Chapter Title	**Section #**		**Subject #**
Information Technology / Information Systems	ITIS		404
Subject Title	Adopted	Last Revised	Reviewed
Risk Assessment and Management	2/28/23	1/2023	NEW

POLICY

Application

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

1. Intent

To define the organization’s approach to managing risk.

2. Purpose

The purpose of this policy is to facilitate compliance with applicable federal and state laws and regulations, protect the confidentiality and integrity of the organizations IT Resources and enable informed decisions regarding risk tolerance and acceptance.

3. Risk Assessment and Management Scope

3.1. The CFO is authorized to perform periodic information security risk assessments to determine areas of vulnerability and to initiate appropriate remediation.

3.2. The Right Door uses formal Information Security Risk Management (ISRM) programs that identify risks and implement plans to address and manage. Examples include the HIPAA risk assessment tool, the Foundational Assessment, and the Nationwide Cybersecurity Review (NCSR). In addition, custom developed risk assessments may be implemented.

3.3. The CFO is responsible for managing the Information Security Risk Management program and coordinating the development and maintenance of program policies, procedures, standards, and reports.

3.4. The ISRM program is based on risk assessment and developed in consideration of organizational priorities, staffing, and budget.

3.5. Risk assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to the organization. The results are to guide and determine the appropriate

Chapter Title Information Technology / Information Systems	**Section #** ITIS		**Subject #** 404
Subject Title **Risk Assessment and Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

management action and priorities for managing information security risks and for implementing controls to protect against these risks.

3.6. The risk assessment must include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the calculated risks against risk criteria to determine the significance of the risks (risk evaluation).

3.7. Risk assessments are performed periodically to address changes in security requirements and the risk situation (e.g., threats, vulnerabilities, impacts, risk evaluation, and data classification).

3.8. Risk assessments are to be undertaken systematically, capable of producing comparable and reproducible results. The information security risk assessment should have a clearly defined scope to be effective and should include relationships with risk assessments in other areas, if appropriate.

Deborah McPeek-McFadden, Board Chairperson	Date		