or other staff.

**Intrusion Alarms** - All Company X computer centers must be equipped with physical intrusion alarm systems that automatically alert those who can take immediate action.

**Secondary Doors** - All secondary computer center doors must be equipped with crash bars which allow the occupants to quickly exit in the event of an emergency, but also set-off a loud battery-powered alarm when they are opened.

**Doors** - Information processing facility rooms must be equipped with riot doors, fire doors, and other doors resistant to forcible entry.

**Door Alarms** - Information processing facility equipment rooms must have doors that automatically close immediately after they have been opened, and that set off an audible alarm when they have been kept open beyond a certain brief period of time.

### Environmental Controls

**Alarm Systems** - All Company X computer centers must be equipped with fire, water, and physical intrusion alarm systems that automatically alert those who can take immediate action.

**Fire Protection** - 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 Company X computer center.

**Water and Flood Protection** - All Company X locations that house computer and communications equipment must meet minimum water damage prevention requirements and minimum water damage alarm precautions established by the Director if IT Services. 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.

**Surge Protection** - If weather and building conditions pose a significant risk of static electricity discharge, all personal computers and workstations must be outfitted with static protection equipment that has been approved by the Information Technology Department.

**Backup Power Utilities** - All new Company X computer or communications centers must be located and provisioned such that they have ready access to two electrical power substations and two telephone central offices and two Internet providers. Unless cost prohibitive, the redundant paths for each respective utility should be across separate areas of the campus.

### Cable Security

**Cabling Installation** - The installation and maintenance of power cables and telecommunication lines must be completed by a registered communications distribution designer who follows current industry security standards.

**Underground Placement** - Power and telecommunications cabling carrying data or supporting information services must be underground, where possible, or subject to adequate alternative protection.

**Routing and Conduits** - Network cabling must be protected from unauthorized interception or damage by using a conduit or by avoiding routes through public areas.

**Segregation** - Power cables must be segregated from communications cables to prevent interference.

**Labels** - Clearly identifiable cable and equipment markings must be used to minimize handling errors.

**Documentation** - A power and telecommunications cabling patch list must be documented and used to reduce the possibility of errors.

**Termination Points** - Telecommunications cabling carrying data or supporting information services must be protected using armored conduit and locked rooms or boxes at inspection and termination points.

**Alternative Routes** - Telecommunications cabling carrying data or supporting information services must be protected using alternative routings and/or transmission media providing appropriate security.

**Electromagnetic Shielding** - Telecommunications cabling carrying data or supporting information services must be protected using use of electromagnetic shielding to protect the cables.

**Inspections** - Telecommunications cabling carrying data or supporting information services must be protected using periodic technical sweeps and physical inspections for unauthorized devices being attached to the cables.

### Equipment Maintenance

**Information Systems Registration** - All hardware must be registered with the appropriate vendors immediately after Company X staff takes delivery of new or upgraded information systems products, or soon after it has been determined that such products are not yet registered.

**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.

**Maintenance Personnel** - All equipment maintenance must be performed by internal employees or a contracted and bonded outside service.

**Equipment Repairs Require Onsite Maintenance** - All Company X equipment that contains sensitive data must be repaired within the Company X physical campus. Machines must not be sent outside of the Company X campus unless all sensitive data has been removed or the vendor has been specifically approved by the Information Security Department.

**Repair Vendors Require Security Evaluation** - All Company X computing and telecommunication equipment that contains sensitive data and need repair or servicing must only be sent to third-parties that have been evaluated and approved by the Information Security Department.

### Equipment Delivery and Removal

**Off-Site Equipment Approval** - Management must authorize the use of any Company X equipment outside of company premises.

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

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Information Processing Facility** -Any physical location where sensitive Company X information is created, processed, or stored using computer and communications systems.

**Partner –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**System Administrator –** An employee or partner who is responsible for managing a Company X multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

**Visitor** -Any person who does not normally work in a Company X facility or who does not perform regular business functions requiring access to or entry into a Company X facility.

References

CPL: 10.2 Data Center Security

ISO/IEC 27002: 11.2 Equipment

HIPAA: Facility Access Controls - Maintenance Records (A)

HIPAA: Facility Access Controls - Contingency Operations (A)

NIST: Physical and Environmental Protection (PE)

PCI: 9.5 Physically Secure Media

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Owner | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |