Administrative Policy

Southwest Wisconsin TECHNICAL COLLEGE

Item	*Details*
Policy Title:	***Data Classification Policy***
Policy Category:	Operational & Information Technology Policies
Related Procedure(s)/ Guideline(s):	
Policy Owner:	Executive Director of Information Technology Services
Date Approved:	6/3/26
Review Dates:	
Revision Dates:	
Policy Scope:	This policy applies to all employees, authorized contractors, vendors, temporary workers, volunteers, and any other authorized users who access, process, store, or transmit College data.
Policy Statement:	Southwest Wisconsin Technical College (Southwest Tech) is committed to protecting the confidentiality, integrity, and availability of its data while enabling appropriate access and use in support of institutional operations, student success, and academic excellence. This policy establishes a standardized framework for classifying College data based on sensitivity, risk, and regulatory requirements. Classification ensures appropriate safeguards are applied and supports compliance with applicable laws and regulations, including, but not limited to, Family Educational Rights and Privacy Act (FERPA), Graham Leach Bliley Act (GLBA), and Payment Card Industry Data Security Standard (PCI-DSS). This policy is not intended to unnecessarily restrict access to

data, but rather to ensure data is used responsibly and securely.

Data Classification Levels

Restricted: Highly sensitive data protected by federal or state statutes or regulations, college regulations, or contractual language. Disclosure or modification of restricted data without authorization would have severe adverse effect on the operations, assets, or reputation of the college or the college's confidentiality obligations. (e.g., SSN, financial data, Personal Health Information (PHI)).

Confidential: Sensitive institutional or student data that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a criminal or civil statute requiring this protection. Confidential data is information that is restricted to members of the college community who have a legitimate purpose for accessing such data. (e.g., FERPA records, GPA)

Internal: Operational data intended for internal use. Internal data is information that is restricted to personnel who have a legitimate need for access, though those with a legitimate need could constitute a large group (e.g. all faculty and staff). Unauthorized use or disclosure could have a limited adverse impact on the College, affiliates, or individuals

Public: Information approved for public release. Disclosure of public data will likely have little or no adverse impact on the College, affiliates, or individuals.

Data Ownership and Responsibilities

- Data Owner: Responsible for classification and access decisions.
- Data Steward: Ensures proper use and data quality.
- Data Custodian (ITS): Implements security controls.
- All Users: Responsible for appropriate handling and reporting issues.

Data Handling and Protection Requirements

- Restricted data requires encryption, multi-factor authorization (MFA), and approved systems only.

- Confidential data requires encryption in transit and limited access.
- Internal data is for internal use only.
- Public data has no restrictions.

Data Handling Standards

- Storage: Restricted data must not be stored on personal devices.
- Transmission: Sensitive data must be encrypted.
- Access: Must follow least privilege.
- Retention: Follow records retention policy.
- Disposal: Secure destruction required.

Technology and System Alignment

Microsoft 365 (Purview, DLP), enterprise systems, and identity management tools will be used in the enforcement of this policy.

Artificial Intelligence (AI) and Data Use

- Restricted and Confidential data must not be entered into AI tools unless approved and protected.
- Users must validate AI outputs.

Monitoring and Enforcement

The College will monitor AI use as necessary to ensure security, compliance, and proper operation. Violations may result in removal of access, disciplinary action, or other remedies in accordance with College policies (Student Code of Conduct / Employee Handbook).

Enforcement and auditing will be monitored using various methods (see table below).

Area	Responsible Role	Cadence	Method
Acceptable Use	Executive Director ITS / AI Council	Annual + ongoing	AI tool approval, training, policy acknowledgment, monitoring

	Auditing	ITS Security / Internal Audit	Quarterly	Log reviews, audit reports
	Enforcement	HR + ITS Security	As needed (Single License Agreement defined)	Incident response workflow
	Risk Assessment	AI Council	Quarterly	Risk register, tool reviews
	Data Protection	Data Stewards + ITS Security	Continuous + annual review	DLP, access controls, audits