Physical Security Of Information Resources Policy

Summary

Physical security measures are an important part of any effort to protect the confidentiality, integrity, and availability of information assets and services. Indeed, adequate physical security is critical to the success of all other information security measures. Without physical access control there can be no protection from unauthorized use of computing resources and without physical environmental control, equipment is prone to theft, unpredictability, and failure.

Purpose

The intent of this policy is to protect the University's computing resources from unauthorized physical access and environmental harm. The policy establishes guidelines and best practices for controlling the physical environment where computing resources reside. Computing resources include, but are not limited to, personal computers, printers, file servers, routers, data switches, cabling, and the associated space where equipment resides.

Policy

Physical Access

- All data centers, data closets, and computer labs, must remain locked when not in use and any devices critical to the University network must be located in lockable dedicated rooms.
- Access to data centers, campus data closets and restricted areas of UITS must be limited to authorized personnel by means of a proximity card access system or other lock measures. Only those personnel requiring access to perform their duties can be granted right of entry. Right of entry documentation is required.
- Users must lock offices and work areas that contain computer equipment or sensitive information.
- All backup tapes and other data storage media are stored in locked, fireproof cabinets when not in use. Transfer of backup media containing historical data to an off-site storage facility is mandatory. See the Data Backup Policy for more details.
- All CSU computer and network equipment must have a label with a unique computer-readable identifier in order to facilitate physical inventory.
- Users must coordinate movement of any type of computer equipment with UITS personnel for proper maintenance of inventory records.

- Report suspected theft, damage, or destruction of computer equipment anywhere on campus to the UITS Help Desk and the University Police.

Environmental Controls

- All data centers, data closets, computer labs, must remain equipped with environmental controls also any other devices that supports the University network must be located in dedicated rooms equipped with appropriate environmental controls.
- Temperature and humidity should be regulated and monitored and fire suppression equipment installed or readily available.
- Critical equipment such as file servers, routers, and data switches must connect to Uninterruptible Power Supplies
- See the CSU Telecommunications Design Manual for additional information.

Procedures and Responsibilities

- Users are responsible for physically safeguarding the computer equipment in their offices and departmental spaces. A designated user safeguards each computer lab and classroom.
- UITS maintains sole authority over the CSU network infrastructure and all computing resources. Authorized UITS personnel have physical access to data centers, data closets, computer labs, offices, and any other location where computing equipment resides based on job requirements.
- UITS personnel may request master or individual keys as necessary to gain access to campus buildings and the rooms containing computing resources. Personnel must adhere to the facilities procedure for obtaining keys and must safeguard the keys at all times.
- Restricted UITS areas include the data center, administrative computing and networking services, desktop support, and the media center. The following applies to these areas:
    - Entrance doors feature a proximity card access system.
    - The Information Security Officer is responsible for granting access to these areas and managing cards and documentation.
    - Contractors and other third parties must show ID, have the purpose of their visit verified, and be escorted by authorized personnel. If a contractor needs repeated access throughout the day, the Information Security Officer may issue them a temporary access card.
    - The Information Security Officer must immediately deactivate lost or stolen cards as well as those assigned to an employee who terminates service.
- During new construction and renovations, the construction manager must adhere to the physical and environmental control requirements set forth in the CSU Telecommunications Design Manual. In addition, they must key the data closets to an existing key or provide new keys to authorized UITS personnel.

Related USG Policy

5.5 (IT Handbook) IT/IS Risk Management & 5.11 (IT Handbook) Minimum Security Standards for USG Networked Devices

Last Update

3/18/2014

Responsible Authority

Chief Information Security Officer