Family Law Software
A CENTERBASE COMPANY

User Endpoint Device Policy

1. Policy Statement

This policy defines the security requirements for all user endpoint devices, including desktops, laptops, mobile phones, and tablets, that are used to access Family Law Software (the "Company") information systems and data. The purpose of this policy is to protect the Company's assets from threats originating from user devices, whether company-owned or personally-owned (BYOD), and to ensure data confidentiality, integrity, and availability.

2. Scope and Responsibility

This policy applies to all employees, contractors, and third parties who use an endpoint device to access the Company's network, applications, or data.

- **Users** are responsible for complying with this policy.
- **The IT Department** is responsible for implementing and managing the technical controls required by this policy.

3. General Requirements

All endpoint devices must adhere to the following security requirements:

- **Endpoint Security Software:** All devices must have Company-approved endpoint protection software (e.g., antivirus, anti-malware, endpoint detection and response) installed and operational.
- **Operating System Updates:** Operating systems must be kept up-to-date with the latest security patches and updates. Users are responsible for installing updates promptly as they are released.
- **Password/Passcode Protection:** All devices must be protected by a strong password or passcode, with automatic screen lock enabled after a period of inactivity.

- **Full Disk Encryption:** All company-owned laptops and desktops, as well as personally-owned devices handling sensitive company data, must have full disk encryption enabled.
- **Secure Network Connection:** Users must only connect to the Company network via a secure, approved method (e.g., corporate VPN). Use of public Wi-Fi networks without a VPN is prohibited when accessing sensitive company data.

4. Company-Owned Devices

- Company-owned devices are subject to regular audits and monitoring by the IT Department to ensure compliance.
- Users must not install unapproved software on company-owned devices.
- These devices should be used primarily for business purposes.

5. Bring Your Own Device (BYOD) Requirements

- Personally-owned devices are permitted to access the Company network only after the user agrees to and complies with the BYOD policy, which is a supplement to this policy.
- Users must consent to allowing the Company to install necessary management software on their personal device to enforce security controls, such as remote wipe capabilities in the event the device is lost or stolen.
- The Company reserves the right to wipe all data from a personal device that has been used to access company systems if the device is lost, stolen, or if the user’s employment is terminated.

6. Incident Response

Users must immediately report the loss or theft of any device containing Company data to the IT Department. This allows for immediate action to protect company information, such as remotely wiping the device.

7. Review

This policy will be reviewed annually.

8. Policy Violations

Violations of this policy may result in disciplinary action, up to and including termination of employment. Unauthorized devices may be removed from the network without warning.