Cochise College
Administrative Policy

Category: Technology
Procedure Number; 6056
Title: Physical & Environmental Security Policy

This policy defines the requirements for protecting Cochise College 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 college business operations.

Procedure: 6056.1
Scope

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

Procedure: 6056.2
Roles & Responsibilities

Campus Security: Responsible to provide professional crime prevention, protection, and law enforcement services to maintain and promote human safety and the security of property for the campus and its associated locations.

College Staff: Responsible for complying with this policy, protecting information resources in their possession, and to report incidents or conditions contrary to this policy.

Facilities Management: Responsible for support and maintenance of all college building facilities, building and physical access locks, HVAC and generator environmental controls.

Information Security Team: Responsible to ensure compliance with this policy as a component of the college's information security program. Responsible to provide security incident management in response to reported incidents.

Procedure: 6056.3
General Policy Statement

College departments housing or maintaining Technology Services resources (e.g. telephone networks, data networks, servers, workstations, storage arrays, tape back-up systems, tapes) must protect the physical space in accordance with the data classification (see *Data Classification Policy*) of the Technology Services Resource or the operational criticality of the equipment. Controls shall be implemented to secure against unauthorized physical access, damage and interference to the premises, information and other assets including, but not limited to, sensitive information and Technology Services Resources.

Procedure: 6056.4
Least Privilege

Physical access controls must be granted at the lowest level of access, rights, privileges, and security permissions needed for an individual to effectively perform authorized tasks on any Technology Services Resource, information asset or within a college managed facility.

It is important to understand the role of the individual who is granted access and how that role impacts the privilege requirements. For example, the role of a contracted worker, an individual responsible for janitorial services in secure areas, and a network administrator each have different roles that require varying levels of privilege.

The following positions are eligible for access to the college server rooms: Chief Technology Officer, Director of Infrastructure and Security, Network Administrator, Systems Administrator, Director of Administrative Computing, Executive Director of Facilities and Operations, Maintenance Technicians and Electricians on both Douglas and Sierra Vista campuses.

Departments must also address the technical, operational and managerial controls necessary to achieve compliance with least privilege in those instances where authorized users have physical access to logically separated data, applications and/or virtualized hosts.

Procedure: 6056.5
Visitor Access

Departments must develop and enforce procedures to monitor and control access to secure Technology Services facilities and offices by visitors. Examples of visitors may include contractors, and vendors. Access procedures shall include:

- Use and maintenance of visitor logs documenting name, purpose of visit, sign-in and sign-out date and time
- Use of visitor identification, e.g. badges
- Escorted access to sensitive areas, including data centers and critical equipment locations

Procedure: 6056.6
Physical Access Controls for Technology Services Facilities & Resources

Departments must implement, or ensure third party implementation of, physical access controls for Technology Services data centers, facilities which house critical Technology Services equipment and offices that they are responsible for, including access controls for public areas, deliveries and loading areas. Access controls must be implemented based on the data classification or operational criticality of the Technology Services Resources that are housed within a given facility or security zone.

A security risk assessment must be performed and documented to locate (map) physical areas and the levels of security needed at each location. Appropriate levels of security controls must be installed at areas needing higher levels of security, these include:

- Location of Technology Services facilities in suitably protected areas with minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities
- Use of physical access controls on all doors and entrances such as locks and keys, electronic card access and security guards to ensure protection and safety of college staff, resources, and property, and to comply with health and safety regulations
- Use of motion and breach detection systems
- Use of video monitoring covering all ingress/egress points providing at least 30 days of recording
- Use of locks for private office doors, desk and cabinet drawers when unattended
- Use of secure storage, password access controls and encryption technologies for all unattended desktop and portable computers, peripherals, mobile storage devices and related equipment
- Use of paper or electronic facility access logs
- Ability to monitor, detect and alert physical alarm conditions, including motion and facility entry/exit (including remote video screening)
- Annual testing on all physical controls systems
- Avoidance of publicly accessible data network jacks in secure areas
- Avoidance of collocating data backup media at same facility where source data is also located

