SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **INFORMATION SECURITY INCIDENT RESPONSE**	Procedure 8.15.01

I. SCOPE

This procedure applies to all College employees, contractors, third-party vendors, and students who access, store, process, or manage the College's sensitive information or IT systems. It encompasses all cybersecurity incidents, including service interruptions, data breaches, and malicious attacks.

II. DEFINITIONS

A. **Cybersecurity Incident:** Any event that threatens the confidentiality, integrity, or availability of the College's IT systems, services, or data.
B. **Cybersecurity Incident Response Plan (CIRP):** A structured document outlining the processes for managing cybersecurity incidents.
C. **Incident Response Team (IRT):** A group responsible for coordinating and executing the College's response to cybersecurity incidents.
D. **Critical Systems:** Systems identified as essential for College operations, including Ellucian Colleague ERP, Office 365, Blackboard LMS, and Building Management Systems (BMS).

III. ROLES AND REPOSNSIBILITIES

A. **Vice President for Information Technology:** Direct the implementation of the CIRP and oversee incident response efforts. Ensure compliance with FERPA, GLBA, and North Carolina Community College System (NCCCS) cybersecurity requirements.
B. **Incident Response Team (IRT):** Coordinate the College's response to cybersecurity incidents, including containment, eradication, and recovery. Notify and communicate with affected parties, regulatory agencies, and law enforcement as required.
C. **IT Division:** Maintain backups, conduct system monitoring, and perform vulnerability assessments. Isolate affected systems and assist with incident investigations.
D. **Information Technology Committee:** Update the CIRP, Information Security Program (ISP), and Disaster Recovery (DR) Plan annually. Submit updates to the President's Cabinet for final approval.
E. **Faculty, Staff, and Students:** Adhere to cybersecurity policies and report any suspected incidents to the IRT immediately.

IV. INCIDENT RESPONSE FRAMEWORK

A. **Incident Classification:**
- Interruption: Prevents a single user from completing normal operations.
- Emergency: Causes significant disruption with serious potential consequences.
- Disaster: Prevents multiple users from completing operations for an extended period.

B. **Initiation, Notification, and Communication:**
- Any employee may activate the Southwestern Community College Cyber Incident Response Call Tree.

- The Vice President for Information Technology shall initiate the NCCCS Cyber Incident Response Call Tree and direct IT staff to isolate affected systems.
- Notify staff, students, vendors, and regulatory agencies as required by compliance standards.

C. **Incident Assessment and Response:** Assess the incident's cause, impact, and scope, including potential additional risks. Contain the threat, eradicate malicious elements, and restore systems using backups.

D. **Post-Incident Review:** Conduct a post-mortem to identify root causes and document findings. Implement corrective actions and update the CIRP to prevent recurrence.

V. PREVENTION AND MONITORING

A. Maintain an inventory of critical systems and sensitive data to prioritize response efforts.

B. Perform regular vulnerability scans, penetration tests, and system monitoring to identify potential threats.

C. Conduct cybersecurity awareness training and encourage incident reporting.

D. Maintain backups, including off-site and air-gapped copies, with restoration points at least 90 days old.

VI. EVALUATION AND REVIEW

The Vice President of Technology and Campus Safety, in collaboration with the IT Division and the Information Technology Committee, will review the CIRP annually. Updates to the CIRP will incorporate new systems, lessons learned from incidents, and advancements in disaster recovery practices.

VII. ENFORCEMENT

Non-compliance with this policy may result in disciplinary action, up to termination of employment or contract termination. Unauthorized actions during an incident response, such as failure to follow containment protocols, will be addressed through disciplinary measures.

VIII. REVIEW AND REVISION

This policy will be reviewed annually or as new incident management practices and regulations emerge. Updates will incorporate lessons learned from incidents and advancements in cybersecurity techniques.

Legal References:

- North Carolina Statewide Information Security Manual, SCIO-SEC-308 - Incident Response
- FERPA (20 U.S.C. § 1232g)
- GLBA (15 U.S.C. § 6801)
- NIST SP 800-61: Computer Security Incident Handling Guide
- CIS Controls v8, Control 17 (Incident Response Management)

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **INFORMATION SECURITY INCIDENT RESPONSE**	Procedure 8.15.01

Cross References:

- Policy 8.03 - Electronic Records Retention
- Policy 8.21 - Secure Configuration Management
- Policy 8.13 - Risk Management
- Policy 8.10 - Information Security Program

Adopted: September 2025

Revised: N/A