



SPACE INSTITUTE

UT Space Institute Policy: IT0130-SI – Personnel Security	
Version: 1	Effective Date: 10/07/2019

Objectives

To establish a procedure for developing and maintaining a Personnel Security Program at the University of Tennessee Space Institute (UTSI) to ensure individuals granted access to systems and data are vetted in order to maintain information security objectives.

Scope

This program 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 program 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.

Program Details

The purpose of this program is to ensure that personnel occupying Positions of Responsibility, including third-party providers, are trustworthy and meet established security criteria for those positions, and that the environment in which they function operates securely and does not constitute an unacceptable security risk.

Roles and Responsibilities

CIO. Has overall responsibility for the Personnel Security Program as the POA.

IT Administrator. Responsible for overseeing the implementation and maintenance of the program.

1. **Personnel Screening**. All regular employees, LDAs, and adjunct faculty members are subjected to background checks before employment offers are made as part of UT System Human Resources’ pre-employment background checks. Additional information can be found at <https://hr.tennessee.edu/jobs/background-checks/>.
2. **Personnel Termination**. When an employee is terminated:
 - All University security/system-related information and property used by the employee is retrieved;
 - User accounts are removed from security groups and information systems when the termination notice is received by IT;
 - Any accounts associated with the employee are disabled 1 year after the termination date; Accounts are deleted 1 semester after disabling.

UT Space Institute Policy: IT0129-SI – Physical and Environmental Protection	
Version: 1	Effective Date: 10/07/2019

3. **Third-Party Personnel Security.** When third-party affiliates have completed their contracted work:
 - All IT assets registered on the network for them is removed;
 - VPN or any other type of remote access is disabled;
 - Any credentials they created or used is disabled or changed.
4. **Personnel Sanctions.** Users are expected to comply with all University policies. Employees who fail to comply are subject to sanctions outlined in UT Policy HR0525 - *Disciplinary Action*.

References

IT0130 - *Personnel Security*

HR0525 - *Disciplinary Action*

NIST SP 800-34 - Security and Privacy Controls for Federal Information Systems and Organizations

Definitions

Positions of Responsibility - Positions that perform job functions that have, can grant, or can approve access to sensitive information or business critical systems.

Sensitive information - Information that is protected against unwarranted disclosure. Protection of sensitive information may be required for legal, ethical, privacy, or proprietary considerations. Sensitive information includes all data which contains: Personally Identifiable Information, Protected Health Information, student education records, card holder data, or any other information that is protected by applicable laws, regulations, or policies.