Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		204

Subject Title **Remote Access Policy**	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 Define requirements of remote Access Provision

2. Purpose

The purpose of this policy is to define the rules and requirements for connecting to the organization's network, both on-premises or cloud-based, from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Obligations of Employees

3.1. It is the responsibility of employees, contractors, vendors and agents with remote access privileges to our corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

3.2. General access to the Internet for recreational use through our company network is strictly limited to our employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing our network from a personal computer, Authorized Users are responsible for preventing access to any company computer resources or data by non-Authorized Users.

3.3. Performance of illegal activities through our company network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see our Acceptable Use Policy. Authorized Users will not use our networks to access the Internet for outside business interests.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		204
Subject Title **Remote Access Policy**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

4. Connection Procedures

4.1. Secure remote access to on site resources will be strictly controlled with encryption through our Virtual Private Networks (VPNs) and strong pass-phrases.

4.2. Authorized Users shall protect their login and password, even from family members.

4.3. While using our corporate owned computer to remotely connect to our corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.4. Use of external resources to conduct our company business must be approved in advance by the CFO.

4.5. All hosts that are connected to our company's internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers.

4.6. Personal equipment used to connect to our company's networks must meet the requirements of company owned equipment for remote access - and be approved by the CFO.

5. Compliance

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring (if applicable), business tool reports, internal and external audits, and/or inspection.

An employee found to have violated this policy may be subject to disciplinary action.

6. Exceptions

Any exception to the policy must be approved by the CFO.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		204
Subject Title **Remote Access Policy**	Adopted 2/28/23	Last Revised 1/2023	Reviewed NEW

Deborah McPeek-McFadden, Board Chairperson	Date		