Family Law Software
A CENTERBASE COMPANY

Incident Recovery Plan

1. Introduction and purpose

This document outlines the organization's approach to recovering from a security incident, with the goal of restoring information systems and business functions to normal operations as quickly and effectively as possible. It is a component of the broader Incident Response Plan and is designed to execute contingency activities once the immediate threat has been contained and eradicated.

Key objectives:

- Minimize the incident's impact on business operations, data, and reputation.
- Restore mission-critical systems and functions based on defined recovery time objectives (RTO) and recovery point objectives (RPO).
- Ensure the integrity and functionality of all systems and data post-incident.
- Incorporate lessons learned to prevent future incidents and improve recovery procedures.

2. Recovery capabilities roadmap

The following roadmap details the strategic approach to building and maintaining a robust recovery capability.

Phase 1: Planning and preparation (Ongoing)

- **Business Impact Analysis (BIA):** Conduct and regularly update a BIA to identify and prioritize critical business functions, the systems that support them, and the maximum tolerable downtime (MTD) for each.
- **Contingency Plan Development:** Create or update information system contingency plans (ISCPs) for all critical systems, ensuring they contain detailed recovery procedures.
- **Backup Strategy:** Implement and enforce a comprehensive backup strategy, including routine, automated backups of critical systems and data. Encrypt all backup data and store at least one copy offsite or in the cloud.

- **Alternate Facilities:** Identify and maintain alternate processing sites (hot, warm, or cold sites) based on the organization's recovery time objectives and budget constraints.

Phase 2: Restoration and validation (Execution)

- **Contingency Plan Activation:** Use the findings from the incident's containment phase to activate the appropriate ISCP.
- **System and Data Recovery:** Restore hardware, operating systems, and applications from clean, verified backups.
- **Security Validation:** Before bringing systems back online, perform a security scan to ensure all malicious artifacts have been removed and any exploited vulnerabilities have been patched.
- **Functionality Testing:** Conduct thorough testing to confirm that restored systems and applications are functioning correctly and that data integrity has been maintained.

Phase 3: Operationalization and Improvement (Post-incident)

- **Post-Mortem Review:** Hold a formal lessons-learned session involving all relevant teams to review the incident and the recovery process.
- **Update Plans:** Incorporate insights from the post-mortem review into the ISCP, incident response plan, and other relevant security procedures.
- **Training and Exercises:** Use the lessons learned to update training for all employees and to create new tabletop or operational exercises to test the improved procedures.
- **Continuous Improvement:** Implement a process for continuous assessment and updating of the recovery roadmap to adapt to new technologies and threats.

3. Information system contingency plan activities

The organization maintains individual contingency plans for critical information systems. These plans are regularly tested and updated to reflect changes in the system's architecture, dependencies, and business requirements.

Key activities include:

- **Notification and Assessment:** The Incident Response Team assesses the incident's impact and determines the necessary ISCP to activate.

- **Resource Mobilization:** The designated recovery team retrieves backup media and moves to the identified recovery location, if necessary.
- **System Restoration:** Following the detailed procedures in the ISCP, the team restores systems, configurations, and data.
- **Functional Testing:** The system and business owners verify functionality to ensure the system is ready for normal operation.
- **Reconstitution:** Activities to return the system to normal operating conditions, including migrating back to the primary site if an alternate location was used.

4. Incorporating lessons learned

To ensure a cycle of continuous improvement, the organization systematically integrates lessons learned from incident handling into all recovery-related activities.

Procedure for lessons learned:

1. **After-Action Report:** Following every significant incident, the IRT generates an after-action report that documents the timeline, response actions, and identifies what worked and what didn't.
2. **Stakeholder Briefing:** The IRT briefs relevant stakeholders, including management, on the incident and the findings from the after-action report.
3. **Procedure Review:** The IRT and system owners review and revise relevant recovery procedures based on the lessons learned. This may involve updating backup schedules, testing protocols, or system configurations.
4. **Training Update:** Training materials and exercise scenarios are updated to reflect the lessons learned, ensuring all personnel are aware of the new and improved procedures.
5. **Testing and Validation:** Updated recovery plans are tested through drills or tabletop exercises to validate the effectiveness of the changes before a real incident occurs.

5. Recovery roadmap for organizational missions and business functions

Recovery efforts prioritize restoring critical business functions based on the BIA. The following steps guide this process:

1. **Identify Critical Functions:** Begin by identifying the business functions and processes with the highest priority, as determined by the BIA.

2. **Assess Dependencies:** Map the information systems that support each critical function and identify any interdependencies.
3. **Prioritized Recovery:** The recovery plan prioritizes the restoration of systems that support the highest-priority business functions, starting with the most critical.
4. **Phased Restoration:** A phased approach is used to restore operations, starting with essential functions and gradually moving toward full operational capacity.
5. **Communication:** Maintain open and consistent communication with business leaders and internal stakeholders throughout the recovery process, providing updates on restoration progress and estimated timelines.