IJEZIE
RISK ADVISORY

INCIDENT RESPONSE & SECURITY INCIDENT REPORTING POLICY

Governing Requirements for the identification, Escalation, and Management of Security Incidents

Ifeanyi Ijezie

Ijezie Risk Advisory | https://github.com/ijeziermf

Incident Response & Security Incident Reporting Policy

Version: 1.0

Effective Date: ________________

Policy Owner: Information Security

Review Frequency: Annual

1. Purpose

The purpose of this policy is to establish requirements for identifying, reporting, responding to, and managing information security incidents in a timely and consistent manner. This policy is intended to minimize the impact of security incidents on organizational operations, data, customers, and regulatory obligations by ensuring effective coordination, escalation, and response.

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and third parties who access or support organizational systems or data. It covers all information systems, applications, networks, and data assets owned, operated, or managed by or on behalf of the organization, including on-premises, cloud, and third-party environments.

3. Policy Statements

3.1 Security Incident Definition

- A security incident is any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of organizational systems, data, or services.
- Security incidents may include, but are not limited to, unauthorized access, malware infections, data breaches, denial-of-service attacks, loss of sensitive data, or misuse of privileges.
- Suspected security incidents shall be treated as incidents until assessed and resolved.

3.2 Incident Identification and Reporting

- All users shall promptly report suspected or confirmed security incidents to Information Security or designated reporting channels.
- Delays in reporting incidents may increase impact and hinder effective response.
- Reporting shall occur regardless of perceived severity or certainty of the incident.
- Information Security shall maintain defined reporting mechanisms and escalation paths.

3.3 Incident Response and Handling

- Security incidents shall be assessed, categorized, and prioritized based on impact and urgency.
- Incident response activities shall include containment, eradication, recovery, and post-incident analysis.
- Evidence relevant to security incidents shall be preserved in accordance with legal, regulatory, and investigative requirements.
- Incident response actions shall be documented throughout the lifecycle of the incident.

3.4 Escalation and Communication

- Security incidents with significant operational, legal, or regulatory impact shall be escalated to executive management in a timely manner.
- Legal, compliance, and communications teams shall be engaged as required based on incident severity.
- External notifications, including regulators, customers, or partners, shall be coordinated through approved channels and in accordance with applicable requirements.
- Unauthorized disclosure of incident information is prohibited.

3.5 Post-incident Review and Improvement

- A post-incident review shall be conducted following significant security incidents.
- Lessons learned shall be documented and used to improve controls, procedures, and response capabilities.
- Identified gaps or control weaknesses shall be tracked through remediation activities.
- Incident trends shall be reviewed periodically to support risk management and governance.

4. Roles and Responsibilities

Information Security

- Leads incident response activities, coordinates investigations, and maintains incident response procedures.

Executive Management

- Provides oversight, decision-making support, and resource prioritization during significant incidents.

Legal and Compliance

- Advises on regulatory, contractual, and legal obligations related to security incidents.

Users

- Report suspected incidents promptly and cooperate with investigations as required.

5. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Violations may also result in legal, regulatory, or contractual consequences. All suspected violations shall be investigated in accordance with organizational procedures.

6. Review and Maintenance

This policy shall be reviewed at least annually or upon significant changes to organizational systems, threat landscape, or regulatory requirements. Updates shall be approved by appropriate governance authorities and communicated to relevant stakeholders.

7. Framework Alignment Reference

- NIST Cybersecurity Framework: RS (Respond)
- NIST SP 800-53: IR (Incident Response), CP (Contingency Planning)
- ISO/IEC 27001: Information Security Incident Management

This policy is intended to support organizational incident response governance and security incident management and may be adapted to align with specific operational, regulatory, or business requirements.

Document Control

Document ID	IRA-IR-001
Approved By	____________________
Classification	Internal
Next Review Date	____________________