Family Law Software
A CENTERBASE COMPANY

Incident Management Plan

1. Introduction and purpose

This document outlines the procedures for the Family Law Software Incident Response Team (IRT) to prepare for, identify, respond to, and recover from security incidents or events. The plan ensures a consistent and effective approach, minimizing the impact of incidents on the organization's business operations, reputation, and data integrity.

Goals of the incident management plan:

- Provide a clear, repeatable, and scalable process for incident response.
- Define roles and responsibilities to ensure a coordinated and rapid response.
- Establish clear communication channels and procedures for all stakeholders.
- Ensure all incident management activities are accurately logged for analysis and reporting.
- Incorporate lessons learned to continuously improve the organization's security posture.

2. Incident reporting for staff

All staff members are responsible for recognizing and reporting potential security events or weaknesses. The rapid reporting of potential incidents is critical to minimizing damage.

How to report a security event or weakness:

- **Initial notification:** If you suspect a security event (e.g., a malware infection, suspicious email, or unauthorized access), immediately report it to the IT Help Desk at support@familylawsoftware.com.
- **Information to provide:** The reporting individual should be prepared to provide the following details:
    - Their name and contact information.
    - The date and time the event was noticed.
    - A description of the event or suspicious activity.

    - The location of the event (e.g., which device or system is affected).
    - Any actions taken (e.g., disconnected from the network).

3. Incident response process

The Incident Response Team follows a systematic, multi-phase process to manage security incidents, based on the NIST framework.

Phase 1: Preparation

- **Proactive measures:** The IRT prepares for incidents by maintaining a secure environment, training staff, and performing regular risk assessments.
- **Response infrastructure:** The team ensures that all necessary communication tools (e.g., conference bridge, secure chat), resources (e.g., forensic software), and incident management systems are in place and ready for use.
- **Documentation:** Incident handling systems are maintained for event investigation and tracking.

Phase 2: Identification and analysis

- **Detection:** Security monitoring tools (e.g., SIEM, EDR) and staff reports are used to detect potential incidents.
- **Triage and analysis:** The IRT confirms whether an event is a genuine security incident, its severity, and its potential impact. This includes gathering relevant system logs and other data.
- **Prioritization:** Incidents are prioritized based on business impact, system criticality, and confidentiality of data involved. Prioritization helps the team allocate resources effectively.
- **Declaration:** Based on the analysis and prioritization, the IRT formally declares a security incident and activates the response plan.

Phase 3: Containment, eradication, and recovery

- **Containment:** The team takes immediate action to limit the incident's scope and prevent further damage. This may involve isolating affected systems or accounts.
- **Eradication:** The root cause of the incident is identified and eliminated. This could involve removing malware, patching vulnerabilities, or deleting compromised accounts.

- **Recovery:** Once the threat is eradicated, affected systems and data are restored to normal operation. This often involves restoring from clean backups and implementing additional security measures.

Phase 4: Post-incident activity (Lessons learned)

- **Post-mortem review:** A meeting is held with all relevant responders to analyze the incident and the effectiveness of the response.
- **Incident report:** A formal report is created documenting what happened, the response actions taken, and the lessons learned.
- **Process improvement:** Based on the review, the IRT updates security procedures, policies, and the incident management plan to prevent similar future incidents.

4. Logging incident management activities

Accurate and comprehensive logging is essential for post-incident analysis, reporting, and legal purposes.

Required logging:

- **Incident tracking system:** All incidents are logged and tracked in the designated incident management platform.
- **Timeline of events:** A chronological record is maintained from the moment of detection until the incident is closed.
- **Evidence preservation:** Procedures must be followed for the secure collection and preservation of digital evidence (e.g., logs, disk images) to support potential forensic investigations.
- **Action log:** All actions taken by the response team are logged in detail, including the time, who performed the action, and the reason.

5. Relevant stakeholders

An effective incident response plan requires cooperation across various departments. The following stakeholders should receive a copy of this plan and be aware of their responsibilities:

- **Executive management:** The Chief Executive Officer (CEO), Chief Operating Officer (COO), and Chief Financial Officer (CFO) need to understand the potential impact of an incident and approve strategic decisions.

- **IT leadership and security team:** The Chief Information Security Officer (CISO) or Head of IT leads the technical response and ensures the incident plan is executed effectively.
- **Human Resources (HR):** HR manages employee-related issues during an incident, including communication, disciplinary actions, or staffing needs.
- **Legal department:** The legal team provides guidance on regulatory reporting requirements, potential legal risks, and documentation.
- **Public Relations (PR) and Communications:** The PR team is responsible for external communications with customers, partners, and the media.
- **Department managers:** Managers of affected departments need to understand potential business impacts and communicate with their teams.
- **External parties:** This may include Managed Security Service Providers (MSSPs) or external forensic experts involved in the response.