SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **INFORMATION CLASSIFICATION AND HANDLING**	Procedure 8.11.01

I. SCOPE

This policy applies to all data created, collected, processed, stored, or transmitted by the College, including data managed by third parties on behalf of the College. It covers all users of the College's data, including employees, contractors, and students.

II. DEFINITIONS

A. **Data Classification:** The process of categorizing data based on its level of sensitivity and the impact of unauthorized disclosure.
B. **Data Handling:** Procedures for accessing, storing, transmitting, and disposing of data based on its classification level.
C. **Data Owner:** The individual or department responsible for ensuring appropriate data classification and handling.

III. RESPONSIBILITIES

A. **Data Owners:** Responsible for classifying data under their control and ensuring compliance with handling requirements.
B. **Users:** Responsible for adhering to data handling procedures based on the classification of the data they access.
C. **Information Technology (IT) Division:** Responsible for implementing technical controls to protect data according to its classification.

IV. DATA CLASSIFICATION LEVELS

A. **Public:** Data that is freely available to the public without restrictions.
B. **Restricted**: Data that requires safeguards due to its sensitive nature, but which does not meet the criteria for highly restricted data.
C. **Highly Restricted:** Data that requires stringent security measures due to its criticality or sensitivity, such as Personally Identifiable Information (PII), Federal Tax Information (FTI), or other similar classifications.

V. DATA HANDLING REQUIREMENTS

A. Data must be classified by Data Owners based on its sensitivity and regulatory requirements.
B. Access to data must be restricted to authorized users in alignment with the principle of least privilege.
C. Data must be stored only on approved systems and devices that meet the College's security standards.
D. Transmission of restricted or highly restricted data must use secure methods, such as encrypted email or file transfer protocols.
E. Disposal of data must follow secure methods, such as shredding or secure digital deletion.

VI. MONITORING AND AUDIT

A. The IT Division will implement monitoring tools to ensure compliance with data classification and handling requirements.

B. Data access logs will be reviewed periodically to identify unauthorized access or misuse.

VII. ENFORCEMENT

A. Violations of this policy may result in disciplinary action, up to and including termination of employment or expulsion from the College.
B. Unauthorized access to or mishandling of data may result in civil or criminal penalties under applicable laws.

VIII. REVIEW AND REVISION

This policy will be reviewed annually or as needed to ensure alignment with regulatory requirements and evolving data security practices.

Legal References:

- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, Controls 3 (Data Protection and Data Encryption)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations
- FERPA (20 U.S.C. § 1232g)

Cross References:

- Policy 8.16 - Information Systems Access Control
- Policy 8.17 Information Systems Operations Security
- Policy 8.20 - Data Management

Adopted: September 2025

Revised: N/A