

UT Space Institute Policy:	
IT0134-SI – System and Communication Protection Program	
Version: 1	Effective Date: 10/06/2019

Objective

To establish a formal, documented system and communication protection program to ensure compliance with requirements established by the University

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 program is based on those guidelines. This program is based on guidelines in NIST Special Publication 800-53 Revision 4, *Security and Privacy 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 program is designed to help ensure the confidentiality, availability, and integrity of business-critical information assets and data, both in storage and during transmission, are protected.

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

Chief Information Officer. Has overall accountability of this System and Communication Protection Program as the Position of Authority.

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

UT Space Institute Policy:	
IT0134-SI – System and Communication Protection Program	
Version: 1	Effective Date: 10/06/2019

Network Protection

UTSI utilizes a SonicWall NSA firewall for boundary protection (SC-7) and to help protect the network from Denial of Service (DoS) attacks (SC-5).

Cryptographic Key Management (SC-12)

UTSI establishes and manages cryptographic keys for required cryptography employed within the information system and documents the use in system security plans.

Collaborative Computing Devices (SC-15)

Systems at UTSI prohibit remote activation of collaborative computing devices except by the IT personnel. Users physically present at the devices are given explicit indication of connection.

Architecture and Provisioning for Name/Address Resolution Service (SC-22)

UTSI has deployed fault-tolerant systems for name/address resolution services for both internal and external queries. Internal and external name/address resolution services are separated via firewall with external queries only being accessible in our network DMZ.

References:

IT0134 - *System and Communication Protection*

NIST SP 800-53 Revision 4 - *Security and Privacy Controls for Federal Information Systems and Organizations*

Definitions:

Boundary Protection - Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).

Cryptographic Key - A string of bits used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.



SPACE INSTITUTE

UT Space Institute Policy:	
IT0134-SI – System and Communication Protection Program	
Version: 1	Effective Date: 10/06/2019

Denial of Service (DoS) - Actions that prevent a system from functioning in accordance with its intended purpose. A system may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

Demilitarized Zone (DMZ) – A physical or logical subnet that separates an internal network from other untrusted networks, usually the internet.