UNT SYSTEM™
Information Technology

INFORMATION TECHNOLOGY STANDARD

IDENTITY AND ACCESS MANAGEMENT

Purpose and Benefits

Identification and Access Management (IAM) is essential to ensure that the right individuals have access to the appropriate resources at the right times for the right reasons. These standards are critical for safeguarding sensitive data and systems from unauthorized access and potential security breaches. The IAM standard will help the UNT System Enterprise manage user identities and their access to resources efficiently and securely and ensure all users are properly authenticated, authorized, and audited.

Authority and Requirements

Identification and Authentication section of the UNT System Information Security Handbook (Page 40-41). The Identification and Authentication requirements of the UNT System Information Security Handbook satisfy the control requirements of IA-Identification and Authentication in the Texas Department of Information Resources Security Controls Standards Catalog.

Definitions

Enterprise Accounts. "Enterprise Accounts" means accounts that grant university-wide access to information resources. They are provisioned, maintained, and deprovisioned by established standard processes overseen by the UNT System Information Technology Identity Management team.

Information Security Program. "Information Security Program" means the policies, Information Security Handbook, control catalog, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions. The Information Security Program shall comply with applicable federal and state laws related to information resources and information security, including but not limited to 1 Texas Administrative Code §202 and the State of Texas Department of Information Resources Security Controls Standards Catalog.

Local accounts. "Local Accounts" means accounts created within applications and operating systems when they are required for functionality or when enterprise accounts cannot be used.

Privileged Accounts. "Privileged Accounts" means accounts with extra privileges related to the management of a device or application.

Service Accounts. "Service Accounts" mean a digital identity used by a software application or service to interact with software applications or operating systems. Service accounts are used when it is necessary for systems or applications to authenticate to other systems or applications without any association to a person. These accounts should be created sparingly, and documentation of their purpose should be kept. Service accounts may not be used by people to authenticate aside from initial testing. Service accounts with elevated privileges must be closely monitored for abuse.

General Implementation

Access to UNT System Enterprise technology assets will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. Requests for user accounts, additions, changes, and deletions of access to UNT System Enterprise endpoints, networks, systems, data, and/or facilities must be formally requested via the ServiceNow ticketing system and must be authorized by the applicable business owner(s) prior to the provisioning or change of access. All request and approval activities must be formally documented with valid business justification. All non-employee requests for access (including contractors, service providers, vendors, and third parties) must adhere to the access request and authorization requirements defined within this Standard.

Governance

- Creation of an identity should only occur when necessary for a business process.
- Service entitlements should only be granted as needed to support the individual's work within the organization.
- Identities should be granted only minimal service entitlements upon creation (self-service).
- Identities should return to a self-service state upon role change. Any entitlements for a new role should be added based on need.
- Upon separation from the organization, an identity must be returned to a self-service state.
- Service entitlements must include a business owner, business justification, and an explicitly defined life-cycle.
- Identities must be disabled if there is no relationship to the organization or business need.
- Identities must be disabled if they are not used for a defined period of time.
- Students and Employees must not share an identity or service entitlements.
- The strongest reasonable method of authentication must be used (e.g., multi-factor authentication, passkeys, etc.)
- Activity related to identities such as creation, deletion, changes in entitlements, disablement, password or MFA authentication change, session activity must be logged and retained.
- Custodians of the canonical source of truth for identity data must implement standards to ensure quality, completeness, and accuracy of the data.
- All procedures involved with the management of identities, or the life-cycle of identities must be documented and periodically reviewed.

Provisioning

All persons associated with the UNT System shall have a unique digital identifier that is never revoked. This unique identifier is the Euid. The authoritative source for pairing an identity to their Euid is the identity management system UNT System Information Technology Identity Management team.

Recommendations for account provisioning:

1. Use enterprise authentication over local authentication whenever possible and reasonable.
2. Departmental/Shared accounts to access data may not be created unless approved through the exception process.

3. Ensure privileged access is granted only to appropriate accounts with need for such access. Ideally, passwords for accounts with privileged should be stored in a privileged access management system.
4. Ensure that non-privileged accounts do not have access to privileged functions and audit any use of privilege.
5. Ensure that any system or application that authenticates or authorizes an account log both successful and failed activities to a standard location and format.
6. Ensure that passwords for service accounts are stored in a secure location and available to individuals responsible for managing those accounts.

Authentication

All accounts must require authentication before use. Unauthenticated access may be used only with data classified as Public, in accordance with the UNT System data classification.

Authentication credentials should be set by the account holder at the time of account creation or temporary passwords for local accounts may be used so long as the temporary password is immediately changed upon login. Temporary passwords must conform to the password requirements in the UNT System Information Security Handbook.

Any application or system, whether on premises or in the cloud, should use enterprise authentication services instead of local accounts and passwords whenever possible and reasonable.

