

UT Space Institute Policy: IT0127-SI – Audit and Accountability Plan	
Version: 1	Effective Date: 10/06/2019

Objective

To establish a formal, documented plan for managing risk and implementing best practices with regards to the creation and retention of audit evidence.

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.

Roles and Responsibilities

Chief Information Officer: Has overall accountability of this Audit and Accountability Plan as the Position of Authority.

UT Space Institute Policy: IT0127-SI – Audit and Accountability Plan	
Version: 1	Effective Date: 10/06/2019

IT Administrators: Responsible for ensuring audit logging is functioning properly and adhere to requirements of this plan.

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.

Audit Events

An event is any observable occurrence in an information system that is significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs.

Information systems should be configured to audit for the following events (AU-2):

- Password changes
- Successful and failed logons
- Administrative privilege usage
- System alerts and error messages

Audit Records Content

Information systems should be configured to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event (AU-3). At minimum, the following elements should be included in each audit record:

- Timestamp - expressed in UTC, GMT, or local time with the UTC offset (AU-8)
- Event source (e.g., IP address, hostname)
- Event information (e.g., error codes or messages, description)
- Event type (e.g., logon, logoff)
- User or account associated with an event
- Source service or application name
- Event outcome (e.g., success, failure)

Audit Storage Capacity

There should be enough storage capacity allocated to reduce the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability (AU-4).

UT Space Institute Policy: IT0127-SI – Audit and Accountability Plan	
Version: 1	Effective Date: 10/06/2019

Audit Review, Analysis, and Reporting

Audit logs and records are to be reviewed and analyzed regularly for indications of inappropriate or unusual activity and any findings reported to the CIO.

Audit Record Retention

Audit records must be retained to provide support for after-the-fact investigations of security incidents and to meet regulatory and University information retention requirements. They must also be retained until they are no longer needed for legal, audit, or any other purposes (AU-11).

References

IT0127 – *Audit and Accountability*

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

Definitions

Analysis - The examination of acquired data for its significance and probative value to the case.

Audit Event - Any security-relevant occurrence in the system which can be a change to the security state of the system and/or an attempted or actual violation of the system access control or accountability security policies.

Audit Record - An individual entry in an audit log related to an audited event.

Event - Any observable occurrence in a system and/or network.