Chapter Title Information Technology / Information Systems	**Section #** ITIS		**Subject #** 407
Subject Title **Vulnerability 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 protect IT resources of the Right Door.

2. Purpose

Vulnerability management is the process of searching for, prioritizing, and remediating vulnerabilities in enterprise systems and software. The Vulnerability Management Policy provides the processes and procedures for ensuring enterprise assets do not contain vulnerabilities. This policy applies to all departments and all assets connected to the enterprise network.

3. Vulnerability Management Scope

3.1. Assess

A process for performing vulnerability management must be established.

3.1.1. This process must be documented and approved.

3.1.2. At a minimum, the vulnerability management process must be reviewed on an annual basis or following significant changes within the enterprise.

3.1.3. IT must monitor vulnerability announcements and emerging threats applicable to enterprise asset inventory.

3.1.4. All systems connected to the enterprise network must be scanned for vulnerabilities.

3.2. Prioritize

Identified vulnerabilities must be prioritized, with more critical vulnerabilities addressed first.

3.3. Remediate

3.3.1. A process for remediating identified vulnerabilities must be established.

Chapter Title Information Technology / Information Systems	**Section #** ITIS		**Subject #** 407
Subject Title **Vulnerability Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

3.3.1.1. This process must be documented and approved.

3.3.1.2. At a minimum, this process must be reviewed on an annual basis or following significant changes within the enterprise.

3.3.1.3. Vulnerabilities that cannot be remediated must be submitted through the vulnerability exception process.

3.3.2. Operating systems must be configured to automatically update unless an alternative approved patching process is used.

3.3.3. Applications must be configured to automatically update unless an alternative approved patching process is used.

3.3.4. All users of enterprise assets have a duty to install updates for business systems and applications in a timely manner.

3.3.5. All users must ensure required reboots occur within a reasonable timeframe to ensure updates are properly installed.

3.3.6. High severity vulnerabilities must be addressed as a matter of priority.

3.4. Monitor

3.4.1. IT should subscribe to a threat information service to receive notifications of recently released patches and other software updates.

3.4.2. IT must notify the decision-making authority if vulnerabilities are not mitigated in a timely manner.

3.4.3. Every month, IT must create a report containing the status of all known vulnerabilities within the enterprise.

Deborah McPeek-McFadden, Board Chairperson	Date		