Purpose

This policy defines the requirements for protecting university information and technology resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources, or interference with ACOM operations.

Scope

This policy applies to all ACOM departments, administrative units, and affiliated organizations that use college information technology resources to create, access, store or manage College Data to perform their business functions.

Effective Date

This policy became effective on August 1, 2013.

Policy

All College information and technology resources should have appropriate physical and environmental security controls applied commensurate with identified risks.

Definitions

1. Core network facilities - the cabling, equipment, and network/telecommunications rooms associated with the high speed backbone of ACOM's campus network that carries aggregated network traffic for all the buildings and external network connections (e.g., the Portal, Internet, and LMS connections). As of August 2013, the core network rooms are located at 445 Health Sciences Blvd on the Dothan, Alabama campus and the Data Center (room 124).

2. Mobile storage devices - Any easily movable device that stores College Data, including but not limited to laptop computers, Personal Digital Assistants (PDAs), Smartphone's, external hard drives, and USB flash drives.

3. Uninterruptable Power Supply (UPS) – A device designed to provide power, without delay, during any period when the normal power supply is incapable of performing acceptably.

4. College Data – Any data related to Alabama College of Osteopathic Medicine ("College") functions that are a) stored on College information technology systems, b) maintained by ACOM faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

Roles and Responsibilities

Responsibility for physical and environmental security of ACOM's information and technology resources is shared by the individuals using these systems, units that own them, and system administrators responsible for managing the systems.

Implementing Procedures

1. Physical Security

- Network wiring and equipment – Network wiring and equipment rooms and cabinets must be locked when unattended with access limited to authorized personnel (typically network support staff) and visitors escorted by said authorized personnel. Other network cabling and devices should likewise be physically secured where feasible. Core network facilities should have the date and time of entry and departure recorded.
- Office doors – All office doors should remain locked after hours or when offices are unattended for a prolonged period of time.
- Mobile storage devices – Mobile storage devices should be stored securely when unattended. Appropriate secure storage methods include a locking security cable attached directly to the device, storage in a locked cabinet or closet, storage in a locked private office, or the like. Encrypting data stored on mobile devices, such as whole disk encryption on laptop computers, likewise reduces the risk of a breach of College Data resulting from theft, loss, or unauthorized access. When traveling with mobile storage devices or using them in public places, appropriate security precautions should be taken to prevent loss, theft, damage, or unauthorized access. Use of tracking and recovery software on laptop computers is encouraged.

2. Environmental Security

- Electrical power – Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptable power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities. Each UPS should have sufficient capacity to provide at least 30 minutes of uptime to the systems connected to it. Systems hosting confidential data should also be protected with a standby power generator where feasible.

Related Laws, Regulations, or Policies

1. ACOM Data Classification and Security Policy

2. ISO/IEC 27002:2005, "Information technology – Security techniques – Code of practice for information security management"http://www.iso.org/iso/catalogue_detail?csnumber=50297, published by the International Standards Organization. This is an international security standard that specifies physical and environmental security controls to protect assets from loss, theft, damage, and unauthorized access.

Questions/Waivers

The Director of Information Systems is responsible for this policy. The Dean or designee must approve any exception to this policy or related procedures.

Questions should be directed to the Director of IS.

Contact us

Emergency

Statements and disclosures