735.0 Data Governance and Security Oversight Policy

Policy Title: Data Governance and Security Oversight Policy
Policy Number: 735.0
Responsible Office: Information Technology Services
Approval Authority: Administrative Council; President's Cabinet (Final Approval)
Applies To: All employees, faculty, staff, student workers, contractors, vendors, and authorized users who create, store, manage, or access institutional data.
Alignment: FERPA; GLBA; recognized cybersecurity and governance frameworks (as updated)
Effective Date: May 2026
Current Version: 1.0.0
Supersedes: None
Next Scheduled Review: January 2027

I. Policy Overview and Purpose

This policy establishes the institutional framework for managing, classifying, accessing, and protecting institutional data at Northeast Mississippi Community College (NEMCC). It defines data ownership, stewardship, system governance, access approvals, access review requirements, and decision-making authority across enterprise systems including the institutional Enterprise Resource Planning (ERP) system, learning management systems, reporting and document management platforms, workflow and automation systems, collaboration environments, and all other current or future systems that store or process institutional data.

This policy operates under the authority delegated by the President in accordance with NEMCC Board Policy and establishes the governance, enforcement, and exceptions framework for all policies and standards within the ITS Policy Suite unless a policy explicitly states otherwise.

II. Scope

This policy applies to all current and future user, systems, applications, platforms, integrations, APIs, and connected services that store, process, transmit, or provide access to Institutional Data, whether hosted on-premises or in the cloud, regardless of whether the system is explicitly named in this policy.

III. Definitions

Account Suspension (AS) — Account Suspension (AS) is an administrative risk-removal mechanism used to immediately restrict authentication and system access when continued access presents institutional risk. AS governance, authorization authority, release authority, and scope are established exclusively within this policy and apply to all ITS policies and standards. AS is not progressive discipline and does not constitute a disciplinary determination.

Authoritative Data Source — The officially designated system or dataset where final, correct institutional data is maintained for a particular domain.

Data Owners — Functional leaders responsible for oversight and classification for institutional data in their domain.

Data Stewards — Individuals responsible for daily management, integrity, and workflow execution within systems that store institutional data.

Deceased Indicator —A permanent institutional status applied to an account in the event of an employee death. The Deceased Indicator prevents inadvertent activation of an account and triggers deactivation of an active account.

Institutional Data — Any data created, received, processed, stored, or transmitted by NEMCC in support of its academic, administrative, operational, financial, or student-services mission.

Technical Stewards (ITS) — System administrators and database administrators responsible for implementing technical controls, provisioning access, deprovisioning accounts, monitoring, logging, and enforcing security configurations.

Users — Any individual who interacts with institutional data as part of their academic, administrative, instructional, or operational duties.

IV. Data Governance Structure

A. Data Owners

The following roles are designated as Institutional Data Owners:

- Director of Admissions – Admissions and Recruitment Data Owner
- Director of Financial Aid – Financial Aid and GLBA-regulated Data Owner
- Distance Learning Coordinator – Learning Management Systems
- Vice President of Finance – Finance, Accounting, Business Office Data Owner
- Vice President of Instruction – Academic, Instructional, Student Services Data Owner

Responsibilities:

- Determine data classification levels within their assigned domain in accordance with Policy 730.2.
- Approve and oversee role-based access controls within their domain, ensuring alignment with documented job duties and least privilege principles.
- Participate in periodic access reviews and role validation processes to confirm continued business necessity.
- Coordinate with Information Technology Services (ITS) to implement appropriate access controls and technical safeguards.

Clarification of Enforcement Authority

Data Owners are responsible for data governance, including classification, access approval, and oversight within their assigned domains. Data Owners do not perform technical enforcement or disciplinary enforcement. Enforcement actions—including access restriction, account suspension, investigation, and disciplinary measures—are executed by Information Technology Services, supervisors, Human Resources, Student Services, or College administration in accordance with applicable policies.

