ACCESS CONTROL

1. Purpose

Employees of the UNT System (System) must adhere to all regulations, policies, and standards related to access control. Access to UNT System information and information resources will be granted and monitored consistent with the principle of least privilege.

Information processing systems owned by or operated on behalf of UNT System should have role-based access control that ensures legitimate users and/or systems have access to data resources that they are explicitly authorized to use.

2. Scope

This standard applies to all employees of the System and establishes access control requirements for all System information resources that store and/or process System data.

3. Definitions

3.1. Authorizing Officials. Individuals responsible for decision making on behalf of a UNT System department or division.

3.2. Information Steward. Delegate of the Information Owner responsible for granting and revoking access to institutional information and granting and revoking permission for the use of institutional information.

3.3. Information Owner. Individual with operational authority for specified information and who is responsible for authorizing the controls for generation, collection, processing, access, dissemination, and disposal of that information.

3.4. Information System/Application Owners. Individuals responsible for the development, procurement, integration, modification, operation and maintenance, implementation of the Information Owner-defined controls, and/or final disposition of an information system.

3.5. Principle of Least Privilege. The security principle that access should be enabled and managed so that each user is granted the minimum system resources and authorizations needed to perform their business function.

3.6. Privileged Access. An escalated level of resource access that allows changes to information systems and can affect the confidentiality, integrity, or availability of information or information resources. Privileged access is granted to users that are responsible for providing information resource administrative services such as system maintenance, data management, and user support.

3.7. Service Account. Non-human privileged account used to run applications, automated services, and various background processes.

3.8. UNT System Information Security Program. The UNT System Information Security Program includes the policies, handbooks, controls catalogs, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions.

3.9. User. An individual or automated application authorized to access information or information resources in accordance with the Information Owner-defined controls and access rules.

4. Responsibilities

4.1. Access Control Procedures

4.1.1. Information System/Application Owners must create and maintain access control procedures for their information resources that comply with the UNT System Information Security Program.

4.1.2. Information System/Application Owners must update procedures at least annually and as needed to address changes to the information resource or supporting processes.

4.1.2.1. Access control procedures should:

4.1.2.1.1. Define and document the types of accounts allowed within the information resource;

4.1.2.1.2. Define the attributes for each type of account;

4.1.2.1.3. Identify account managers and privileged access users; and

4.1.2.1.4. Include requirements for access authorizations.

4.1.3. Access control procedures must include a process for changing shared or group account credentials when users are removed from the group.

4.2. User Access Creation

4.2.1. Information System/Application Owners must grant access based on the Principle of Least Privilege.

4.2.2. Information System/Application Owners must consider separation of duties when creating user access.

4.2.3. Information System/Application Owners should avoid generating shared or group accounts.

4.2.4. Information System/Application Owners must collect and maintain access authorizations prior to granting users access to an information resource.

4.2.4.1. Access authorizations for users must include:

4.2.4.1.1. Business justification for the account; and

4.2.4.1.2. Approval from Information System/Application Owners, supervisors, and information owners or information stewards, as applicable.

4.2.4.2. Access authorizations for privileged access users (including service accounts) must include:

4.2.4.2.1. Details of the privileged access granted;

4.2.4.2.2. Business justification of the privileged access granted;

4.2.4.2.3. Approval from Information System/Application Owners, supervisors, and information owners and information stewards, as applicable; and

4.2.4.2.4. Approximate length of privileged access.

4.2.4.3. Information System/Application Owners must verify access authorizations biennially for users and annually for privileged access users.

4.3. Monitoring User Access

4.3.1. Information System/Application Owners must monitor user access to ensure validity and currency.

4.3.2. Information System/Application Owners must conduct reviews of user access at the following intervals:

4.3.2.1. Annual reviews of general users; and

4.3.2.2. Quarterly reviews of privileged users and service accounts.

4.3.3. Information System/Application Owners must conduct quarterly access reviews for all users of high-risk information resources.

4.3.4. Supervisors must maintain employee access authorizations for information resources to ensure appropriate continued use of information resources.

4.4. Modifying User Access

4.4.1. Supervisors must notify Information System/Application Owners within three business days when changes to an employee's role occurs.

4.4.2. Information System/Application Owners must modify user access based on changes to business justifications documented in access authorizations and as appropriate for changes in a user's role.

4.5. Disabling User Access

4.5.1. Supervisors and other authorizing officials must notify Information System/Application Owners within three business days when employees are terminated or transferred, and/or when usage or business need changes for a user or service account.

4.5.2. Information System/Application Owners must disable access upon a user's termination, transfer, or when a change to business occurs where access is no longer needed.

4.5.3. Information System/Application Owners must immediately revoke user access when directed by authorizing officials in the event of a violation of security policy, procedure, or mandate.

DOCUMENT VERSION LOG			
Version	**Approved By**	**Date**	**Description**
1	Rich Anderson	10/19/2023	New Access Control Standard