



UT Space Institute Policy: IT0133-SI – Security Planning Program	
Version: 1	Effective Date: 11/27/2019

Objective

To establish a formal, documented program to ensure that Security Plans providing an overview of security requirements and the controls to address those requirements are in place for critical information systems.

Scope

This plan applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee Space Institute (UTSI) including its remote centers.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

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

Principles

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this plan is based on those guidelines. This plan is based on guidelines in NIST Special Publication 800-53 Rev4 *Recommended Security Controls for Federal Information Systems and Organizations*.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

UTSI must develop or adopt and adhere to a plan that demonstrates compliance with related policies and standards. This plan is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of University policy is assumed if a User accesses, uses, or handles University resources.

Plan Details

This plan addresses the security control requirements to guide the effective implementation and management of audit controls and records.

This plan addresses the control requirements to guide the effective implementation and management of security plans, policies, and procedures.

Roles and Responsibilities

Chief Information Officer: Has overall accountability of this Security Planning Policy as the Position of Authority.

IT Administrators: Responsible for ensuring security planning activities are carried out and updated as stated in policy.



UT Space Institute Policy: IT0133-SI – Security Planning Program	
Version: 1	Effective Date: 11/27/2019

Applicable Systems

This plan applies to all IT systems under the responsibility of UTSI personnel. A list of these systems can be found in the UTSI System Classification and Risk Assessment sheet.

Program

Being a unit of the University of Tennessee Knoxville, UTSI has adopted the security program from their campus (PL-1). This involves the creation and maintenance of System Security Plans (PL-2) that provide an overview of security requirements for the systems on our campus and a description of the controls that are in place or planned. A listing of these controls can be found in Appendix A of the IT0121-SI-Information Security Program document.

System Security Plans will be revised as changes are made to the systems and will be reviewed annually (PL-3).

Rules of behavior for system users are provided in the Acceptable Use Policy available on the UTSI website and are provided to new faculty, staff, and students during orientation (PL-4).

References

IT0133 – *Security Planning Policy*

IT0121-SI – *Information Security Program*

NIST SP 800-53 Rev4 - *Recommended Security Controls for Federal Information Systems and Organizations*