B. Data Stewards

Data Stewards include designated operational personnel in each functional area who manage the daily integrity of institutional data.

NEMCC Data Stewards include:

- Admissions staff
- Financial Aid specialists
- Business Office accountants and finance personnel
- Faculty, Academic Advisors, and Student Success Center staff
- Academic division support staff
- LMS Administrators and Distance Learning support personnel
- Institutional Research staff
- ITS technical stewards (Banner, LMS, Evisions, Document Management)

Responsibilities:

- Maintain accuracy, integrity, and timeliness of data
- Ensure data is handled in accordance with its classification
- Report issues, errors, or incidents to Data Owners and ITS

C. Information Technology Services (ITS)

ITS is responsible for:

- Implementing technical access controls
- Provisioning and deprovisioning accounts based on Data Owner approval
- Monitoring system logs and detecting unusual activity
- Apply and enforce Account Suspension (AS) holds when authorized under this policy and prevent any modification to accounts while an AS hold is active.
- Enforcing password, authentication, and security requirements
- Maintaining system availability, security, and integrity
- Supporting periodic access reviews

D. Users

Users must:

- Access only the systems and data they are authorized to use
- Follow all data classification and handling requirements
- Report suspected unauthorized access or data exposure to ITS immediately
- Cooperate with investigative or disciplinary processes

E. Operational Ownership Table

Data Domain / System Area	Data Owner (Functional Leader)	Data Stewards (Operational Personnel)	Operational Responsibilities
Admissions and Recruitment Data	Director of Admissions	Admissions Staff	Maintain accuracy, correct data issues, ensure FERPA compliance.
Financial Aid and GLBA-regulated Data	Director of Financial Aid	Financial Aid Specialists	Maintain records, safeguard data, complete reviews.
Finance, Accounting, and Business Office Data	Vice President of Finance	Accountants and Business Office Personnel	Maintain accuracy, ensure proper handling, coordinate corrections.
Instruction and Academic Data	Vice President of Instruction	Faculty, Academic Advisors, Division Support Staff	Maintain course and academic data accuracy..
Student Services and Student Experience Data	Vice President of Instruction	Student Success Center Staff, Advising Personnel	Manage advising/support records; maintain accuracy; protect confidential data.
Canvas Learning Management System	Vice President of Instruction	LMS Administrators, Distance Learning Support Staff	Maintain course shells, permissions, accessibility, and content integrity.
Document Management (BDM)	Admissions, Financial Aid, Finance, Instruction	Departmental Staff managing Document Management content	Maintain indexing, retention, secure access.

Banner ERP – Institutional Data	Admissions, Financial Aid, Finance, Instruction, Students	Data Stewards; ITS Technical Stewards	Maintain records, approve access, correct data, support reviews.
ITS Technical Stewardship	Director of Information Technology Services	ERP Admins, DBAs, Security Personnel	Implement controls, monitor logs, provision access, ensure security.

V. Data Domains and System Governance

Each system family is governed by a designated Data Owner and supported by Data Stewards and Technical Stewards (ITS).

VI. Access Approval and Provisioning

- All access must align with predefined role-based access models approved by the appropriate Data Owner.
- Individual permissions outside of predefined roles are prohibited unless formally documented and approved through the Standard Exceptions Process.
- Access requests for ERP systems must originate from the employee's supervisor or authorized departmental representative.
- Data Owner approval is embedded within established role definitions. Access granted consistent with an approved role does not require separate case-by-case authorization.
- ITS may not provision or modify access outside of established role definitions without documented Data Owner authorization.
- Acceptable documentation includes ticketing system records, email request, or formal access request forms submitted by the employee's supervisor. Documentation must be retained in accordance with institutional record keeping standards.
- Restricted data (including SSNs) follows the SSN Access Policy (730.1).
- Access must align with job duties and least privilege.
- Permissions must be removed immediately upon separation or role change.

