Family Law Software
A CENTERBASE COMPANY

Information Security Awareness and Training Program

This document outlines the organization's policy for ensuring all staff are aware of, and committed to, adhering to critical information security and confidentiality requirements.

1. Scope and Objectives

The **Awareness and Training Program** is mandatory for all employees, contractors, temporary staff, and third-party personnel who access the organization's information systems or confidential data.

Objectives:

1. Ensure all personnel are aware of their responsibilities regarding the protection of organizational assets and confidential data.
2. Provide annual training on current threats and security policies.
3. Establish an auditable record of each individual's commitment to these policies.

2. Program Components

2.1. Initial and Annual Training Sessions

All staff must participate in annual information security awareness sessions.

- **New Hires:** Must complete the mandatory Information Security Training within 14 days of their start date. Access to critical systems will be restricted until completion.
- **Annual Refreshers:** All personnel must complete an annual refresher training session, typically scheduled during the first quarter of the fiscal year. This training covers current threats, compliance updates, and policy refreshers.

2.2. Core Content Awareness

Training and awareness materials must ensure **staff are aware of the following key documents and concepts** relevant to their security obligations:

Document/Concept	**Required Awareness Focus**
Information Security Policies	Acceptable Use Policy, Data Classification, Password Standards, Incident Reporting Procedures.
Code-of-Conduct	Ethical handling of company resources, prohibitions against misuse of systems, and professional behavioral expectations.
Non-Disclosure Agreements (NDAs)	Obligations for protecting proprietary business information, trade secrets, and internal strategies.
Confidentiality Agreements	Procedures for handling client, partner, and personally identifiable information (PII) to meet regulatory and legal duties.

3. Annual Acknowledgment and Compliance

3.1. Annual Policy Statement

In conjunction with the annual information security awareness sessions, **staff should sign an annual statement that they understand the policies.**

1. **Acknowledge and Attest:** At the conclusion of the annual training session, all personnel are required to electronically sign (or physically sign, if required) a formal statement.
2. **Statement Content:** The statement attests that the individual has:
   - Completed the mandatory annual Information Security Awareness Training.
   - Read, understood, and agreed to comply with all relevant **Information Security Policies**, the **Code-of-Conduct**, and all applicable **Non-Disclosure or Confidentiality Agreements**.
   - Understands the consequences of policy violation, up to and including disciplinary action or termination.

3.2. Record Keeping and Audit

- The Human Resources (HR) and Information Security departments are jointly responsible for maintaining a definitive record of all completed training and signed annual statements.
- These records must be retained for the duration of the individual's employment plus a minimum of three (3) years to satisfy regulatory and audit requirements. Failure to complete the annual requirements will result in immediate suspension of system access until compliance is confirmed.