Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		408
Subject Title **Mobile Device 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

The purpose of this policy is to define the use of mobile devices when accessing IT Resources.

3. Scope of Mobile Device Management

Users must adhere to this policy and all policies while using mobile devices to access IT Resources.

3.1. Organization-Owned Mobile Devices

3.1.1. Mobile devices issued to employees of the organization are to be used for business purposes only and remain the property of The Right Door.

3.1.2. Mobile devices owned by The Right Door must be returned by departing employees to IT when leaving the organization or when the device is no longer needed to conduct business.

3.2. Bring Your Own Devices (BYOD) (when applicable)

3.2.1. When accessing IT Resources with a personal mobile device, the User must follow all IT policies and is subject to the rules governing data.

3.2.2. The Right Door does not accept liability for the maintenance, backup, or loss of data stored on Users' personal mobile devices.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		408
Subject Title **Mobile Device Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

3.2.3. Users are responsible for backing up all software and data to appropriate backup storage systems.

3.2.4. The Right Door is not liable for the loss, theft, or damage of any User's personal mobile devices, including but not limited to when the device is being used for business or during business travel.

3.2.5. The User's personal mobile device may be subject to disclosure in the event of litigation, and the User will be required to cooperate with the Right Door in providing access to the device for that purpose.

3.3. Terms and Conditions

3.3.1. Users of mobile devices that access IT Resources, which include non-Right Door-owned devices, must comply with the following security and risk management measures:

3.3.2. If your device is lost, stolen, or compromised, you must report it immediately to the IT Department.

3.3.3. The Information Technology department provides security and risk management software for accessing IT Resources.

3.3.4. Mandatory security and risk management software is required.

3.3.5. The Right Door does not accept liability for any damages due to the installation of the software mentioned above on non-organizational-owned devices.

3.3.6. All devices must be secured using a PIN (6-digit minimum) or other password protection.

3.3.7. All devices must enable automatic lockout for idle devices for (5) five or fewer minutes, where possible.

3.3.8. All devices must have remote wipe capability installed and enabled, where possible.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		408
Subject Title **Mobile Device Management**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

3.3.9. Users of mobile devices that access IT Resources will be subject to remote locking or data wiping if lost, stolen, or otherwise compromised. To implement these security requirements, Users may contact IT Help Desk.

3.3.10. Any device used for business must not be shared with anyone.

3.4. User Code of Conduct

3.4.1. Users of mobile devices that access IT Resources are expected to take reasonable measures to protect the security and integrity of that data, including:

3.4.1.1. Following the rules in the Acceptable Use Policy,

3.4.1.2. Protecting the physical security of the device,

3.4.1.3. Maintaining the software configuration of the device (i.e., operating system or installed applications),

3.4.1.4. Installing an up-to-date and secure operating system and application software as they become available, Following the IT policies of The Right Door.

3.4.1.5. Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes, or security setting changes and working with the IT Help Desk to test and validate any configuration, application, or settings.

Deborah McPeek-McFadden, Board Chairperson	Date		