ITS may place an Account Suspension (AS) hold on an account during urgent terminations or safety/security investigations. While an account is under an AS hold, no reactivation or changes to roles, permissions, or group memberships may occur. Release of an Account Suspension (AS) hold requires written authorization from the originating administrative authority as defined in this policy.

VII. Security Awareness and Training

All employees shall complete mandatory cybersecurity awareness training on an annual basis.

Completion of required training is a condition of continued access to institutional systems. Failure to complete required training within designated timelines may result in suspension or restriction of system access.

Individuals with privileged, administrative, or access to Restricted data (including Social Security Numbers) may be subject to enhanced or role-specific security training requirements.

The College shall maintain documentation of training completion for audit, compliance, and regulatory purposes.

The College may conduct periodic simulated phishing or social engineering exercises to assess awareness and reduce institutional risk. Participation in such exercises is mandatory for employees with active system access.

Results of awareness exercises may inform additional targeted training or access restrictions when appropriate.

The College shall conduct and document periodic risk assessments that evaluate internal and external risks to the security, confidentiality, and integrity of covered data, including financial aid information, and shall update safeguards based on assessment results.

VIII. Periodic Access Review (Recertification)

Access will be reviewed annually. Supervisors and Data Owners must recertify continued need; access is removed immediately upon job changes or separation.

IX. Data Quality and Stewardship Requirements

- Data must be accurate, timely, and maintained according to functional business rules.
- Data Stewards must correct identified errors promptly.
- Data Owners must define authoritative data sources and approve changes to structures, forms, and workflows.

X. Third-Party Systems and Vendor Governance

Technology services or systems that store, process, transmit, or access Northeast Mississippi Community College (NEMCC) institutional data may not be purchased, implemented, activated, or used by departments without prior review and approval by Information Technology Services (ITS).

Departments must contact Information Technology Services (ITS) before purchasing, implementing, or activating any software, cloud service, or technology system that will store, process, transmit, or access institutional data.

ITS will coordinate the vendor security review process and work with the appropriate Data Owner to evaluate vendor security controls, data protection requirements, and regulatory compliance before the system is approved for institutional use.

Vendors providing systems or services that store, process, transmit, or access institutional data may be required to complete the NEMCC Vendor Security and Compliance Assertion or an equivalent vendor security review prior to procurement, implementation, or contract execution.

ITS and the appropriate Data Owner must review vendor security documentation prior to initial system implementation and periodically thereafter based on vendor risk classification. Vendor security reviews are conducted on a risk-based schedule established by ITS and may also occur when contracts are renewed, systems change, or security concerns arise.

Before institutional data is stored or processed in a third-party system, ITS and the appropriate Data Owner must review available vendor security documentation (such as SOC 2 reports, CAIQ assessments, or equivalent materials) to verify that the vendor provides:

- Appropriate encryption capabilities
- Compliance with applicable regulations including FERPA and GLBA
- Adequate contractual safeguards for institutional data
- Appropriate access controls, logging, and security protections

Restricted institutional data may not be stored in third-party systems unless explicitly approved by both the Data Owner and ITS and only after verification that appropriate encryption, logging, and access controls are in place.

Vendors, contractors, consultants, and other third-party agents with access to Confidential or Restricted institutional data must comply with the same data protection, security, and privacy standards required of College employees.

For vendor-hosted systems, the College shall require contractual assurances that appropriate vulnerability management, patch management, and security update processes are maintained. ITS shall review vendor security documentation or attestations to confirm ongoing compliance.

XI. Exceptions

This section establishes the authoritative exceptions framework for all policies and standards within the ITS Policy Suite unless a policy expressly provides otherwise.

The College recognizes that limited exceptions may be necessary when no reasonable alternative exists and when institutional risk can be appropriately mitigated. Exceptions are not routine accommodations and shall not be granted for convenience.

All exception requests must:

- Be submitted in writing.

