Family Law Software
A CENTERBASE COMPANY

Security Assessment Plan

1. Introduction

The purpose of this Security Assessment Plan is to establish a systematic process for evaluating the effectiveness of Family Law Software's information security controls. This plan outlines the methodology, frequency, and responsibilities for monitoring and measuring control performance to ensure that risks to information assets are managed to an acceptable level

---

2. Scope

This plan applies to all information security controls implemented to protect Family Law Software's information systems and data. It covers controls related to:

- **Administrative Controls:** Policies, standards, and procedures (e.g., Acceptable Use Policy, Information Classification Policy).
- **Technical Controls:** System-level security measures (e.g., encryption, access controls, network security).
- **Physical Controls:** Security measures for physical assets and facilities (e.g., data centers, offices).

---

3. Assessment Activities

The effectiveness of security controls will be measured through a combination of the following activities:

- **Vulnerability Scanning: Automated scans** will be conducted regularly on both internal and external networks to identify known vulnerabilities.
- **Penetration Testing:** An **ethical hack** will be performed by an internal or external team to simulate a real-world attack and identify exploitable weaknesses. This will be conducted at least annually.

- **Risk Assessments:** Regular **risk assessments** will be performed to identify new threats and vulnerabilities, evaluate existing controls, and determine if they are adequately mitigating risk.
- **Control Audits: Periodic reviews** of control implementations and documentation will verify compliance with policies and standards. This includes checking logs, reviewing user access lists, and confirming that security patches are applied.
- **Continuous Monitoring:** Real-time monitoring tools will be used to collect data on system activity, network traffic, and security events to detect and respond to threats as they occur.

---

4. Metrics and Reporting

Key performance indicators (KPIs) and metrics will be used to measure control effectiveness and communicate risk posture to leadership. Examples include:

- **Time to Remediate:** The average time from when a vulnerability is discovered to when it's fully remediated.
- **Compliance Rate:** The percentage of systems that are compliant with security policies (e.g., all laptops have disk encryption enabled).
- **Vulnerability Density:** The number of high-risk vulnerabilities per system.
- **Incident Response Time:** The average time from when a security incident is detected to when it is contained.

Reports on these metrics will be generated on a quarterly basis and reviewed by the executive team.

---

5. Roles and Responsibilities

- **Security Team:** Responsible for executing the assessment activities, analyzing results, and reporting on control performance.
- **System Owners:** Accountable for the security of their systems and for ensuring that remediation actions are completed.
- **Leadership:** Responsible for reviewing reports, approving risk tolerance levels, and allocating resources for security improvements.