Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		403
Subject Title Software Asset Management	Adopted	Last Revised	Reviewed
	2/28/23	1/20/23	6/24/24

POLICY

Application

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

1. Intent

The IT department unit is responsible for all software asset management functions. This information is relayed to other departments as needed. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them.

2. Purpose

2.1. Software asset management is the process of procuring, identifying, tracking, maintaining, and removing software on enterprise assets. This Software Asset Management Policy provides the policies for governing the software asset lifecycle while an enterprise is using a software asset. A software inventory must be created and maintained to support the enterprise's mission and to help ensure only authorized software is installed and used. This software inventory must be up-to-date and reflect the current state of software across the enterprise.

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

2.2.1. The reason for the request,

2.2.2. Risk to the enterprise of not following the written policy,

2.2.3. Specific mitigations that will not be implemented,

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		403
Subject Title Software Asset Management	Adopted	Last Revised	Reviewed
	2/28/23	1/20/23	6/24/24

2.2.4. Technical and other difficulties, and

2.2.5. Date of review.

3. Software Asset Management Scope

   3.1. Procurement

      3.1.1. Only individuals from IT are approved to procure software.

      3.1.2. IT must maintain a list of approved software vendors.

      3.1.3. Software must only be purchased from vendors on the approved software list.

   3.2. Installation

      3.2.1. Any software installed on enterprise assets, alongside other relevant information within the software asset, must be recorded within the software inventory. This must include:

         3.2.1.1. Title of software

         3.2.1.2. Developer or publisher of software

         3.2.1.3. Date of acquisition

         3.2.1.4. Date of installation

         3.2.1.5. Duration of usage

         3.2.1.6. Business purpose

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		403
Subject Title Software Asset Management	Adopted	Last Revised	Reviewed
	2/28/23	1/20/23	6/24/24

        3.2.1.7. App Store(s)

        3.2.1.8. Version(s)

        3.2.1.9. Uniform Resource Locator (URL)

        3.2.1.10. Deployment mechanism

        3.2.1.11. End-of-support (EoS) date, if known

        3.2.1.12. End-of-life (EoL) date, if known

        3.2.1.13. Any relevant licensing information

        3.2.1.14. Decommission date

    3.2.2. IT must verify the software asset inventory at least every six months.

    3.2.3. Only software that has been approved by IT may be installed.

    3.2.4. Only cloud services that have been approved by IT may be used within the enterprise.

    3.2.5. Mobile devices may only obtain software from IT approved sources.

  3.3. Usage

    3.3.1. In general, refer to the enterprise's Acceptable Use Policy.

    3.3.2. There are no IG1 safeguards that support this portion of the software asset management process.

  3.4. Discovery

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		403
Subject Title Software Asset Management	Adopted	Last Revised	Reviewed
	2/28/23	1/20/23	6/24/24

3.4.1. IT must review all software installed on enterprise assets on a monthly basis.

   3.4.1.1. All installed software on enterprise assets must be reported to IT on a regular basis.

   3.4.1.2. All newly discovered software must be checked against the list of approved software in the software asset inventory.

3.4.2. Identified software not included within this inventory must be investigated as the software may be unauthorized.

3.4.3. Assets containing unauthorized software must be removed from the network unless temporary access is granted by the IT business unit.

3.4.4. The presence of unauthorized software must be properly investigated.

3.4.5. All newly discovered (authorized) software must be added to the software inventory.

3.4.6. Unauthorized software must be removed from use on enterprise assets or receive a documented exception.

3.5. Update and Upgrade

All updates and upgrades must be approved by IT prior to installation. IT configuring a device for automatic updates, or directing users to do so, constitutes a tacit approval.

3.6. Removal

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		403
Subject Title Software Asset Management	Adopted	Last Revised	Reviewed
	2/28/23	1/20/23	6/24/24

3.6.1. Software to be decommissioned must be removed from all enterprise assets.

3.6.2. Assets containing retired software must be protected with additional defensive mitigations, such as removal from the network or isolation.

3.6.3. IT must make a copy of the user data as needed.

3.6.4. Ensure that any retired software did not store data in other servers or cloud infrastructure not owned by the enterprise.

Nancy Patera, Board Chairperson	Date		