

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY ELECTRONIC SIGNATURES	Procedure 8.04.01
-----------------------------------	--	----------------------

I. PROCEDURE

The purpose of this procedure is to establish guidelines for the use, management, and legal recognition of electronic signatures within the College. By adopting electronic signatures, the College aims to provide efficient and improved services to its employees, students, and the public, while ensuring compliance with applicable state and federal laws.

II. SCOPE

This policy applies to all employees, students, contractors, and third-party service providers who utilize electronic signatures in official College transactions. It covers all approved electronic signature technologies and systems authorized for use by the College.

III. DEFINITIONS

- A. **Electronic Signature:** An electronic sound, symbol, or process attached to or logically associated with a document and executed with the intent to sign it.
- B. **Digital Signature:** A type of electronic signature that uses cryptographic techniques to ensure authenticity, integrity, and non-repudiation.
- C. **Approved Electronic Signature System:** Any system or tool authorized by the College for creating, applying, and verifying electronic signatures.

IV. RESPONSIBILITIES

- A. **IT Division:** Ensure that electronic signature systems comply with security, privacy, and audit requirements, and provide training and technical support.
- B. **Users:** Maintain the confidentiality of their accounts and use electronic signatures only for authorized purposes. Users must adhere to the requirements of Policy 8.02 - Acceptable Use.
- C. **Business Units:** Identify transactions suitable for electronic signatures and ensure appropriate records are maintained in compliance with retention policies.

V. APPROVED USES

A. Permitted Transactions:

- Students may use electronic signatures for registration, financial aid processes, bill payments, updating contact information, logging into campus systems, and submitting classwork or tests.
- Employees may use electronic signatures for submitting grades, viewing payroll data, completing forms, accessing protected data, and using administrative systems.
- Third parties may use electronic signatures for contracts, service agreements, and other authorized transactions with the College.

B. Restricted Transactions:

- Documents requiring notarization or witness signatures unless supported by an approved electronic signature system.
- Transactions involving classified or highly sensitive data unless explicitly authorized.

VI. SECURITY REQUIREMENTS

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY ELECTRONIC SIGNATURES	Procedure 8.04.01
-----------------------------------	--	----------------------

- A. Electronic signatures must be applied using College-approved systems that provide encryption, identity verification, and secure audit trails.
- B. Multi-factor authentication (MFA) is required for systems used to create or verify electronic signatures.
- C. Users must not share account credentials or allow unauthorized access to their accounts.

VII. RECORD RETENTION

Records containing electronic signatures must be retained in compliance with Policy 8.03 - Electronic Records Retention. Such records must remain accessible for audits, legal inquiries, and operational needs.

VIII. LEGAL RECOGNITION

Electronic signatures will be recognized as legally binding if they clearly indicate the signer's intent, are executed using approved systems, and comply with the North Carolina Uniform Electronic Transactions Act (N.C.G.S. § 66- 311 et seq.) and the Electronic Signatures in Global and National Commerce Act (E-SIGN Act).

IX. ENFORCEMENT

Unauthorized or fraudulent use of electronic signatures is strictly prohibited and may result in disciplinary action, up to termination, and/or legal consequences. Regular audits will be conducted to ensure compliance with this policy.

X. REVIEW AND REVISION

This policy will be reviewed annually or as necessary to ensure alignment with technological advancements, regulatory updates, and College requirements.

LEGAL REFERENCES:

- N.C.G.S. § 66-311 et seq. (North Carolina Uniform Electronic Transactions Act)
- Electronic Signatures in Global and National Commerce Act (E-SIGN Act)
- Statewide Information Security Manual, NC Department of Information Technology (NCDIT SCIO-SEC-316)
- CIS Controls 5 (Account Management), 16 (Application Software Security)

CROSS REFERENCES:

- Policy 8.02 - Acceptable Use Policy
- Policy 8.03 - Electronic Records Retention
- Policy 8.10 - Information Security Program

Previously Referenced as: October 2013 (4.05.03)

Adopted: September 2025

Revised: N/A