# 700.5 Account Lifecycle and Access Management Policy

Policy Title: Account Lifecycle and Access Management Policy
Policy Number: 700.5
Responsible Office: Information Technology Services
Approval Authority: Administrative Council; President's Cabinet (Final Approval)
Applies To: All employees, faculty, staff, students, student workers, contractors, vendors, retirees, guests, and any individuals with accounts authenticated through College identity systems
Alignment: FERPA; GLBA; DMCA/HEOA; NIST SP 800-53 Rev. 5; NIST SP 800-63 Digital Identity Guidelines
Effective Date: May 2026
Current Version: 1.0.0
Next Scheduled Review: January 2027

## I. Policy Overview and Purpose

This policy establishes the institutional governance framework for the creation, modification, suspension, retention, and termination of identity accounts used to access Northeast Mississippi Community College (NEMCC) systems and institutional data.

Effective identity lifecycle management protects institutional systems, prevents unauthorized access, ensures timely removal of access when roles change or individuals separate from the institution, and supports compliance with FERPA, GLBA, and institutional data governance requirements.

Operational lifecycle procedures, automation processes, and retention timelines are defined in the Identity Lifecycle Standard (700.5.1).

## II. Scope

This policy applies to all institutional identity accounts, including:

- Employee accounts
- Student accounts
- Student worker accounts
- Contractor and vendor accounts
- Guest accounts
- Privileged or administrative accounts
- Service accounts
- Shared mailboxes
- Legacy Identity Accounts

This policy applies to all systems that authenticate through College identity providers or otherwise grant access to institutional systems or institutional data.

## III. Definitions

**Account Suspension (AS) —** A temporary administrative suspension applied to an account when continued system access presents institutional risk. When applied, authentication and provisioning actions are blocked until formally released.

**Authorized User** — Any individual granted access to College systems or institutional data based on role, employment status, academic status, or contractual relationship.

**Deceased Indicator** — A permanent institutional status applied to an account following an employee death. This indicator prevents any reactivation or modification of the account.

**Identity Account** — The core authentication identity used to access institutional systems and services.

**Privileged Account** — An account with elevated permissions or administrative capabilities requiring enhanced security protections.

**Provisioning** — Creation of an identity account and assignment of initial access permissions.

**Deprovisioning** — Removal of access rights, system permissions, and authentication capability when access is no longer authorized.

**Role-Based Access Control (RBAC)** — A method of managing system permissions using predefined role definitions approved by Data Owners.

**Service Account** — A non-person account used by systems or automated processes.

## IV. Roles and Responsibilities

### Human Resources

- Maintains authoritative employment records
- Notifies ITS of employment changes and separations

### Supervisors and Division Heads

- Request appropriate access for employees
- Notify ITS when roles change or employment ends
- Participate in periodic access reviews

### Information Technology Services (ITS)

- Provisions, modifies, suspends, and terminates identity accounts
- Implements lifecycle automation and authentication controls
- Maintains identity infrastructure and security monitoring
- Conducts periodic access reviews and audits

**Data Owners**

- Approve role-based access definitions
- Ensure access aligns with business necessity and least privilege

**Users**

- Use only assigned accounts
- Protect credentials
- Follow Acceptable Use and Authentication policies

## V. Identity Lifecycle Governance

Identity accounts must follow a defined lifecycle consisting of:

- Provisioning
- Modification
- Suspension
- Termination

Lifecycle events must originate from authoritative institutional records such as:

- Human Resources employment records
- Admissions records
- Enrollment status
- Institutional administrative determinations

Provisioning and deprovisioning must follow predefined role-based access models approved by Data Owners in accordance with the Data Governance Policy (735.0).

Operational procedures, lifecycle triggers, automation mechanisms, and retention timelines are defined in the **Identity Lifecycle Standard (700.5.1)**.

## VI. Account Suspension Authority

ITS may suspend accounts immediately when necessary to:

- mitigate security risk
- respond to suspected compromise
- enforce institutional policy
- support investigations

- address urgent termination events

When required, an **Account Suspension (AS)** hold may be applied to prevent authentication and automated lifecycle processing.

Release of an AS hold requires written authorization from:

- the Director of Human Resources for employee accounts, or
- the Vice President of Student Services for student accounts.

## VII. Access Reviews and Recertification

ITS conducts periodic access reviews for systems and privileged roles.

Supervisors and Data Owners must verify that access permissions remain appropriate and aligned with job duties.

Access must be removed immediately upon role change or separation.

## VIII. Special Account Categories

Special account categories include:

- privileged accounts
- service accounts
- shared mailboxes
- legacy identity accounts

These accounts require enhanced security controls, including ownership assignment, logging, and compliance with the Password and Authentication Policy (700.4).

Operational management of these account types is defined in the identity Lifecycle Standard (700.2.1).

## IX. Exceptions

- Exceptions to lifecycle requirements must follow the Standard Exceptions Process defined in the Data Governance Policy (735.0).

Exceptions must:

- document the operational need
- identify risks
- define compensating controls
- include an expiration date

Exceptions require approval from:

- the appropriate Data Owner
- the Director of Information Technology Services

## X. Enforcement

Violations of this policy may result in:

- removal of system access
- suspension or revocation of accounts
- mandatory retraining
- disciplinary action
- referral to Human Resources or Student Services
- legal or regulatory reporting when required

ITS may take immediate technical action to protect institutional systems and institutional data.

## XI. Revisions

This policy will undergo annual review by Information Technology Services.

Operational lifecycle procedures and timelines may be updated through the Identity Lifecycle Standard (700.5.1) provided those changes remain consistent with the governance requirements of this policy.

| Version | Date | Description | Approved By |
|---|---|---|---|
| 1.0.0 | Jan 2026 | Initial release of Account Lifecycle and Access Management Policy | President's Cabinet |