SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **COMPLIANCE WITH IT POLICIES AND CONTINUOUS IMPROVEMENT PROCEDURE**	Procedure 8.01.01

I. PURPOSE

The purpose of this procedure is to outline the College's commitment to complying with its Information Technology (IT) policies while fostering continuous improvement. This policy establishes a framework for prioritizing critical compliance efforts, achieving meaningful progress in security and operational practices, and aligning with legal, regulatory, and industry standards.

The College's compliance efforts will initially prioritize the CIS Controls Implementation Group 1 (IG1) to implement foundational security practices that support continuous improvement while minimizing administrative burden.

II. DEFINITIONS

A. **CIS Controls Implementation Group 1 (IG1):** A set of foundational cybersecurity controls defined by the Center for Internet Security (CIS) designed for small to medium-sized organizations. IG1 focuses on basic protections against common cyber threats, emphasizing practical and cost-effective solutions.
B. **Intentional Violations:** Deliberate actions that knowingly disregard IT policies, compromise security, or circumvent procedures for personal or organizational gain. Examples include sharing confidential information without authorization or intentionally bypassing security controls.
C. **Non-Intentional Violations:** Actions that inadvertently result in non-compliance with IT policies, often due to insufficient training, unclear guidance, or incomplete implementation. Examples include accidental misuse of systems or failure to follow procedures because of gaps in understanding.
D. **Compliance Maturity Period:** The transitional phase during which the College is actively working to implement, refine, and achieve compliance with newly adopted IT policies and practices.
E. **Critical Violations:** Violations that result in significant risks to the College's data, systems, or operations, regardless of intent. These include unauthorized access to sensitive systems or breaches of confidentiality obligations.
F. **Corrective Measures:** Non-punitive actions aimed at addressing non-compliance, such as training, process updates, or system improvements, to prevent recurrence and support continuous improvement.

III. COMPLIANCE FRAMEWORK

A. **Address High-Priority Risks:** Concentrate compliance efforts on areas identified as high-risk or critical to the College's operations and mission.
B. **Implement Incremental Improvements:** Work systematically to implement IG1 practices, such as inventory management, access control, and incident response, while maintaining operational efficiency.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **COMPLIANCE WITH IT POLICIES AND CONTINUOUS IMPROVEMENT PROCEDURE**	Procedure 8.01.01

C. **Foster a Culture of Security:** Provide practical training and awareness programs to encourage compliance without overburdening users or staff.
D. **Perform Targeted Reviews:** Limit reviews to key areas, such as progress in implementing specific IG1 controls and addressing critical compliance needs.

IV. ROLES AND RESPONSIBILITIES

A. **Vice President for Information Technology**: Direct and prioritize compliance efforts to align with institutional goals and available resources. Report progress on critical compliance initiatives to the President's Cabinet.
B. **IT Division**: Focus on implementing practical improvements aligned with IG1 controls. Perform limited compliance reviews that assess progress in critical areas without excessive tracking or reporting.
C. **Employees, Students, and Vendors:** Adhere to all IT policies and participate in security training. Report security concerns or potential risks to the IT Department.

V. MONITORING AND REVIEW

A. **Targeted Compliance Reviews:** The IT Department will conduct reviews limited to: Progress in implementing prioritized IG1 controls. Addressing identified critical risks or vulnerabilities.
B. **Annual Assessment**: The Vice President for Information Technology will oversee an annual review of compliance efforts, focusing on progress in key areas rather than exhaustive tracking of all activities.
C. **Practical Adjustments:** Compliance reviews will inform adjustments to IT policies to ensure they remain achievable and aligned with institutional priorities.

VI. ENFORCEMENT GUIDELINES FOR ALL IT POLICIES

A. **Intentional vs. Non-Intentional Violations:** Deliberate actions that knowingly disregard IT policies, compromise security, or circumvent procedures will result in disciplinary action. Non-intentional violations, often stemming from insufficient training, will focus on corrective measures such as training, coaching, or procedural updates. Non-intentional violations that significantly compromise or disrupt the College's operation may also lead to disciplinary action.
B. **Corrective Measures:** Non-intentional violations will generally be addressed through actions such as additional training, updates to procedures, or process improvements to prevent recurrence.
C. **Leadership Accountability:** Supervisors and department heads are responsible for fostering compliance within their teams and addressing systemic issues contributing to non-compliance.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **COMPLIANCE WITH IT POLICIES AND CONTINUOUS IMPROVEMENT PROCEDURE**	Procedure 8.01.01

D. **Proportional Enforcement:** Enforcement during the compliance maturity period will prioritize high-risk or intentional violations, with non-critical violations emphasizing corrective actions over punitive measures.

VII. REVIEW AND REVISION

This policy will be reviewed annually to ensure it supports efficient and effective compliance efforts and remains aligned with institutional goals.

LEGAL REFERENCES

- North Carolina Statewide Information Security Manual
- CIS Controls v8
- NIST Cybersecurity Framework
- State Board of Community Colleges Code, 1B SBCCC Subchapter 700 - Information Security Program

Previously Referenced as: N/A

Adopted: September 2025

Revised: N/A