Family Law Software
A CENTERBASE COMPANY

Information Security Policy

1. Introduction

This policy establishes the rules and responsibilities for the protection of all information assets belonging to Family Law Software. The goal is to ensure the confidentiality, integrity, and availability of our information and systems, and to comply with legal, regulatory, and contractual obligations.

2. Scope

This policy applies to all employees, contractors, partners, and any third parties who access or use the Company's information systems or data, regardless of location or device. It covers all information assets, whether in digital or physical form, including hardware, software, data, and intellectual property.

3. Policy Principles

- **Confidentiality:** We will protect sensitive information from unauthorized access and disclosure.
- **Integrity:** We will ensure that information is accurate, complete, and reliable, and that it is not subject to unauthorized modification.
- **Availability:** We will ensure that information and systems are accessible to authorized users when needed for business operations.
- **Compliance:** We will comply with all relevant legal, regulatory, and contractual requirements.

4. Policy Sections

- **4.1. Access Control:**

- Access to information assets will be granted on a "need-to-know" and "least privilege" basis.
- All users will be assigned unique login credentials.
- Access rights will be reviewed and revoked upon job termination or change in role.

- **4.2. Acceptable Use of Assets:**
  - Users must adhere to the **Acceptable Use Policy** for all Company-owned and personal devices used for business purposes.
  - Prohibited activities include unauthorized software installation, illegal activities, and misuse of Company resources.
- **4.3. Data Classification and Handling:**
  - All information will be classified and handled according to its sensitivity level, as defined in the **Information Classification and Labelling Process Policy**.
  - Information must be stored, transmitted, and disposed of in a manner consistent with its classification.
- **4.4. Incident Management:**
  - All security incidents, including suspected data breaches, system compromises, or policy violations, must be reported immediately to the IT Security team.
  - The Company will maintain and follow an incident response plan to address and recover from security events.
- **4.5. Physical Security:**
  - Physical access to facilities, data centers, and equipment rooms will be restricted to authorized personnel.
  - Assets will be secured to prevent theft, damage, or unauthorized access.
- **4.6. Third-Party Management:**
  - Third-party vendors and partners who handle Company data must undergo a security assessment and agree to meet our security standards.

    - Contracts will include security clauses that define responsibilities and liability.

- **4.7. Training and Awareness:**
    - All users will receive regular security awareness training to understand their responsibilities under this policy.
    - Training will cover topics such as phishing, social engineering, and safe data handling practices.

5. Policy Enforcement and Review

Violations of this policy will result in disciplinary action, up to and including termination of employment. This policy will be reviewed at least annually to ensure it remains relevant and effective.

6. Effective Date

This document is effective as of December 1, 2025.