THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0506 - Information Technology Account and Credential Management	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to establish User Account lifecycle management and inventory processes of University accounts used for access to University Information Technology Resources. This will include guidelines for credential creation and issuance, account and credential usage, modifying access, and account termination.

II. Account and Credential Management Policy

The Central IT Department must communicate the requirements and processes for account and credential management to the campus community annually to engage campus communities and individuals in the shared responsibility of secure account management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

This policy applies to both University-owned User accounts and any User account not managed by the University but used for University IT services, such as IT Service Provider accounts. User accounts include the following:

- Standard User accounts: These are the most common type of User account associated with your primary affiliation, such as being a student or Employee with the University and are used for everyday tasks like running software or personalizing your desktop.
- Privileged accounts: These accounts have full access to all settings on a System and are used for making changes to System settings or managing other accounts.
- Guest accounts: These accounts are used by temporary or intermittent Users of a System or Asset. They allow Users to log in without making changes to the System's settings or accessing other Users' Asset, System, or Data.
- System accounts: These accounts are used for storing System files and processes.
- Root accounts: These accounts are used for System administration.
- Database accounts: These accounts are used for database access.
- Service accounts: A special type of account used to enable automated processes or applications to interact with various IT services or Systems without requiring user intervention.

1. The Data Owner must provide approval on the authorization and access of the University Data under their management.

2. The Data Steward, who is the person identified by the Data Owner to act, and to approve or deny access to Data, must be consulted on the authorization and access of the University Data under their management.

3. Onboarding

a. The Central IT Department will create a process for modifying access, permissions, and roles to User accounts. Newly created accounts must be represented within this process.

b. Students employed by the University in a temporary, part-time capacity, including Graduate Assistants, are to receive a separate account that is to be used for work activities only.

c. The permissions granting process must enforce the principle of least privilege that includes separation of incompatible duties.

d. Unnecessary default or generic accounts must be changed before a new System is deployed into the University's Resources.

e. Employees with administrative control within business-critical Systems or who can assign or revoke rights, roles and privileges in said Systems must have a background check performed every four years.

4. Account Creation

a. The Central IT Department will create a process for:

i. Creating accounts and assigning privileges.

ii. Ensuring that administrator privileges are only provided to administrative accounts.

iii. Assigning privileged accounts that are only used for appropriate installation and maintenance tasks, not for daily use, and that are unique and assigned to a specific individual, unless technically constrained by a System or application.

c. The Central IT Department will create a process to maintain an account inventory of the University's accounts. At a minimum the account inventory must contain the following information for each account:

i. Person's name.

ii. Account name.

iii. Date of account creation and disablement.

iv. Business unit.

v. Account status (i.e., enabled, disabled).

d. The Central IT Department will create a process to validate all centrally managed accounts that are enabled within the inventory are authorized, at a minimum annually.

5. Credential Creation and Issuance

a. All passwords for a University User account must be unique to the individual.

b. Passwords created by Users for University User accounts, because they are unique, must not also be used for the User's own personal accounts.

c. Passwords must not be shared by Users.

6. Account and Credential Usage

a. The Central IT Department will create a process for enforcing User authentication requirements and password management to maintain account access security.

b. All Users must use multifactor authentication to access externally facing applications.

c. All Users must use multifactor authentication to access applications hosted by an IT service provider, where supported.

d. All remote Users must use multifactor authentication to access the University's internal Systems and applications.

e. Multifactor authentication is required for all privileged accounts on all the University's Systems, whether managed on-site or through an IT Service Provider.

f. All default User passwords must be changed at the first login.

g. Accessing a System that contains Protected University Data without multifactor authentication must be approved as an exception by the POA and will only be considered where access is required.

h. Passwords created for use with multifactor authentication must be at a minimum of 16 characters long and meet complexity requirements as defined by the Central IT Department.

i. Passwords must be changed every 180 days for User accounts that do not use multifactor authentication. Passwords must be changed immediately for a known or potential User account compromise.

j. Passwords that are required by a compliance or state or federal requirement to be changed under a specific timeframe must be changed according to the requirement.

