

UT Space Institute Policy: IT0132-SI – Identification and Authentication Plan	
Version: 2	Effective Date: 10/07/2019

Objective

To establish formal, documented identification and authentication plan for managing risk from user access and authentication into business-critical information systems and to provide the minimum requirements to control that risk.

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 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.

Roles and Responsibilities

Chief Information Officer. Has overall accountability of this Identification and Authentication Plan as the Position of Authority.

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

Plan Details

All IT systems must be protected against unauthorized modification, disclosure, or destruction in order to ensure information remains confidential, accurate, and available when needed. This plan is to be reviewed annually (IA-1).



UT Space Institute Policy:	
IT0132-SI – Identification and Authentication Plan	
Version: 2	Effective Date: 10/07/2019

Identifier Management (IA-4). New faculty, staff and students are directed in their new hire/orientation packet to complete the New User Account form at <https://www.utsi.edu/new-user-account/>. This generates a help ticket for IT personnel to create the account. The answering IT personnel verifies with advisor/supervisor and/or HR and creates the user account after confirmation.

Identifier is created to match the NetID generated by the UT Knoxville campus.

Upon notice of separation with University or inactivity, identifier is marked for deletion one year from notification date.

Authenticator Management (IA-5). When a new employee AD account has been created, the password is set to a default password by IT personnel. The account is marked to require that the user reset the password upon first logon.

Authenticator Feedback (IA-6). The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

Additional Information. More information on password requirements, account inactivity, and service account requirements can be found in IT1002-SI - Password Standard.

References

IT0132 - *Identification and Authentication*

IT1002-SI - *Password Standard*

NIST SP 800-34 Revision 4 - *Security and Privacy Controls for Federal Information Systems and Organizations*

Definitions

Active Directory (AD) - The Windows OS directory service that facilitates working with interconnected, complex and different network resources in a unified manner.

Authenticator - The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Identifier - Unique data used to represent a person's identity and associated attributes.