Physical and Environmental Controls

Table of Contents

Getting Started

Physical and environmental security programs define the various measures or controls that protect organizations from loss of connectivity and availability of computer processing caused by theft, fire, flood, intentional destruction, unintentional damage, mechanical equipment failure and power failures. Physical security measures should be sufficient to deal with foreseeable threats and should be tested periodically for their effectiveness and functionality.

1. **Determine** which managers are responsible for planning, funding, and operations of physical security of the Data Center.
2. **Review** best practices and standards that can assist with evaluating physical security controls, such as ISO/IEC 27002:2013 or NIST 800-53.
3. **Establish** a baseline by conducting a physical security controls gap assessment that will include the following as they relate to your campus Data Center:
    - Environmental Controls
    - Natural Disaster Controls
    - Supporting Utilities Controls
    - Physical Protection and Access Controls
    - System Reliability
    - Physical Security Awareness and Training
    - Contingency Plans
4. **Determine** whether an appropriate investment in physical security equipment (alarms, locks or other physical access controls, identification badges for high security areas, etc.) has been made and if these controls have been tested and function correctly.
5. **Provide** responsible managers guidance in handling risks. For example, if the current investment in physical security controls is inadequate, this may allow unauthorized access to servers and network equipment. Inadequate funding for key positions with responsibility for IT physical security may result in poor monitoring, poor compliance with policies and standards, and overall poor physical security.
6. **Maintain** a secure repository of physical and environmental security controls and policies and establish timelines for their evaluation, update and modification.
7. **Create** a team of physical and environmental security auditors, outside of the management staff, to periodically assess the effectiveness of the measures taken and provide feedback on their usefulness and functionality.

Top of page

Overview

The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

Physical and environmental safeguards are often overlooked but are very important in protecting information. Buildings and rooms that house information and information technology systems must be afforded appropriate protection to avoid damage or unauthorized access to information and systems. In addition, the equipment housing this information (e.g., filing cabinets, data wiring, laptop computers, and portable disk drives) must be physically protected. Equipment theft is of primary concern, but other issues should be considered, such as damage or loss caused by fire, flood, and sensitivity to temperature extremes.

Top of page

Secure Areas

Objective: To ensure the institution appropriately protects buildings and rooms to prevent unauthorized access, damage, or interference to the information systems therein.

Critical IT equipment, cabling and so on should be protected against physical damage, fire, flood, theft *etc*., both on- and off-site. Power supplies and cabling should be secured. The **physical facility** is usually the building(s) housing the system and network components. The physical characteristics of these structures determine the level of such physical threats as fire, roof leaks, or unauthorized access. Security perimeters should be used to protect areas that contain information and information processing facilities -- using walls, controlled entry doors/gates, manned reception desks and similar measures. The facility's general **geographic location** determines the characteristics of natural threats, which include earthquakes and flooding; man-made threats such as burglary, civil disorders, or interception of transmissions; and damaging nearby activities, including toxic chemical spills, explosions, and fires. Physical protection against damage from fire, flood, wind, earthquake, explosion, civil unrest and other forms of natural and man-made risk should be designed and implemented.

Ensuring complete physical security is impossible, especially in an institution of higher education. While there are several university facilities that have extensive security safeguards in place because of the nature of the services and information contained therein, most of our buildings and rooms allow unfettered access to members of the public. General building and room security safeguards should be in harmony with the overall atmosphere of the building while factoring in threats to the information contained within.

The security of facilities housing information resources can be protected by a number of means (e.g., locked doors with limited key distribution, locked machine cabinets, glass break sensors on windows, motion detectors, door alarms, fire suppression, appropriate heating, cooling and backup power). As with all security issues, the cost of implementing such protection measures has to be weighed against the risks. In some circumstances, the simple act of ensuring that all doors and windows in the room remained closed and locked while unoccupied might suffice. In another case, the sensitivity or criticality of the information contained on and the service provided by building, room, or piece of equipment might be such that more stringent actions are taken.

Appropriate physical safeguards must be placed on equipment that stores or processes institutional data. In addition to physically securing this equipment, consideration must be given to other environmental related aspects that could, if not managed correctly, cause an interruption of service or availability and thus disrupt the university's mission. Careful thought must be given to ensure proper power (e.g., Uninterruptable Power Supplies, generator power backup, redundant power feeds), adequate fire protection, proper heating and cooling, and so on. These environmental safeguards must be commensurate with the sensitivity of the data contained in or processed by the equipment.

