| SOUTHWESTERN COMMUNITY COLLEGE | INFORMATION TECHNOLOGY<br>**DATA MANAGEMENT** | Procedure 8.20.01 |
|---|---|---|

## I. PROCEDURE STATEMENT

Managing data within an enterprise includes data classification, inventory, handling, retention, and disposal. The *Data Management Procedure* provides the processes and procedures for governing data within the enterprise. This includes creating a data inventory and classifying data based on sensitivity. Additionally, procedures for securely protecting data from unauthorized access or modification alongside appropriate for methods for how users should handle their data during their day-to-day work activities. Finally, authorized methods to destroy and remove data from the enterprise are discussed.

## II. RESPONSIBILITY

- The IT Division ("IT") is responsible for managing the enterprise's data as this information is housed on workstations and servers primarily maintained by IT. Information owners are responsible for coordinating data maintenance activities with IT.

- Users have the responsibility to protect data associated with their role from unauthorized access and disclosure. IT is responsible for informing all users of their responsibilities associated with protecting data entrusted to them.

## III. DEFINITIONS

**Data Acquisition** – The process of gathering data which can then be displayed, stored, and analyzed.

**Data Inventory** – A record of all data relevant to an enterprise for analysis, decision-making, or other justifiable need.

**Data Classification** – Organizing data by categories that can be used to dictate protection and security efforts by priority.

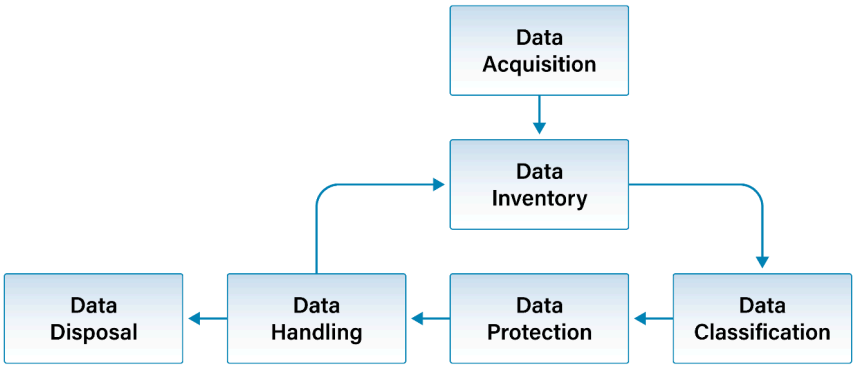
**Data Protection** – The process of safeguarding data from corruption, compromise, or loss.

**Data Handling** – The process of ensuring that data is stored in a safe and secure manner during usage and afterward.

**Data Disposal** – The process of removing enterprise data from enterprise assets, to include hard paper copies.

## IV. DATA MANAGEMENT LIFECYCLE

| SOUTHWESTERN COMMUNITY COLLEGE | INFORMATION TECHNOLOGY **DATA MANAGEMENT** | Procedure 8.20.01 |
|---|---|---|




Components of a data inventory may include:

- **Identifier** – This can be a filename or other unique identifier.
- **Data type** – Financial, Personally Identifiable Information (PII), or other type of data.
- **Data owner** – The individual or business unit entrusted with the data.
- **Data classification/label** – While data classification is not an IG1 requirement, enterprises should, at a minimum capture data sensitivity using sensitive or non-sensitive categories. If capable, enterprises can further classify data using topic area (e.g., PII).
- **Data location** – Where the data is stored.
- **Data format** – Type of file, which may be database or long-term storage device/service.

**Data retention** – Required time frame for retention of data for legal, regulatory, or business requirements.

## V. DATA ACQUISITION

There are no IG1 safeguards that support this portion of the data management process.

## VI. DATA INVENTORY

A. IT must conduct an inventory of data on an annual basis.
   1. All sensitive data must be marked accordingly in the data inventory.
   2. A data owner must be associated with all data tracked within the inventory.
   3. Data with specific data retention needs must be labeled accordingly.

B. All data owners are required to contact IT upon the creation of, or obtaining, sensitive data to ensure the data is tracked within the data inventory.

## VII. DATA CLASSIFICATION

A. IT must establish and enforce labels for sensitive data.
B. IT must review data classification labels and their usage on an annual basis.

| SOUTHWESTERN COMMUNITY COLLEGE | INFORMATION TECHNOLOGY **DATA MANAGEMENT** | Procedure 8.20.01 |
|---|---|---|

## VIII. DATA PROTECTION

A. IT must configure access control lists on enterprise assets in accordance with user's need to know. This is to include laptops, smartphones, tablets, centralized file systems, remote file systems, databases, and all applications.
B. Sensitive data must be encrypted on all user devices.

## IX. DATA HANDLING

A. IT must develop and maintain a written data retention plan.

    1. All data and documents must be preserved for the appropriate amount of time as dictated by regulatory, legal, and business requirements.

## X. DATA DISPOSAL

A. IT, or other authorized parties, must destroy data that have outlasted their specified retention timeframes.
B. All users are required to contact IT before disposing of sensitive data.
C. Non-sensitive data may be disposed of without speaking to IT via common destruction methods (e.g., trash, commonplace deletion from a computer system).
D. Sensitive data destruction must be performed in a manner that preserves confidentiality.
    1. Reports, correspondence, and other printed media:
        i. Shredding – Documents must be shredded using IT approved cross-cut shredders,
        ii. Shredding Bins – Disposal must be performed using locked bins located on-site using an IT approved shredding service, or
        iii. Incineration – Materials are physically destroyed using an IT approved incineration service.
    2. Portable Media (e.g., Solid State Drives (SSDs), digital video discs (DVDs), universal serial bus (USB) data storage devices):
        i. Physical Destruction – Complete destruction of media by means of shredding, crushing, or disassembling the asset and ensuring no data can be recovered.
    3. Hard Disc Drives (HDDs) and other magnetic media to include printer and copier hard-drives:
        i. Overwriting – Using a program to write binary data sector by sector onto the media, or
        ii. Physical Destruction – Crushing, disassembling, or degaussing the asset to ensure no data can be extracted or recreated.
    4. Tape Cartridges
        i. Degaussing – Using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state, or
        ii. Physical Destruction – Complete destruction of the tapes.
    5. Third-party service provider systems (e.g., cloud services) must be disposed of by first requesting the appropriate methods to permanently delete data

stored in their systems, and then performing those actions according to the received instructions.

6. All destruction of data must be logged in the data inventory, when applicable.
    i. IT must obtain proof of destruction if using a third-party disposal contractor.

**LEGAL REFERENCES:**

- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, Control 3 (Data Protection)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

Adopted: September 2025

Revised: N/A