

UT Space Institute IT Procedure: Account and Credential Management	
Version: 1	Effective Date: 10/01/2025

Purpose

To provide guidance and structure for the campus to create and maintain consistent processes for user account lifecycle management and inventory processes of University accounts used to access IT resources. This includes processes to address the credential creation and issuance, account and credential usage, modifying access, and account termination.

Scope

This procedure applies to University owned or managed Assets, Systems, and Resources only. It does not apply to Assets, Systems, and Resources not owned by the University unless specifically stated in the policy.

Procedure

This procedure is partially inherited from the account management process and systems of the UT System. Currently, UTSI maintains its own Active Directory infrastructure for access to local computers and resources on the UTSI campus. All other University resources are accessed via UT System accounts. This procedure pertains only to the process in place at UTSI.

All UTSI accounts are managed via Active Directory and are established via the UTSI HR Sign-In process where users must complete the New User Request Form.

Only UTSI IT staff have access to accounts with escalation privileges.

Initial passwords are generated by the IT department upon account creation. Users are prompted to change this password on the first login. Password requirements are follows:

Passwords must be at least twelve characters in length for accounts using MFA and 14-characters for accounts not using MFA.

Passwords must contain characters from all of the following four categories (IA-5):

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, \$, #, %)

Passwords must be changed every 90 days.

UT Space Institute IT Procedure: Account and Credential Management	
Version: 1	Effective Date: 10/01/2025

The disabling of user accounts is triggered by the HR Sign-Out process or by direction from HR or Executive staff. Unused or inactive accounts are reviewed and disabled monthly. Disabled accounts are deleted quarterly.

Service accounts (SCCM, SCVMM, SQL, etc) necessary for enterprise software are stored in Active Directory with a description of their function.

Default and generic local system accounts are disabled or renamed during the system setup process (see IT4912-Secure Configuration Management). Generic or shared Active Directory accounts, except those authorized by the CIO/CISO, are prohibited.

Guest accounts created for third-party support must remain disabled until needed and password reset after each use.

Access to file and print services, server resources, software, and VPN access etc. must be requested through a separate helpdesk ticket. Access to these services and resources are controlled with Active Directory groups with each being labeled with its purpose and owner. Owner permission is required to be documented in a helpdesk ticket before user accounts can be added to any security group.

Remote access to the UTSI network requires VPN access with MFA for login.

All changes to automated processes, server setups, and network appliances are to be approved by campus CIO and documented in helpdesk tickets.

Exceptions

Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

Related Policies

- [IT0001 – General Statement on Information Technology Policy](#)
- [IT0003 – Information Technology Security Program Strategy](#)
- [IT0004 – Information Technology Risk Management](#)



SPACE INSTITUTE

UT Space Institute IT Procedure: Account and Credential Management	
Version: 1	Effective Date: 10/01/2025

- [IT0005 – Data Categorization](#)
- [IT0014 – Information Technology Security Awareness Training Management](#)
- [IT0017 – Information Technology Incident Response Management](#)
- [IT0102 – Information Technology Asset Management](#)
- [IT0311 – Information Technology Data Access, Management, and Recovery](#)
- [HR0580 – Code of Conduct](#)
- [IT0002 – Acceptable Use of Information Technology Resources](#)
- [IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing](#)
- [IT1516 – Information Technology Service Provider Management and Application Software Security Management](#)
- [IT4912 – Information Technology Secure Configuration Management](#)
- [IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy](#)