

UT Space Institute Policy: IT0129-SI – Physical and Environmental Protection	
Version: 1	Effective Date: 10/04/2019

Objectives

To develop a procedure for Physical and Environmental Protection at the University of Tennessee Space Institute (UTSI) that aligns with System-wide policy IT0129 and National Institute of Standards and Technology (NIST) 800 publication series.

Scope

This procedure applies to all users of and information technology (IT) resources owned, operated, or provided by UTSI.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the Institutes IT resources.

Information transmitted or stored on UTSI IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles

This procedure is specific to UTSI. Each User of UTSI resources is required to be familiar and comply with University policies; acceptance is assumed if the user accesses, uses, or handles UTSI information technology resources.

The Chief Information Officer (CIO) is the Position of Authority (POA) for IT at UTSI and is responsible for IT security at the Space Institute.

Standard Details

This procedure describes the Physical and Environmental Protection controls implemented for facilities that house information systems and are not designated as publicly accessible. The controls apply to UTSI employees and visitors. Personnel, such as; employees, contractors and others, that are provided a key fob for access are not considered visitors.

Roles and Responsibilities

CIO. Has overall responsibility for the Physical and Environmental Protection controls as the POA and grants and reviews access to the facilities annually.

IT Administrator. Responsible for overseeing the implementation, monitoring, and maintenance of the following controls.

1. *Physical Access Authorizations*. Only authorized individuals can assess the control room through the use of authorization credentials (key fobs / keys). The CIO reviews and grants access to individuals requiring access to the control room and IT closets located throughout the campus. The CIO will maintain and annually review the list of individuals with authorized access. Individuals will be removed from the list when access is no longer required.
2. *Physical Access Control*. Physical access authorizations are enforced at entry points using keys or key fobs for access. Visitors will be escorted when requiring access to the control room and IT closets. UTSI Physical Plant conducts an annual key inventory and controls access to those areas controlled by access control devices. Locks are rekeyed and new keys cut anytime keys are lost.

UT Space Institute Policy: IT0129-SI – Physical and Environmental Protection	
Version: 1	Effective Date: 10/04/2019

3. *Monitoring Physical Access.* Key fob access must be logged for auditing and incident response purposes. Access logs are to be reviewed monthly and can be requested to aid in incident response.
4. *Visitor Access Records.* Visitors must sign-in at office room F-136 when requiring access to the control center and IT closets. An IT employee will escort the visitor to the area requiring access. When entering the control center, visitors will sign the visitor log and indicate the time of entry and time of departure.
5. *Emergency Shutoff.* Shutoffs are located in the control center for personnel to cut power in emergency situations.
6. *Emergency Power.* The control center is supported by uninterruptible power supplies (UPSs) in the event of commercial power failure. The UPS must supply enough power to facilitate the transition to long-term alternate power (building generator) or an orderly shutdown of servers, if necessary.
7. *Emergency Lighting.* The control center and building are covered by emergency lighting in the event of a power outage.
8. *Fire Protection.* The control center is protected by a fire detection and automatic suppression system. The system is inspected annually.
9. *Temperature and Humidity Controls.* Temperature and humidity are maintained and monitored in the control center. Alarms are setup if temperature or humidity exceed acceptable levels.

Discretionary Controls

Discretionary Controls are security controls whose scope is limited to a specific area or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower established controls.

1. *Physical Access Authorizations*
 - a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides;
 - b. Issue authorization credentials for facility access;
 - c. Review the access list detailing authorized facility access by individuals regularly; and
 - d. Remove individuals from the facility access list when access is no longer required.
2. *Physical Access Control*
 - a. Enforce physical access authorizations at entry/exit points to the facility where the information system resides by;
 - 1) Verifying individual access authorizations before granting access to the facility;
 - 2) Controlling ingress to the facility using physical access control devices.
 - b. Maintain physical access audit logs for entry/exit points;
 - c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible;
 - d. Escort visitors and monitor visitor activity;

UT Space Institute Policy: IT0129-SI – Physical and Environmental Protection	
Version: 1	Effective Date: 10/04/2019

- e. Secure keys, combinations, and other access control devices;
- f. Inventory keys to ITS facilities annually; and
- g. Change combinations and keys when keys are lost, combinations are compromised, or individuals are terminated.

3. *Monitoring Physical Access*

- a. Monitor physical access to the facility where the information system resides to respond to physical security incidents;
- b. Reviews physical access logs monthly and upon occurrence of events or potential indications of events; and
- c. Coordinate results of reviews and investigations with the organizational incident response capability.

4. *Visitor Access Records*

- a. Maintain visitor access records to the facility where the information system resides; and
- b. Review visitor access records monthly.

5. *Emergency Shutoff*

- a. Provide the capability of shutting off power to the information system or individual system components in emergency situations;
- b. Place emergency shutoff switches or devices to facilitate safe and easy access for personnel;
- c. Protect emergency power shutoff capability from unauthorized activation.

6. *Emergency Power.* Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or the transition of the information system to long-term alternate power in the event of a primary power source loss.

7. *Emergency Lighting.* Maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

8. *Fire Protection.* Maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

References

IT0129 - Physical and Environmental Protection

NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations