Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		301
Subject Title **Data Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

POLICY

Application

This policy shall apply to The Right Door for Hope, Recovery and Wellness.

1. Intent

To Provide the contextual framework for Data Management within the Right Door for Hope Recovery and Wellness.

2. Purpose

Managing data within an enterprise includes data classification, inventory, handling, retention, and disposal. The Data Management Policy 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.

3. Responsibility

The IT Department 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.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		301
Subject Title **Data Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

4. 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 enterprise of not following the written policy,
- Specific mitigations that will not be implemented,
- Technical and other difficulties, and
- Date of review.

5. Scope of Data Management

5.1. Data Acquisition

There are no IG1 safeguards that support this portion of the data management process. The Right Door will recommend to external partners that any information sent to the Right Door be done so in a secure manner.

5.2. Data Inventory

IT must conduct an inventory of data on an annual basis.

- All sensitive data must be marked accordingly in the data inventory.
- A data owner must be associated with all data tracked within the inventory.
- Data with specific data retention needs must be labeled accordingly.

5.3. Data Classification

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

5.4. Data Protection

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.

Sensitive data must be encrypted on all user devices.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		301
Subject Title **Data Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

5.5. Data Handling

IT must develop and maintain a written data retention plan.

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

5.6. Data Disposal

IT, or other authorized parties, must destroy data that have outlasted their specified retention timeframes.

All users are required to contact IT before disposing of sensitive data.

Non-sensitive data may be disposed of without speaking to IT via common destruction methods (e.g., trash, commonplace deletion from a computer system).

Sensitive data destruction must be performed in a manner that preserves confidentiality.

Reports, correspondence, and other printed media:

- Shredding – Documents must be shredded using IT approved cross-cut shredders,
- Shredding Bins – Disposal must be performed using locked bins located on-site using an IT approved shredding service, or
- Incineration – Materials are physically destroyed using an IT approved incineration service.

Portable Media (e.g., Solid State Drives (SSDs), digital video discs (DVDs), universal serial bus (USB) data storage devices):

- Physical Destruction – Complete destruction of media by means of shredding, crushing, or disassembling the asset and ensuring no data can be recovered.

Hard Disc Drives (HDDs) and other magnetic media to include printer and copier hard-drives:

- Overwriting – Using a program to write binary data sector by sector onto the media, or
- Physical Destruction – Crushing, disassembling, or degaussing the asset to ensure no data can be extracted or recreated.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		301
Subject Title **Data Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

Tape Cartridges

- Degaussing – Using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state, or
- Physical Destruction – Complete destruction of the tapes.

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.

All destruction of data must be logged in the data inventory, when applicable.

IT must obtain proof of destruction if using a third-party disposal contractor.

Deborah McPeek-McFadden, Board Chairperson	Date		