780.1 – Incident Response and Security Incident Management Policy

Policy Title: Incident Response and Security Incident Management Policy
Policy Number: 780.1
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, and authorized users of College systems or institutional data
Alignment: FERPA; GLBA Safeguards Rule; Mississippi data breach notification requirements; NIST incident response and cybersecurity guidance (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 identifying, reporting, responding to, documenting, and resolving information security incidents. It protects institutional data, preserves evidence, limits operational disruption, and supports compliance with legal and regulatory obligations.

Incident response activities include coordination with College-managed backup and recovery controls to preserve, protect, and restore affected institutional data. Backup and restoration processes support the integrity, availability, and recoverability of student records and other institutional data in alignment with institutional continuity and disaster recovery procedures.

II. Scope

This policy applies to all College-owned or managed systems, cloud services, third-party platforms, and personal devices used to access institutional systems or data, regardless of where an incident originates.

III. Definitions

Account Compromise — Unauthorized access to a user, service, or privileged account.

Containment — Immediate actions taken to limit damage or prevent further exposure.

Data Breach — Unauthorized acquisition, access, disclosure, alteration, or destruction of Confidential or Restricted Institutional Data as defined in the Data Classification and Handling Policy (730.2).

Incident Response Team (IRT) — The group responsible for managing security incidents.

Ransomware Event — Malicious software that encrypts, exfiltrates, or disrupts institutional systems or data.

Security Incident — Any actual or suspected event that jeopardizes the confidentiality, integrity, or availability of institutional systems or data.

IV. Reporting Requirements

All users must immediately report suspected or confirmed:

- Phishing attempts
- Account compromise
- Malware infection
- Unauthorized access
- Loss or theft of devices containing institutional data
- Exposure of Confidential or Restricted information
- Suspicious system behavior

Reports must be submitted to Information Technology Services (ITS) immediately upon discovery.

Failure to report a known security incident may result in disciplinary action.

V. Incident Response Team (IRT)

Information Technology Services (ITS) leads institutional incident response.

Depending on the nature of the incident, the IRT may include:

- Director of Information Technology Services
- Human Resources (employee-related incidents)
- Vice President of Student Services (student-related incidents)
- Vice President of Finance (financial or GLBA-regulated data incidents)
- Vice President of Instruction (academic systems incidents)
- Communications/Public Relations (if public disclosure is required)
- College Administration
- Legal Counsel (as appropriate)

ITS coordinates all technical response actions.

VI. Incident Response Phases

The College follows a structured incident response lifecycle:

A. Identification

ITS evaluates reported events to determine whether a security incident has occurred.

B. Containment

ITS will take immediate action to prevent further harm, which may include:

- Disabling accounts
- Temporarily disabling authentication, terminating active sessions, restricting access, or removing devices from the network to contain active threats.
- Application of an Account Suspension (AS) hold following the governance and authorization requirements defined in the Data Governance and Security Oversight Policy (735.0) and the ITS Enforcement and Escalation Standard (735.0.1).
- Removing devices from the network
- Revoking access
- Blocking malicious IP addresses
- Preserving logs and evidence

C. Eradication

ITS removes malicious code, closes vulnerabilities, resets credentials, and eliminates unauthorized access mechanisms.

D. Recovery

Systems are restored to normal operations in a controlled manner.

E. Post-Incident Review

ITS conducts an after-action review to:

- Identify root cause
- Evaluate response effectiveness
- Recommend corrective improvements
- Determine policy or control changes

VII. Data Breach Determination

ITS, in consultation with College Administration and Legal Counsel (when applicable), will determine whether an incident constitutes a data breach under:

- FERPA
- GLBA Safeguards Rule
- Mississippi data breach notification law
- Other applicable federal or state regulations

The appropriate Data Owner will be consulted for incidents involving data within their domain. The determination must be documented.

VIII. Notification

If a breach is confirmed, the College will determine appropriate notification actions, which may include:

- Notification to affected individuals
- Notification to regulatory agencies
- Notification to law enforcement
- Notification to cyber insurance carrier
- Public communication, if required

All external communications must be coordinated through College Administration and designated communications officials.

No employee may independently disclose incident details externally without authorization.

IX. Documentation and Record Retention

ITS must maintain documentation of all security incidents, including:

- Date and time of detection
- Nature and scope of incident
- Systems and data affected
- Actions taken
- Breach determination outcome
- Notification decisions
- Corrective actions implemented

Incident documentation must be retained in accordance with institutional record retention schedules and legal requirements.

X. Vendor and Third-Party Incidents

Vendors that store or process institutional data must notify the College of suspected or confirmed security incidents involving institutional data without unreasonable delay, consistent with contractual obligations.

ITS and the appropriate Data Owner will coordinate vendor-related investigations and response actions.

XI. Testing and Review

The College may conduct periodic incident response tabletop exercises to evaluate readiness and response effectiveness.

XII. Enforcement and Sanctions

Violations of this policy may result in enforcement actions in accordance with the Data Governance and Security Oversight Policy (735.0) and the ITS Enforcement and Escalation Standard (735.0.1).

XIII. 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 Incident Response and Security Incident Management Policy	President's Cabinet