Equipment removed from university premises is particularly vulnerable to loss or theft. Therefore, the equipment must be protected when off-site, at home, or while in transit from one location to another.

Secure Areas Resources:

- Joe St Sauver - Physical Security: A Crucial (But Often Neglected) Part of Cybersecurity
- Joe St Sauver - Physical Security of Advanced Network and Systems Infrastructure
- Cornell University Policy - Responsible Use of Video Surveillance Systems
- Indiana University - Facilities Physical Security, Safety, and Privacy Program
- Indiana University Policy - Video and Electronic Surveillance
- Virginia Polytechnic Institute and State University Policy - Safety and Security Camera Acceptable Use
- Wayne State University Policy - Video Surveillance
- Oakland University Policy - Surveillance and Monitoring Technologies
- Penn State University Policy - Electronic Security and Access Systems
- The University of Iowa - Federal Information Security Management Act (FISMA) Plan
- The University of Iowa - Video Surveillance Policy
- University of Manitoba Perspectives of Closed Circuit Television Surveillance
- University of Manitoba Closed Circuit TV (CCTV) Monitoring Policy
- University of Idaho Access Control Policy

Top of page

Equipment

Objective: To ensure the institution appropriately protects information systems equipment from physical and environmental threats.

IT equipment should be maintained properly and disposed of securely. Information stored in equipment being disposed, redistributed, or sold must be securely removed to prevent the disclosure of the information to unauthorized parties.

The system's operation usually depends on **supporting facilities** such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of systems and may cause physical damage to system hardware or stored data. Equipment should be protected from disruptions caused by failures in supporting utilities such as HVAC, water supply and sewage. Power and telecommunications cabling carrying sensitive data should be protected from interception or damage. **Maintenance** contracts should be in place to make certain equipment will be correctly maintained to ensure its continued availability and integrity. Equipment, information or software should not be taken **off-premises** without prior authorization. Appropriate security measures should be applied to off-site equipment, taking into account the different risks of working outside the organization's premises.

There are many types of equipment involved in the creation, collection, storage, manipulation, and/or transmission of information. Filing cabinets are used to store student transcripts. Computer systems are used to process and maintain intellectual property. Data networking equipment and cables are used to transmit voice and video communications. While the value of the equipment cannot be disregarded, the information stored in the device is arguably more valuable than the device itself. Physical and logical security safeguards should be based on the type of data being processed by the equipment. A sound asset management strategy is important to ensure all important equipment is tracked and secured appropriately (see Asset and Data Management chapter for additional information).

All equipment containing storage media should be checked to ensure that sensitive data and licensed software have been removed or securely overwritten prior to **secure disposal**.

In the event that equipment is lost or stolen there are a number of steps that must be taken. Immediately inform the Information security office (or those responsible for information security in the institution) of the loss. Providing as much information as possible about the contents (social security numbers, credit card numbers, protected health information, personally identifiable information, etc.), use (are there passwords on the device that could be used to access secure institution resources) and lifecycle (has the device been shared with others, has it been scrubbed recently of data within, etc.) of the stolen property is essential to determining the risk involved and the required actions involved in its recovery or remote wiping of data housed. Identification of IP addresses, hostnames, computer names registered or other associations with the stolen property provides additional information leading to its return or calculating the impacted loss. Evidence that the device is registered a device management system (mobile management system, online location service, etc.) may enable the risk to be mitigated without the devices recovery. Confirmation that the device is encrypted or backed up also affords data relative to its risk of loss to the institution. Finally have campus police been informed of the theft or loss in order to file appropriate reports for insurance purposes or data loss prevention activities.

Physical security begins with low visibility for secure locations. Unnecessary signage announcing high impact data facilities and network closets should be avoided. Mechanical locks with different keying options, some of which allow multiple key codes for added security are turning to electronic access solutions with entry audit capabilities. Complete access solutions consisting of electronic access control devices and remote monitoring capabilities are becoming more prevalent where access is granted to multitudes of people throughout the day. Fully networked RFID and biometric readers provide additional security where ID cards can be shared, lost or stolen.

