INCIDENT RESPONSE PLAN

Effective 11.25.25; Updated 2.14.26

1. Purpose

This Incident Response Plan is maintained to ensure a prompt, coordinated, and effective response to information security incidents, including events that may affect the confidentiality, integrity, or availability of systems or data. The objectives of this plan are to minimize impact, support legal and regulatory compliance, and restore normal operations as quickly as possible. This plan operates in coordination with related information security, privacy, and business continuity policies.

2. Scope

This plan applies to all systems, applications, cloud infrastructure, data, employees, contractors, and third parties acting on the organization's behalf. It includes incidents involving institutional, client, reporter, or personal data.

3. Roles and Responsibilities

- **Director of IT:** Leads incident response activities, including technical investigation, containment, remediation, and recovery.
- **General Counsel:** Oversees legal assessment, regulatory obligations, contractual notifications, and communications strategy.
- **Executive Management:** Provides decision-making support and approves material remediation or disclosure actions.
- **Third-Party Providers:** Provide specialized forensic, security, or infrastructure support under organizational supervision as needed.

4. Incident Identification and Reporting

Security incidents may be identified through system monitoring, automated alerts, user reports, third-party notifications, or routine security reviews. All suspected incidents must be reported immediately to the Director of IT for evaluation and triage.

5. Incident Classification

Incidents are assessed and classified based on their type, severity, scope, and potential impact. Classification also considers the sensitivity of affected data, the impact on systems or customers, and any applicable legal or regulatory implications.

6. Containment and Mitigation

Upon confirmation of a security incident, appropriate actions are taken to contain and mitigate risk. These actions may include isolating affected systems, revoking or resetting credentials, applying configuration changes or patches, or temporarily disabling impacted services or integrations to prevent further harm.

7. Investigation and Analysis

A documented investigation is conducted to determine the root cause of the incident, the systems and data affected, and the timeline of events. The investigation also assesses whether personal or institutional data was involved. Evidence is preserved as appropriate to support remediation efforts, legal review, regulatory requirements, or law-enforcement inquiries.

8. Notification and Communication

In the event of a confirmed security incident involving personal or institutional data, notifications are made in accordance with applicable U.S. state breach notification laws, the General Data Protection Regulation (GDPR) and other applicable non-U.S. data protection laws, relevant contractual obligations, and other applicable legal requirements. Ethics Suite notifies affected clients without undue delay after becoming aware of a Security Incident, consistent with its obligations under applicable Data Processing Agreements and data protection laws.

Where notification would impede a criminal investigation or jeopardize public or national security, notification may be delayed at the written request or direction of law enforcement, consistent with applicable law. Once any such delay is lifted, notifications are made promptly and without undue further delay.

Ethics Suite cooperates with affected clients and takes commercially reasonable steps to assist in the investigation, mitigation, and remediation of the incident. Where an incident implicates regulatory obligations in multiple jurisdictions, including under the GDPR, notifications to supervisory authorities and affected parties are made without undue delay and within applicable statutory deadlines. All notification determinations, timing, and communications are coordinated by the General Counsel in consultation with the Director of IT to ensure accuracy, consistency, and compliance.

9. Eradication and Recovery

Following containment, the underlying cause of the incident is removed, system integrity is validated, and services are restored in a controlled manner. Systems are monitored closely after recovery to confirm normal operation and to reduce the risk of recurrence. Where an incident impacts system availability or business operations, recovery activities are coordinated with the organization’s Disaster Recovery and Business Continuity Plan.

10. Post-Incident Review

After the incident has been resolved, a post-incident review is conducted to document lessons learned, evaluate the effectiveness of the response, and identify corrective actions or control improvements. Policies, procedures, or training materials are updated as necessary based on the review findings.

11. Documentation and Recordkeeping

All security incidents, response actions, communications, and outcomes are documented and retained in accordance with applicable data retention and information security policies.

12. Plan Review and Maintenance

This Incident Response Plan is reviewed at least annually and updated as needed to reflect changes in systems, threat landscape, regulatory requirements, or business operations.