Family Law Software
A CENTERBASE COMPANY

**Authentication Information Management Policy**

## 1. Purpose and Scope

### 1.1 Purpose

This policy establishes the formal process for the secure **management, use, and protection of all secret authentication information** used within the organization. The goal is to minimize the attack surface, reduce password-related risks, and ensure the integrity of the authentication process.

### 1.2 Scope

This policy applies to all employees, contractors, and systems that utilize or manage authentication information for access to the organization's networks and information systems.

## 2. Management of Secret Authentication Information

### 2.1 Definition of Secret Authentication Information

Secret authentication information includes any data or item used to verify a user's identity. This includes, but is not limited to:

- **Usernames** and User IDs.
- **Passwords** and Passphrases.
- **Electronic Certificates** (e.g., PKI private keys).
- **Multi-Factor Authentication (MFA)** tokens, codes, or seeds.
- **Biometric Data** used for verification.

### 2.2 User Awareness and Confidentiality

A formal training and awareness program must be in place to **identify and inform all users** of the following:

- The critical need to keep all secret authentication information **confidential and secure**.
- The different **types of authentication information** used (e.g., corporate passwords, MFA codes, system keys).
- Proper handling, storage, and non-disclosure requirements for all authentication information.

**2.3 Process for Managing Authentication Information**

The organization follows a developed process for managing the lifecycle of authentication information, which includes:

- Mandating the use of a **centralized Password Manager** for storing and sharing any shared system credentials.
- Enforcing the **Access Control Policy**f or password complexity and rotation.
- Securely provisioning and revoking electronic certificates and hardware tokens.

**3. Authentication Methods and Attack Surface Reduction**

**3.1 Authentication Strategy for Attack Surface Reduction**

The organization employs authentication methods designed to **manage the attack surface** and mitigate risks associated with password compromise.

- **Single Sign-On (SSO):** SSO is the preferred method for all internal applications to **reduce the number of identical passwords used** by users across disparate systems.
- **MFA Mandate:** Multi-Factor Authentication is required for all remote access and all systems handling sensitive or mission-critical data.

**3.2 Rules for Multi-Factor Authentication (MFA)**

The authentication process includes the following rules for managing and using MFA:

- **Enrollment:** All users with access to MFA-protected systems must be enrolled immediately upon account creation.
- **Approved Methods:** Only security-approved MFA methods (e.g., mobile authenticator apps, FIDO2 security keys) are permitted. SMS-based MFA is discouraged where more secure options are available.

- **Loss/Compromise:** Users must immediately report the loss or compromise of any MFA device/token to the IT Service Desk for immediate revocation and re-provisioning.

**3.3 Management of Temporary and Default Credentials**

The organization implements methods to manage temporary and default authentication information:

- **Temporary Authentication Information:** Any temporary password or initial login credential issued to a new user **must be immediately expired** and require a mandatory, strong password change upon first use.
- **Default Vendor Passwords:** On all new systems, hardware, or software installations, the default vendor password or authentication setting **must be changed or disabled immediately** before the system is connected to the production network.

**4. Policy Review and Validation**

The process for authentication information, including the effectiveness of the methods used (e.g., password length, MFA adoption rate), will be **reviewed at least annually** by the Security Team to validate that authentication methods remain effective against current threat landscapes and to ensure compliance with the Access Control Policy.