Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		201
Subject Title	Adopted	Last Revised	Reviewed
Account and Credential Management / Authorized Access	2/28/23	1/20/23	2/26/24

POLICY

Application

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

1. Intent

   Account and credential management is the process of creating, provisioning, using, and terminating accounts and credentials in the enterprise. The Account and Credential Management Policy provides the processes and procedures for governing accounts and credentials.

2. Purpose

   2.1. Responsibility - The IT department is responsible for all account and credential management functions. This information is relayed to other business units within the organization as required or needed. IT is responsible for informing all users of their responsibilities in the use of any accounts and credentials assigned to them.

   Users are responsible for using their accounts in a manner consistent with organization's acceptable use policy.

   2.2. Exceptions - Exceptions to this policy are likely to occur. Requests for exception must be made in writing and must contain:

   2.2.1. The reason for the request,
   2.2.2. Risk to the enterprise of not following the written policy,
   2.2.3. Specific mitigations that will not be implemented,
   2.2.4. Technical and other difficulties, and
   2.2.5. Date of review.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		201
Subject Title Account and Credential Management / Authorized Access	Adopted 2/28/23	Last Revised 1/20/23	Reviewed 2/26/24

3. Requirements

3.1. Onboarding

3.1.1. IT must maintain procedures for modifying access, permissions, and roles to user accounts.

3.1.2. Newly created accounts must be represented within this process.

3.1.3. Changing user roles must be included in this process.

3.1.4. The permissions granting process must enforce the principle of least privilege.

3.1.5. Unnecessary default or generic accounts must be changed before a new system is deployed into the enterprise.

3.2. Account Creation

3.2.1. IT must develop procedures for creating accounts and assigning privileges.

3.2.2. Administrator privileges must only be provided to administrative accounts.

3.2.2.1. Administrator and privileged accounts must only be used for appropriate installation and maintenance tasks; not for daily use.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		201
Subject Title Account and Credential Management / Authorized Access	Adopted 2/28/23	Last Revised 1/20/23	Reviewed 2/26/24

3.2.2.2. Administrator accounts must be unique and assigned to a specific individual, unless technically constrained by a system or application.

3.2.3. It is the responsibility of IT to maintain an account inventory.

3.2.4. At a minimum the account inventory must contain the following data for each account:

3.2.4.1. Person's name
3.2.4.2. Account name
3.2.4.3. Date of employment start and stop
3.2.4.4. Business unit
3.2.4.5. Account status (i.e., enabled, disabled)

3.2.5. All enabled accounts within the inventory must be regularly validated once a quarter, or more frequently

3.3. Credential Creation and Issuance

3.3.1. All passwords must be unique.
3.3.2. Passwords created by users must not also be used for personal accounts.
3.3.3. Passwords must not be shared by users.
3.3.4. Passwords created for use with multifactor authentication must be at a minimum 8 characters long.
3.3.5. Passwords created for use without multifactor authentication must be at a minimum 14 character long.

3.4. Account and Credential Usage

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		201
Subject Title Account and Credential Management / Authorized Access	Adopted 2/28/23	Last Revised 1/20/23	Reviewed 2/26/24

3.4.1. All users must use multifactor authentication to access externally facing applications.
3.4.2. All users must use multifactor authentication to access applications hosted by a third-party service provider, where supported.
3.4.3. All remote users must use multifactor authentication to access internal systems and applications.
3.4.4. Multifactor authentication is required for all administrative accounts on all enterprise assets, whether managed on-site or through a third-party provider.
3.4.5. All default user passwords must be changed at the first login.

3.5. Monitor

There are no safeguards that support this portion of the account and credential management process. The CFO may monitor processes used in the account management process.

3.6. Modify Access

3.6.1. All user accounts that have not been accessed within 45 days of creation must be disabled.
3.6.2. Accounts of individuals on extended leave, as defined by human resources, must be disabled.
3.6.3. The Account Creation and Account Termination procedures must include the ability to change a user's role.

3.7. Account Termination

IT must develop procedures for revoking account access.

Chapter Title	Section #		Subject #
Information Technology / Information Systems	ITIS		201
Subject Title Account and Credential Management / Authorized Access	Adopted 2/28/23	Last Revised 1/20/23	Reviewed 2/26/24

Nancy Patera, Board Chairperson	Date		