Reference	Clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3	**Version**	1	NF
Distribution	Executive Team	**Document Type:**	Policy	
Responsible	Andrew Lewis	**Created**	8 February 2022	
Author	Paul Cavicchia	**Review Date**	30 June 2024	
File Path				

PASSWORD POLICY

Policies & Procedures

Version	Date	Author	Reviewed by	Review Date	Summary of Changes
1	8 Apr 2021	Karen Prelovsky	Andrew Lewis	08/04/2024	Initial Version
					This policy extends to CTI RTO

Approved: ___________________________________

Andrew Lewis (CEO)

Date: ______________________

Policy

1 Policy Statement

It is imperative that users practice due diligence in controlling access to their systems by protecting their user accounts with passwords that are not easily guessed or deduced. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire corporate network of Newfurn. As such, all employees (including contractors and vendors with access to systems of Newfurn) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords

2 Purpose

The purpose of this policy is to ensure that security practices are introduced and maintained by all employees with respect to password-protected information infrastructure.

3 Scope

IT Assets

The policy is applicable to all IT systems and services.

Document Control

The Password Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document.

Distributions and Maintenance

The Password Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document will be with the Executive Assistant to the CEO.

4 Privacy

The Password Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

5 Responsibility

The Password Policy shall be implemented by the CEO.

CEO

- Provides management oversight of the process for administering passwords for Newfurn systems
- Publishes and maintains policy documentation for the creation, safeguarding, and control of the passwords
- Grants access and reviews access every year to determine the continued need for access; and, if the need continues, re-approves through submission ticketing system.
- Approves access to supervisor passwords and passwords for similar privileged accounts used on Newfurn’s network

IT Contractor - SimpleBiz

- Communicates to the users the system access and password requirements outlined in this policy
- Informs Newfurn’s HR Manager when access is to be removed
- Immediately informs Newfurn’s HR Manager if it is suspected that password has been compromised

- Issues and manages passwords for systems and applications under their control in accordance with the policy described below
- Issues passwords for privileged accounts to the primary system administrator and no more than one designated alternate system administrator; these passwords shall be changed when necessary due to employment termination, actual or suspected password compromise

Users

- Understand their responsibilities for safeguarding passwords
- Use Newfurn's data in accordance with job function and company policies
- Understand the consequences of their failure to adhere to statutes and policy governing information resources
- Immediately notify the supervisor if it is suspected that password has been compromised

6 Policy

General

a) Password policy shall ensure that all user accounts are protected by strong passwords and that the strength of the passwords meets the security requirements of the system.
b) The concept of aging shall be used for passwords. Passwords on their expiry shall cease to function.
c) Users shall be educated about password protection and the password policy shall be implemented to ensure that users follow best practices for password protection.
d) IT systems shall be configured to prevent password reuse.
e) For critical information systems, account lockout strategy shall be defined. This shall be based on a risk analysis of the system as well as the costs to be incurred in case such a strategy is implemented.

Access Authorization Requirements

Access to Newfurn's resources shall be controlled and shall be based on an approval by the CEO.

Individuals shall be granted access only to those information systems necessary for the performance of their official duties; users must receive the CEO and CFO's approval prior to being granted access to Newfurn's information resources. This requirement includes contracted employees and all other non-Newfurn personnel who have been granted access.

Passwords shall be used on all Newfurn automated information systems to uniquely identify individual users.

Passwords shall not be shared with, used by, or disclosed to others; generic or group passwords shall not be used.

To preclude password guessing, an intruder lock-out feature shall suspend accounts after specified invalid attempts to log on; manual action by a security system administrator is required to reactivate the ID.

Password Parameters

All user and system passwords, even temporary passwords set for new user accounts, should meet the following characteristics:

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	100 days
Minimum password age	0 days
Minimum password length	7 characters (contain a special character, upper and lower case)
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Screensaver timeout	15 minutes

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	20 invalid logon attempts
Reset account lockout counter after	30 minutes
Passwords may not contain	The user’s account name value or entire display name, both checks are not case sensitive.
The passwords contain characters from three of the following categories	Uppercase letters, lowercase letters, base 20 digits, special characters (~!@#$%^&*_-+=’|\(){}[]”’<>,.?/) any Unicode character that’s categorised as an alphabetic character but isn’t lowercase or uppercase.

Email – IT Health Report

All head office and store emails are on Microsoft 365	
Email Spam protection is provided by MailGuard	
Multifactor Authentication has been enforced for:	• Executives • Directors • General Managers

Password and Account Security

Lockout policy will be implemented for unsuccessful login attempts.

Screen-saver password must be enabled after 15 minutes of inactivity of the user. Users must not be allowed to change the inactivity time.

Administrative account passwords must be changed promptly upon departure of personnel (mandatory or voluntary) or suspected compromise of the password. User accounts will be disabled promptly upon departure of personnel (mandatory or voluntary). Users should immediately change their password if they suspect it has been compromised.

Passwords may be not visible on a screen, hardcopy printouts, or any other output device

7.Enforcement

Unauthorized personnel is not allowed to see or obtain sensitive data. Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.