Administrative Policy

Southwest Wisconsin TECHNICAL COLLEGE

Item	*Details*
Policy Title:	Data Security & Retention Policy
Policy Category:	Ethics, Legal & Compliance Information Technology
Related Procedure(s)/ Guideline(s):	
Policy Owner:	Executive Director of Information Technology Services
Date Approved:	8/23/24
Review Dates:	
Revision Dates:	10/6/2026
Policy Scope:	This policy applies to students, employees, Board members, contractors, vendors, and other authorized individuals who access, use, manage, transmit, store, or maintain College data.
Policy Statement:	Southwest Wisconsin Technical College (Southwest Tech) recognizes that as part of college operations data including sensitive data is collected and stored in both an electronic and physical format. The purpose of this policy is to describe how sensitive data must be handled, stored, and secured in order to meet Southwest Tech's data protection standards; comply with applicable laws, statutes, and regulations; and protect the rights of staff, students, and any related data subjects. This Data Security & Retention Policy applies to all business processes, information systems and components, personnel, and physical areas of Southwest Tech. This policy applies to the storage and handling of sensitive data and any other procedures related to sensitive data of any individual in both electronic and physical format and the lifecycle management of such data.

Sensitive Data Covered by This Policy

Sensitive data includes, but is not limited to:

- Personally Identifiable Information (PII), as defined by Wisconsin Legislature s. 19.62(5)
- Protected Health Information (PHI), as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Student Records, as defined by the Family Educational Rights and Privacy Acts of 1974 (FERPA)
- Customer record information, as defined by the Gramm Leach Bliley Act (GLBA)
- Card holder data, as defined by the Payment Card Industry Data Security Standard (PCI DSS)
- Confidential personnel information

Baseline Requirements

- Employees will keep all data secure by taking reasonable precautions and following guidelines outlined within this policy and any associated procedures.
- Data may not be shared informally. Data access levels will be determined based on role and existing access controls.
- Southwest Tech will provide training to all employees to help them understand their responsibilities when handling data.
- Sensitive data will not be disclosed to any unauthorized person, either within the organization or externally.
- Authorized entities or persons are required to have a legitimate business purpose, data sharing agreement, contracted vendor responsibilities statement, and or non-disclosure agreement which declares the data being shared as sensitive.
- Multi-factor authentication (MFA) shall be required for accounts accessing College systems, applications, email services, cloud environments, or institutional data as determined by Information Technology Services (ITS).

- Users are responsible for maintaining approved authentication methods and complying with established MFA requirements.
- Third-party service providers that access, process, store, transmit, or host College data shall be subject to appropriate security, privacy, and contractual review requirements. Vendors may be required to provide documentation demonstrating compliance with applicable security, privacy, and regulatory requirements before access to College data is authorized.

Data Handling

Data users (record creators, handlers, and controllers) will handle sensitive data in a manner that is in accordance with the laws, regulations, and standards covered by this policy.

- When working with sensitive data, or when a user's account has access to sensitive data, users will ensure screens/computers are locked with a secure password when left unattended.
- Data users may not informally share sensitive data.
- Sensitive data may not be shared via email unless the data is protected by encryption. Contact the Charger Help Desk if you need assistance in ensuring data is transmitted securely.
- Data users shall not unnecessarily duplicate sensitive data.
- Where applicable, data users will provide each data subject with information regarding the processing of their information.
- Data users will act in the best interest of data subjects when handling sensitive data.

Southwest Wisconsin Technical College utilizes authentication, identity verification, and access management controls to verify users accessing institutional systems and data. Users granted access to College systems shall be assigned unique user credentials and are responsible for maintaining the confidentiality of their authentication information.

Information Technology Services shall establish and maintain standards governing password complexity, password expiration, multi-factor authentication, account security, and

related access control requirements, and users must comply with all established authentication and credential management requirements as a condition of access to College systems and data.

Data Storage

- When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts.
- Data users shall protect sensitive data with strong passwords.
- Data users will refrain from saving data directly to end-user devices.
- Data users will refrain from using removable media; if data is stored on removable media devices, they must be stored securely.
- Southwest Tech data must be stored on secure drives and servers and may only be uploaded to Southwest Tech-approved cloud computing service(s).
- Computing hardware that stores sensitive data shall be housed in secure locations.
- Data users will refrain from storing data on paper and only print when necessary.
- When not actively in use, paper or files containing sensitive data must be kept in a locked drawer or filing cabinet.
- Data users must ensure paper documents containing sensitive data are not left where unauthorized people could view them, for example, on a printer.

Data Accuracy

- Data users must take reasonable steps to ensure sensitive data is as accurate as possible.
- Data stored at Southwest Tech is held in centralized locations. Data users should refrain from duplicating/ copying data to create local versions. The use of additional data sets may have a negative impact on data integrity. Where this practice may be required, data users must be aware of additional liabilities and safeguards that may be applicable.
- Where applicable, Southwest Tech will ensure data subjects can easily update their information.

Data Retention

- Data should be periodically reviewed and deleted or disposed of in the proper manner if no longer required by policy, procedure, or regulation.
- Centralized data backups shall be executed by authorized Southwest Tech ITS personnel.
- Paper documents in designated departments must be shredded and disposed of securely when no longer required. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.

Data Protection

- Southwest Tech ITS staff (ITS) will utilize necessary physical and technical controls and organizational measures to ensure all infrastructure containing data is protected and secured.
- Data users must promptly report suspected information security incidents, unauthorized disclosures, lost or stolen devices, phishing attempts, cybersecurity concerns, or potential data breaches to Information Technology Services.
- Security incidents should be reported through established ITS support channels, including the College's ticketing system, designated reporting mechanisms, or official ITS contact methods.
- ITS will analyze data security processes to identify potential areas of weakness and will consult with the appropriate individuals to assess and remediate risk.