Electronic access solutions eliminate managing multiple keys and provide real-time remote access monitoring and audit trail reporting meeting compliance requirements where required. Electronic access reporting can provide simple open/close information as well as additional data involving which credential was used, the time and duration of the event; and the type of access activated. In the event a security breach does occur, the audit trail can be used to forensically reconstruct a series of events leading up to the suspicious activity.

Networking security access keep equipment and spaces secure, connecting building security and equipment access through standardized security credential protocols. Electronic locks can communicate with IP security cameras or other security devices, expanding the scope and capabilities of a security network.

Naturally minimizing access to secure spaces is the best method of controlling the security of those facilities. Only those who absolutely need access should be among those granted that permission. Most technology can be managed remotely without actual physical access to the equipment. Where physical access is determined necessary, that access should be monitored, recorded and audited absolutely.

Fire, humidity, smoke and temperature control systems are all available which can provide monitoring capabilities and automated activity including alarms, fire suppression and alerts. These should all be deployed to keep systems operating with appropriate training (use of gas masks, fire extinguishers, emergency power shutdown management systems, etc.) provided for those responsible for their maintenance and safety.

All of these systems and processes can be implemented over time but should be part of a physical security system for technology. Relatively inexpensive in cost, the assurance that equipment housing essential institution data is safe and secure is well worth the cost.

Equipment Security Resources:

- 7 Things You Should Know about Mobile Security
- Indiana University Policy - Disposal and Redistribution of University Property
- Guidelines for Information Media Sanitization
- Copier and Multi-Function Device Security
- The University of Iowa - Federal Information Security Management Act (FISMA) Plan
- Introduction to Full Disk Encryption (FDE)

Top of page

Resources

EDUCAUSE Resources

- 7 Things You Should Know about Mobile Security
- Physical Security
- Financial and Door-Access Threats of University ID Cards, 2009 Security Professionals Conference
- Mobile Data Paranoia---Three Perspectives on Encryption, 2010 Security Professionals Conference
- Copier and Multi-Function Device Security
- Guidelines for Information Media Sanitization
- Business Continuity and Disaster Recovery
- Introduction to Full Disk Encryption (FDE)

Initiatives, Collaborations, & Other Resources

- Joe St Sauver - Physical Security: A Crucial (But Often Neglected) Part of Cybersecurity
- Joe St Sauver - Physical Security of Advanced Network and Systems Infrastructure
- Cornell University Policy - Responsible Use of Video Surveillance Systems
- Indiana University - Facilities Physical Security, Safety, and Privacy Program
- Indiana University Policy - Video and Electronic Surveillance
- Indiana University Policy - Disposal and Redistribution of University Property
- Virginia Polytechnic Institute and State University Policy - Safety and Security Camera Acceptable Use
- Wayne State University Policy - Video Surveillance
- Oakland University Policy - Surveillance and Monitoring Technologies
- Penn State University Policy - Electronic Security and Access Systems
- The University of Iowa - Federal Information Security Management Act (FISMA) Plan
- The University of Iowa - Video Surveillance Policy
- University of Manitoba Perspectives of Closed Circuit Television Surveillance
- University of Manitoba Closed Circuit TV (CCTV) Monitoring Policy
- University of Idaho Access Control Policy
- How to Build Physical Security into a Data Center (CSO Online, Sarah D. Scalet)
- To Body Cam or Not, That is the Question (Tracy Mitrano, Inside Higher Ed)

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management **Chapter 11**: Physical and Environmental Security	**800-100**: Information Security Handbook: A Guide for Managers **800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-12**: An Introduction to Computer Security - The NIST Handbook **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems	**APO02.02** **APO13.01** **DSS01.04** **DSS04.02** **DSS05.02** **DSS05.04** **DSS05.05** **BAI09.03**	**Req 9** **Req 10** **Req 11**	**ID.AM-4** **ID.BE-4** **ID.BE-5** **PR.AC-2** **PR.DS-3** **PR.IP-5** **PR.IP-6** **PR.MA-1** **PR.MA-2** **PR.PT-2**	**45 CFR 164.310 (a)(1)** **45 CFR 164.310 (b)** **45 CFR 164.310 (c)** **45 cfr 164.310 (d)(1)**

Top of page