User Access Management Policy

Document Number: ITS-0029 **Date Published(sys):** 12/11/2024

General Description

Policy Summary:

This policy governs the management of use access to Trinity University's Information Resources. It ensures that computer and network accounts are created, controlled, and monitored to support accountability and protect the University's information security program.

Purpose:

The User Access Management Policy aims to establish a framework for managing access to Trinity University's Information Resources in a secure, accountable, and efficient manner. By creating, controlling, and monitoring user accounts, the policy ensures that access is granted appropriately, aligns with job responsibilities, and protects institutional data's confidentiality, integrity, and availability. This policy supports the University's broader information security program and safeguards its digital assets against unauthorized access and misuse.

Scope:

This policy applies to all individuals who require access to Trinity University's Information Resources, including but not limited to faculty, staff, students, contractors, consultants, vendors, and any other authorized users. It encompasses all systems, networks, applications, and data owned, managed, or maintained by the University. The policy governs the creation, management, monitoring, and termination of user accounts and the processes for granting, modifying, and revoking access privileges to ensure the security and accountability of the University's digital assets.

Exceptions:

Specific Trinity University systems may need to be exempted from the User Access Management Policy in some instances due to technical limitations or requirements stemming from third-party contractual obligations. Any exceptions must be thoroughly documented, including the rationale and scope of the exemption, and submitted for review and approval through the Trinity

University Exceptions Management Process. This ensures all exceptions are appropriately evaluated and aligned with the University's security framework.

Responsible Department:

Information Technology Services

Policy Content

Policy

The User Access Management Policy establishes the following key processes to ensure secure and appropriate access to Trinity University's Information Resources:

1. **Account Lifecycle Management**:
    - Procedures for requesting, approving, issuing, and closing user accounts are clearly defined and enforced.
2. **Access Privilege Assignment**:
    - Access privileges are assigned based on the Principle of Least Privilege (PoLP). This information security concept limits user's access to only the data, resources, and applications necessary to perform their job responsibilities.
3. **Periodic Access Reviews**: The Information Technology Services (ITS) Department collaborates with department managers to conduct periodic user reviews. These reviews must be performed at least annually to ensure access privileges remain necessary and appropriate for each user's job roles and responsibilities. ITS must document and approve any required changes to access as part of the review process.

Process Overview

Access Privileges and Security Principles

Security Principles for Access

- **Business Needs**: Access is granted based on the requirements of a user's role and responsibilities within the University.
- **Least Privilege**: Users are assigned only the minimum access necessary to perform their duties effectively.
- **Data Minimization:** - Access to data is restricted to the specific information essential for fulfilling the user's role.

Formal Access Request

- All account and permission requests, including those for privileged and limited user accounts, must be submitted using a documented access request process.
- This includes requests for initial access, role changes, duty shifts, and account deactivation due to termination or suspension.

Authentication Standards:

- Alternative authentication mechanisms without unique ID and passwords require formal approval from Information Technology Services before implementation.
- Multifactor Authentication (MFA) must be implemented wherever technically feasible.

Remote Access Requirements:

- MFA is mandatory for all remote connections to University systems and services.
- Remote access must be monitored, with alerts enabled for unusual activity.

Account Deactivation:

- Access rights must be promptly disabled or revoked when a user is terminated or no longer has a valid reason for access.

Annual Access Review:

- User accounts and associated access rights must be reviewed annually to ensure they remain necessary and appropriate.

Access Management Oversight:

- The Information Technology Services Department (ITS) oversees the management of access to all applications and services.
- Exceptions to this policy require documents, review, and approval by the University's Chief Information Security Officer (CISO), Chief Information Officer (CIO), or their designee.

Continuous Monitoring:

- All account access is subject to continuous monitoring and periodic review to detect and mitigate unauthorized or inappropriate use.

Vendor and Contractor Access Management

Trinity University engages vendors and contractors to support critical business processes, manage systems and applications, and perform tasks on behalf of the institution. To ensure the security and integrity of University systems, the following requirements apply:

Confidentiality Standards

- Before access is granted, vendors and contractors must sign a Non-Disclosure Agreement (NDA) or have appropriate confidentiality safeguards in place, as approved by the Office of Risk Management.

Access Management

- The ITS department will maintain an up-to-date list of all vendors and contractors with access to University systems.
- User accounts will not be created without a documented service expiration date. When access is no longer required, accounts will be disabled and deleted per the University's Electronic Retention Policy.

Security Requirements

- Vendors and contractors must use Multi-Factor Authentication to access University systems.
- Their activities and access privileges will be continuously monitored and formally reviewed annually by the ITS department.

Compliance

- Vendors and contractors must comply with all Trinity University policies, procedures, and applicable laws and regulations. Non-compliance may result in the immediate revocation of access and termination of the contractual relationship.

These measures ensure vendor and contractor access aligns with Trinity University's commitment to safeguarding institutional data and resources.

Enforcement

Compliance with the User Access Management Policy is mandatory for all users, including faculty, staff, students, contractors, and vendors. Violations of this policy may result in disciplinary action, including revocation of access privileges, termination of employment or contracts, or referral to appropriate administrative or legal authorities.

The Information Technology Services (ITS) department monitors adherence to this policy and reports any violations to the Chief Information Security Officer (CISO) or designee. Instances of non-compliance involving contractors or vendors will be escalated to the Office of Risk Management and may result in immediate access and contractual agreements termination.

Performance Evaluation

Consequences of Policy Violation:

Performance Evaluation: To ensure adherence to this Policy and protect the integrity of University resources, Trinity University reserves the right to monitor the network and attached computers. In addition, Trinity University shall have the authority to examine files, logs, and account information and to test passwords to protect the security of the University's information, network, computing resources, and its users.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Computer Account	**Purpose**: A computer account is specific to a single computer or device. It allows a user to log in and access resources stored locally on that machine. **Characteristics**: • Tied to the specific device (e.g., desktop or laptop). • May include local user profiles, personal settings, and locally stored data. • Permissions and access are limited to that particular computer. • Often used for standalone devices or when a user doesn't need access to networked resources.
Network	**Purpose**: A network account allows users to log in and access shared resources

Term:	Definition:
Account	across a network, such as files, applications, printers, and services. **Characteristics**: • Managed centrally (e.g., through Active Directory or a similar system). • Enables roaming profiles, meaning a user can log in from different devices on the network and retain access to their settings and data. • Provides access to shared drives, intranet services, email, and other networked resources. • Typically more secure, with permissions and policies applied by the organization

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v.1	12/11/2024 9:45 AM	Pamela Mota

Vice President Approval:

Name:	Title:
Mark Detterick	Vice President for Finance and Administration