7. Modify Access

a. The Central IT Department will create a process for:

i. Modifying account access to maintain account security including managing role-based access.

ii. All centrally managed user accounts that have not been accessed within 45 days of creation to be disabled.

iii. All University-owned and managed accounts of individuals on extended leave, as defined by Human Resources, to be disabled.

b. The account creation and account termination process must include the ability to change a User's status.

8. Account Termination

a. The Central IT Department will create a process(es) for:

i. Revoking account access that includes both voluntary and involuntary termination of access when a User no longer requires access as a part of their role at the University.

ii. When a User's University employment is terminated, account termination must occur within 24 hours of the termination. All User credentials must be revoked immediately upon Employee separation from the University.

iii. Managing student terminations, including both voluntary and involuntary.

iv. The campus community that manages retiree terminations.

v. Guests, friends, and contractors, with password self-service mechanisms that does not allow them to re-enable their own account.

Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

1. The Central IT Department will create a process to establish and maintain an inventory of service accounts (IG2).

a. The inventory, at a minimum, must contain department owner, review date, and purpose.

b. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly.

2. The Central IT Department will create a process(es) with guidance for:

a. The campus community to centralize account management through a directory or identity service (IG2).

b. Establishing and maintaining an inventory of the University's authentication and authorization Systems, including those hosted on-site or at a remote IT Service Provider (IG2).

c. Reviewing and updating the inventory, at a minimum, annually, or more frequently.

d. Campus community to control all the University's Assets through a directory service or single sign on (SSO) provider, where supported (IG2).

e. Defining and maintaining role-based access control, through determining and documenting the access rights necessary for each role within the University to successfully carry out its assigned duties (IG3).

f. Performing access control reviews of the University's Assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually.

III. Exceptions

The University's Chief Information Officer is authorized to grant exceptions to the University's Information Technology Policies. Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

SECTION 2. Reason for the Policy

This policy establishes the requirements for information technology account and credential management as described in CIS Control 5 (Account Management) and CIS Control 6 (Access Control Management) for the University of Tennessee in support of System-wide Policy: IT0001 – General Statement on Information Technology Policy. All Users must familiarize themselves with System-wide Policy: IT0001.

SECTION 3. Scope and Application

This policy applies to all Users of IT Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

SECTION 4. Procedures

Each campus/institute will adopt procedures related to this policy.

SECTION 5. Definitions

See IT0001 – General Statement on Information Technology Policy for definitions of terms.

SECTION 6. Penalties/Disciplinary Action for Non-Compliance

Any violation of this policy may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct (HR0580 – Code of Conduct) in the Human Resources Policy and Procedures.

The University may temporarily or permanently remove access to its information technology Resources if an individual violates this policy.

SECTION 7. Responsible Official & Additional Contacts

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	System Chief Information Officer and System Chief Information Security Officer	(865) 974-4810 or (865) 974-0637	cio@tennessee.edu or iso@tennessee.edu
Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

[Text Wrapping Break]_____

SECTION 8. Policy History

Revision 1:

_____

SECTION 9. Related Policies/Guidance Documents

A. University Policies

a. IT0001 – General Statement on Information Technology Policy

b. IT0002 – Acceptable Use of Information Technology Resources

c. IT0003 – Information Technology Security Program Strategy

d. IT0004 – Information Technology Risk Management

e. IT0005 – Data Categorization

f. IT0014 – Security Awareness Training Management

g. IT0017 – Information Technology Incident Response Management

h. IT0102 – Information Technology Asset Management

i. IT0311 – Information Technology Data Access, Management, and Recovery

j. IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing

k. IT1516 – Information Technology Service Provider Management Application Software Security Management

l. IT4912 – Information Technology Secure Configuration Management

m. IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense

B. Center for Internet Security Critical Security Controls Navigator

https://www.cisecurity.org/controls/cis-controls-navigator/

_____