- Identify the specific policy requirement from which relief is requested.
- Provide documented business justification.
- Identify all affected systems, data classifications, and user populations.
- Describe associated risks.
- Define compensating controls sufficient to mitigate identified risks.
- Include a defined start date and expiration date.
- Be approved by the appropriate Data Owner.
- Be approved by the Director of Information Technology Services.

Exceptions may not:

- Override legal or regulatory obligations.
- Override Account Suspension (AS) holds.
- Remove mandatory protections for Confidential or Restricted Institutional Data.
- Extend lifecycle timeframes beyond limits established in Board-approved policies.

Approved exceptions must be documented and retained in accordance with institutional record retention schedules. Long-term exceptions shall be reviewed at least annually to confirm continued necessity and risk posture.

Individual policies within the ITS Policy Suite may reference this exceptions framework without restating its provisions.

XII. Standards Authority and Delegation

Information Technology Services (ITS) is authorized to develop, issue, maintain, and update standards, procedures, and operational controls that implement and support approved ITS policies.

Standards serve as implementation documents and must remain consistent with the governing policy. Standards may not expand, restrict, or otherwise alter the scope, authority, intent, or enforcement provisions of any Board-approved or Cabinet-approved policy.

Substantive changes that modify policy scope, authority, compliance obligations, or institutional governance structure require formal policy revision and approval through the College's established governance process.

Standards may be updated as necessary to address evolving security risks, regulatory requirements, technical changes, or operational needs, provided such updates remain aligned with approved policy.

The Director of Information Technology Services is designated as the institution's Qualified Individual under the GLBA Safeguards Rule and is responsible for overseeing, implementing, and reporting on the College's information security program as it relates to financial aid and other covered information.

The Qualified Individual shall provide a written report at least annually to the President and appropriate governing body or designated administrative authority regarding the overall status of the information security program, material risk assessments, service provider oversight, security events, and recommended improvements.

XIII. Enforcement and Sanctions

This section establishes the institutional enforcement framework applicable to all ITS policies and standards.

Violations of ITS policies may result in corrective, administrative, technical, or disciplinary actions depending on the nature and severity of the violation.

Enforcement actions fall into three categories:

A. Corrective and Supervisory Actions

Applied to minor, accidental, or first-time violations. These actions may include retraining, supervisor notification, documented warning, or policy education.

B. Administrative Risk Removal — Account Suspension (AS)

Account Suspension (AS) is an administrative risk-removal mechanism applied when continued system access presents institutional risk. AS is not progressive discipline and does not constitute a disciplinary determination.

AS governance, authorization authority, release authority, and scope are established exclusively within this policy and apply to all ITS policies and standards. When an AS hold is applied, authentication is prevented, provisioning and modification of access are blocked, and automated lifecycle processes are overridden. AS supersedes any lifecycle, retention, or automated provisioning provisions described in other ITS policies.

AS may be authorized only by designated administrative authorities as defined in this policy. Release of an AS hold requires written authorization from the originating administrative authority.

Individual policies may reference or apply an Account Suspension (AS) hold but may not redefine its authority, authorization, or release requirements.

C. Emergency Technical Containment

Information Technology Services may take immediate technical action when necessary to protect institutional systems, accounts, or data during cybersecurity incidents, confirmed compromise, or active threats. Such actions are temporary containment measures and must be documented.

All enforcement actions must be documented and retained in accordance with institutional record retention requirements.

Individual policies may reference this enforcement framework without restating its provisions.

XIV. Revisions

This policy shall be reviewed annually to ensure continued accuracy, regulatory compliance, and alignment with institutional practices. Revisions shall follow the College's established approval process, and all individuals are responsible for compliance with the current approved version. Version history shall be maintained in accordance with institutional documentation standards.

Version	Date	Description	Approved By
1.0.0	Jan 2026	Initial release of Data Governance and Security Oversight Policy.	President's Cabinet