Chapter Title Information Technology / Information Systems	**Section #** ITIS		**Subject #** 409
Subject Title **Incident Response**	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 outline incident response requirements

2. Purpose

The purpose of this policy is to clearly define IT roles and responsibilities for the investigation and response of computer security incidents and Data Breaches.

3. Incident Response Scope

3.1. The IT Team detects and investigates security events to determine whether an incident has occurred, the extent, cause, and damage of incidents.

3.2. IT directs the recovery, containment and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so.

3.3. If the incident involves the unauthorized use or disclosure of PHI, IT will notify the CEO and Compliance Officer.

3.4. CFO, or designee, coordinates response with internal and external parties when existing agreements place responsibility for incident investigations on the external party.

3.5. During the conducting of security incident investigations, IT is authorized to monitor relevant IT resources and retrieve communications and other relevant records of specific users of IT resources, including login session data and the content of individual communications without notice or further approval.

3.6. Any external disclosure of information regarding information security incidents must be reviewed and approved by the CEO in consultation with the CFO, and other stakeholders as appropriate.

Chapter Title Information Technology / Information Systems	**Section #** ITIS		**Subject #** 409
Subject Title **Incident Response**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

3.7. IT coordinates with law enforcement, government agencies and relevant Information Sharing and Analysis Centers (ISACs) in the identification and investigation of security incidents. IT is authorized to share external threat and incident information with these organizations that does not identify any member of The Right Door.

4. Review and Adjudication

4.1. All members of the Right Door are responsible for promptly reporting any suspected or confirmed security incident involving data or an associated information system, even if they have contributed in some way to the event or incident. Reports are to be made to the IT Department. Members of the Right Door must cooperate with incident investigations, and may not interfere, obstruct, prevent, retaliate against, or dissuade others from reporting an incident or cooperating with an investigation.

4.2. IT is responsible for responding to, and periodic reporting on, Low Severity security incidents. High Severity incidents reported to or discovered by IT are to be promptly reported to the MS-ISAC SOC for assistance. IT along with the MS-ISAC SOC is responsible for responding to High Severity.

Deborah McPeek-McFadden, Board Chairperson	Date		