Data Management Standard

Purpose

Managing data within District 6 includes data classification, inventory, handling, retention, and disposal. The *Data Management Standard* provides the processes and procedures for governing data within the District. 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 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 District are discussed.

Responsibility

- The IT business unit is responsible for managing the District'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.

Exceptions

Exceptions to this policy are likely to occur. Requests for exception must be made in writing and must contain:

- The reason for the request,
- Risk to the District of not following the written policy,
- Specific mitigations that will not be implemented,
- Technical and other difficulties, and
- Date of review.

Policy

Data Acquisition

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

Data Inventory

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

Data Classification

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

Data Protection

1. IT must configure access control lists on District assets in accordance with each user's need to know. This includes laptops, smartphones, tablets, centralized file systems, remote file systems, databases, and all applications.
2. Sensitive data must be encrypted on all user devices.

Data Handling

1. IT must develop and maintain a written data retention plan.
    a. All data and documents must be preserved for the appropriate amount of time as dictated by regulatory, legal, and business requirements.
    b. There should be a bias towards destroying data which does not clearly need to be kept.

Data Disposal

1. IT, or other authorized parties such as student information systems, finance, or human resources, must destroy data that have outlasted their specified retention timeframes.
2. All users are required to contact IT or before disposing of sensitive data.
3. Non-sensitive data may be disposed of without speaking to IT via common destruction methods (e.g., trash, commonplace deletion from a computer system).
4. Sensitive data destruction must be performed in a manner that preserves confidentiality.
    a. Reports, correspondence, and other printed media:
        i. Shredding – Documents must be shredded using 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.
    b. 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.
    c. 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.
    d. Magnetic Media (generally 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.
    e. 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.
5. All destruction of data must be logged in the data inventory, when applicable.
    a. IT must obtain proof of destruction if using a third-party disposal contractor.

Revision History

Each time this document is updated, this table should be updated
.

Version	Revision Date	Revision Description	Name
V1.0	01/02/2023	Initial Written Standard	Scott Tisinger