Procedure: 6056.7
Equipment & Environmental Security

Departments are responsible for ensuring that college managed facilities (including Technology Services data centers, offices or facilities that house telephone networks, data networks, servers, workstations, and other Technology Services related systems) should implement adequate environmental safeguards to ensure availability and protect against damage (e.g. from high heat, high humidity, etc.). Environmental safeguards that must be evaluated, implemented and maintained as appropriate include:

- Secure installation and maintenance of network cabling that protects against damage to the physical cabling and/or unauthorized interception of data traversing the network cables
- Use of industry standard methods for maintaining consistent power supply including backup generators and/or Uninterrupted Power Supplies (UPS)
- Use of electrical surge protection

- Use of industry standard network components including routers, switches, intelligent hubs and associated cabling
- Use of water leak detection devices
- Use of fire detection and suppression devices including fire extinguishers and sprinkler systems
- Protection against environmental hazards such as floods, fires, etc.
- Ability to monitor, detect and alert environmental alarm conditions, including fire, leak, flood, power, temperature and humidity
- Annual testing on all environmental and protective systems

Any changes to the deployed environmental safeguards that may affect the availability of assets or information must be reported immediately to the appropriate college leadership, impacted business and data owners, as well as the Information Security Team.

Procedure: 6056.8
Data Center Facility Design

In addition to the physical and environment controls previously stated, all on premise data center facilities housing sensitive data or business critical services should take into consideration the following design and construction requirements:

- Redundant HVAC and power distribution
- Emergency generator with suitable capacity to support data facility equipment power load including HVAC systems
- Uninterruptable Power Supplies (UPS) providing sufficient run-time under supported load for emergency generator to come on-line
- Emergency power shutdown controls
- Equipment racks with locking door access
- Raised flooring

Procedure: 6056.9
Equipment Maintenance

Departments must have equipment maintenance Procedures in place to accomplish the following:

- Ensure that all Technology Services equipment and support systems, including physical and environmental, are maintained and updated per manufacturer recommendations to ensure availability and integrity of the data and services provided by the equipment
- Ensure that appropriate lifecycle replacement planning is in place to proactively avoid equipment end-of-support or end-of-life dates

- Ensure that all maintenance, troubleshooting and repair services are provided by authorized personnel
- Keep current documentation including maintenance logs, fault logs, diagnostic details, service records and corrective measures taken
- Ensure adequate controls are implemented for any equipment sent off-site prior to sending the equipment. At a minimum this includes:
    - Securely remove any sensitive data that does not need to reside on the equipment
    - Have reasonable assurance that the party responsible for the equipment while it is off site understands and accepts responsibility for protecting the equipment, information about the equipment or information stored on the equipment at the appropriate level based on the sensitivity classification of the equipment and associated information

Procedure: 6056.10
Secure Disposal, Removal or Reuse of Equipment

Departments must ensure secure handling and disposal of Technology Services related equipment, particularly hardware that contains data classified as having high or medium sensitivity. Procedures must, at a minimum, ensure the following:

- Secure removal or overwriting of licensed software prior to disposal
- Effective and permanent removal of the contents/data on the storage device of computing equipment using industry standard techniques or tools to make the original information non-retrievable (*Note*: using the standard delete or format function is an unacceptable method of achieving this goal)
- Ensure all equipment containing storage media, e.g., fixed hard drives are checked to verify that any licensed software, device configuration or information classified as having medium or high sensitivity are removed or overwritten prior to disposal
- Ensure that all damaged storage devices, particularly those containing information classified as having high or medium sensitivity, are repaired or destroyed

Procedure: 6056.11
Compliance

This policy is a component of Cochise College information security program intended to comply with the PCI-DSS, FERPA, GLBA and other regulations.

Procedure: 6056.12
Exceptions

The Chief Technology Officer (CTO) or a designated appointee is authorized to make exceptions to this policy.

Procedure: 6056.13
Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. The college reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Procedure: 6056.14
Definitions

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Heating, Ventilation and Air Conditioning (HVAC): The system is used to provide heating and cooling services to facilities.

Mobile Storage Device: 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.

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.

User: Any Cochise College faculty, staff, student or partner who has been authorized to access any college electronic information resource.