Family Law Software
A CENTERBASE COMPANY

Password Policy

1. Purpose and Scope

1.1 Purpose

This policy defines the minimum security requirements for the selection, use, and management of passwords and other secret authentication mechanisms to protect organizational information systems and data from unauthorized access.

1.2 Scope

This policy applies to all user, service, and system accounts across all organizational systems and networks.

2. Password Complexity and Management

2.1 Password Complexity Requirements

All user and administrative passwords must adhere to the following minimum complexity requirements, which are technically enforced by all authentication systems:

- **Minimum Length:** 12 characters (14 characters for privileged/administrator accounts).
- **Complexity Enforcement:** Must use a combination of at least three of the following four character types:
    - **Uppercase letters** (A-Z)
    - **Lowercase letters** (a-z)
    - **Numbers** (0-9)
    - **Symbols** (e.g., ! @ # $ % ^)
- **History Check:** Passwords must not be one of the user's last ten used passwords.

2.2 Password Change Intervals

To manage risk from potential credential compromise, passwords must be changed at regular intervals:

- **Standard User Accounts:** Passwords must be changed at least every **90 days**.
- **Privileged/Administrative Accounts:** Passwords must be changed at least every **60 days**.

3. Management of Authentication Information

3.1 Default and Temporary Credentials

The organization mandates strict management of initial and temporary authentication information:

- **Default Secret Authentication Information:** Any **default vendor passwords or authentication information** on new hardware, software, or cloud assets **must be changed or disabled before the first use** or connection to the company network.
- **Temporary Secret Authentication Information:** Any temporary password or initial credential issued to a user (e.g., new hire onboarding, password reset) **must be reset upon the first log in** to company assets. The system must force the user to set a new, complex password immediately.

3.2 Secret Authentication Mechanism Resets

Any process for resetting a user's password, Multi-Factor Authentication (MFA) token, or other **secret authentication mechanism requires validation that the user is indeed authorized** to make the request.

- **Verification:** The IT Service Desk or automated system must perform a multi-point verification (e.g., verification code sent to a known email/phone, security questions, or call-back to a pre-registered number) before processing any secret authentication reset.
- **Logging:** All password and MFA reset events must be logged, including the method of user validation used.

4. Policy Review

This policy will be formally reviewed on an annual basis to ensure that the standards for complexity, change intervals, and reset procedures remain effective against evolving cyber threats.