

UT Space Institute Policy:	
IT0131-SI – Security Assessment and Authorization Plan	
Version: 1	Effective Date: 10/07/2019

Objective

To establish a formal, documented program to manage the confidentiality, integrity, and availability of business-critical information systems at UTSI through the assessment of security controls.

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 describes how UTSI will:

- Periodically assess the security controls of information systems to determine if the controls are adequate and implemented effectively;
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities of information systems;
- Authorize the operation of information systems and any associated information system connections; and
- Monitor information system security controls on a continuous basis to ensure continued effectiveness of the controls.

UT Space Institute Policy:	
IT0131-SI – Security Assessment and Authorization Plan	
Version: 1	Effective Date: 10/07/2019

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.

Roles and Responsibilities

Executive Director or designee. Responsible for authorizing the operation of information systems as the Position of Authority.

Chief Information Officer. Has overall accountability of this Security Assessment and Authorization Plan.

IT Administrator. Responsible for overseeing the implementation, maintenance, and execution of this plan and associated procedures.

System Baseline

The System Baseline provides a comprehensive overview of a particular system. It includes information such as name, IP address, system type, description, purpose, and initial setup steps. A security assessment will be conducted upon the creation of the system with results documented in the UTSI System Classification and Risk Assessment sheet.

Security Assessments

Assessments of security controls on all UTSI systems will be conducted when a system is created and annually thereafter to determine the effectiveness of implemented controls and if any deficiencies exist. The list of controls can be found in Appendix B of IT0121-SI – *Information Security Plan*. The results from the security assessment will be documented in the UTSI System Classification and Risk Assessment sheet (CA-2).

Continuous Monitoring

Continuous monitoring facilitates the ongoing evaluation of the effectiveness of security controls deployed to all UTSI systems (CA-7). This is accomplished through:

- Configuration management processes
- Periodic security assessments of applicable security controls
- Monitoring and reporting of system status
- Responding accordingly to monitoring results

Plan of Action and Milestones

When deficiencies are discovered during assessments or continuous monitoring activities, remedial actions must be documented. The IT Administrator will develop a plan of action and milestones to correct found deficiencies and include in the System Security Plan (CA-5).

System Interconnections

System interconnections and Interconnection Security Agreements (ISAs) must be reviewed annually and updated as needed (CA-3). System interconnections are to be included in the System Security Plan.



SPACE INSTITUTE

UT Space Institute Policy:	
IT0131-SI – Security Assessment and Authorization Plan	
Version: 1	Effective Date: 10/07/2019

References

IT0121-SI - *Information Security Plan*

IT0131 - *Security Assessment and Authorization*

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

Definitions

Authorizing Official. Official or position with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to University operations and assets.