Passwords must be encrypted in transit over any network and encrypted when stored.

Authorization

Authorizations are the implicit or explicit permission to use a resource associated with an account. Once the use of an account is authenticated, a system or resource may determine if the person or software requesting access is authorized to use it. The management and maintenance of authorizations is shared responsibility of UNT System IT and local system and application administrators.

System and Application-Level Authorizations

In some cases, accounts may need to be defined explicitly in an application or system. When an account is defined in a local system or application, some authorizations may be implicitly granted, such as the ability to use some or all functions of the application or system.

Privileged Authorizations

Certain authorizations grant access to administer a system or application and/or access to see data that is created or maintained by others. Privileged access should be granted based on the specific person's job duties, not the duties of the person's organizational unit. Use of privilege should be recorded by the system or application.

1. Privileged access may be granted permanently only if that specific person's job duties routinely require that level of access, otherwise, the access must be temporary.

2. All authorization requests must be documented, including the nature of the request, the period for which it has been granted, all related approvals that were obtained, and the names of the approvers.

Access Management

Information System/Application Owners and System Administrators must control and manage access in accordance with the UNT System Information Security Handbook and Access Control Standard.

Auditing

Ensure that any account or authorization created, deleted, removed, or changed is audited and available for review. This log would contain proof of approvals for the creation, deletion, removal, or change and the system and any system or application-level log that the account or authorization was modified, if such can be logged.

Information System/Application Owners and System Administrators must conduct routine audits of account and authorization activity to ensure that only authorized use is occurring and maintain audit documentation accordingly.

Cybersecurity and IT Compliance and Internal Audit may request evidence to confirm audits of the accounts and authorizations of any university information system are being performed. Audit documentation must show the following:

1. There is a request for every account with elevated privilege, shared account, or service/process account;
2. The request was approved by all applicable parties;
3. The request is compliant with applicable regulation, policy, and best practice;
4. The granted privileges were required for the approved administrative use;
5. Requests for temporary privileges are revoked on the agreed expiration date;
6. Every active account is held by a person with an active affiliation at the institution; and
7. The account holder's job function still requires the granted privilege.

Deprovisioning

Access managed through Enterprise Accounts should terminate upon triggered processes supported by Human Resources. System Administrators should ensure Active Directory accounts are disabled for their area of responsibility.

When access is managed locally, the system or application must account for termination of access when an individual's affiliation changes. Some individuals will retain access to their account based on affiliation even though a role may have ended (e.g. alumni).

Upon transfer from one department to another the System Administrator and Information System/Application owner should ensure that access is deprovisioned to ensure only access necessary for the employee to perform current business functions under their new role are preserved, all others require disabling.

Active Directory accounts will be disabled eighteen (18) months following cessation of employment, end of contract term, graduation or discontinuation of enrollment.

Local Implementation

Only enterprise accounts for employees will automatically generate Active Directory accounts for each employee, which will appear in the designated Active Directory Organizational Unit ("OU"). System Administrators will ensure the Active Directory account exists in the correct institution OU prior to granting access to groups and local account access. System Administrators must manually create Active Directory accounts for non-employees and configure with a predetermined expiration date.

System Administrators will provision user permission to groups as needed based on requests submitted by the hiring manager, supervisor, or other authorizing official. Requests should be submitted through the ServiceNow ticketing system for all access permissions, including but not limited to: Email and fileshares. System Administrators must limit access for non-employees to only what is necessary to fulfill contractual obligations.

System Administrators and Information Resource/Application Owners must provision local accounts for employees and non-employees based on business need only and in accordance with the Principle of Least Privilege.

System Administrators should regularly check Role Removal Listing reports for employees who are terminated to ensure Active Directory and local accounts are deprovisioned immediately.

Active Directory accounts for employees transferring within departments should be placed in the proper OU. Accounts for employees transferring to a separate department should be placed in Active Directory Lost Users OU for the new department System Administrator to place in the correct OU.

Exceptions and Compensating Controls

Exceptions to Information Security policies and this standard may be approved by the Chief Information Security Officer or their delegate when accompanied with sufficient justification and compensating controls, in accordance with the UNT System Information Security Program.

The Chief Information Security Officer may revoke an exception at any time.

References and Notes

DIR Security Controls Standards Catalog
UNT System Information Security Regulation 06.1000

UNT System Information Security Handbook
UNT System Access Control Standard

Approvals and Revision History

	Name	Title	Date
Authored By:	Christine Sikes	Director of IT Governance, Risk, & Compliance	6/24/2024
Approved By:	Rich Anderson	Chief Information Security Officer	7/3/2024

Date	Approved By	Version	Notes
7/3/2024	Rich Anderson	1.0	New Identity and Access Management Standard
9/12/2024	Rich Anderson	1.1	Added Language for Governance