**Incident Response Policy (IRP)**

**Policy ID:** SEC-IRP-001  
**Version:** 1.0  
**Approval Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 12 months]  
**Owner:** Chief Information Security Officer (CISO)  
**Applies To:** All employees, IT/security personnel, contractors, and third parties involved in incident identification, handling, and escalation

**1. Purpose**

The purpose of this policy is to define [COMPANY NAME]’s approach to detecting, responding to, containing, and recovering from information security incidents. It ensures timely action to minimize harm and meet regulatory, contractual, and business obligations.

**2. Scope**

This policy applies to all personnel, systems, applications, and data environments managed or owned by [COMPANY NAME] that are affected by or involved in any type of cybersecurity incident, including but not limited to:

* Unauthorized access attempts
* Malware infections or ransomware attacks
* Data loss, data breaches, or exfiltration
* Insider threats or misuse of systems
* Denial-of-service (DoS) or system disruption events

**3. Policy Statements**

**3.1 Incident Detection and Reporting**

* All users are responsible for promptly reporting suspected or confirmed security incidents to the Security Team. *(NIST IR-6; ISO 27001 A.5.25)*
* Security event monitoring systems must be deployed to detect and alert on potential incidents in real time. *(NIST AU-6, IR-5; ISO 27001 A.5.20, A.5.25)*
* All incidents must be logged and tracked through a formal ticketing or incident response system. *(NIST IR-4; ISO 27001 A.5.25)*

**3.2 Incident Classification and Prioritization**

* Incidents must be classified by severity level (e.g., Low, Medium, High, Critical) based on impact to confidentiality, integrity, availability, or legal obligations. *(NIST IR-4; ISO 27001 A.5.25)*
* Classification must guide resource allocation, escalation, and communication actions. *(NIST IR-4(1); ISO 27001 A.5.30)*

**3.3 Containment, Eradication, and Recovery**

* Immediate containment steps must be taken to isolate affected systems and limit further exposure. *(NIST IR-4; ISO 27001 A.5.30)*
* Root cause analysis must be conducted, and affected systems must be validated before being restored to production. *(NIST IR-5, IR-4(3); ISO 27001 A.5.26)*
* Recovery efforts must be coordinated with the Disaster Recovery Plan (DRP) to minimize downtime and data loss. *(NIST CP-2; ISO 27001 A.5.31)*

**3.4 Notification and Escalation**

* Internal stakeholders must be notified based on incident severity and impact level. *(NIST IR-4(2); ISO 27001 A.5.25)*
* External notifications to regulators, affected customers, or partners must follow applicable legal and contractual requirements. *(NIST IR-6; ISO 27001 A.5.25)*
* The Legal and Compliance teams must approve all breach-related communications. *(NIST PL-4; ISO 27001 A.5.25)*

**3.5 Post-Incident Analysis and Lessons Learned**

* After resolution, a formal post-incident review must be conducted to document what occurred, how it was handled, and what improvements are needed. *(NIST IR-4(4); ISO 27001 A.5.26)*
* Incident trends must be analyzed regularly to identify gaps in controls and enhance organizational resilience. *(NIST CA-7; ISO 27001 A.5.23)*

**4. Roles and Responsibilities**

|  |  |
| --- | --- |
| **All Users** | Report suspected incidents and cooperate with response teams. |
| **IT and Security Team** | Detect, classify, respond to, and recover from incidents. Maintain incident tracking systems. |
| **Incident Response Lead** | Coordinate technical response, communications, and documentation. |
| **Legal and Compliance** | Validate notification obligations and ensure appropriate breach reporting. |
| **HR and Management** | Support investigations of insider-related threats and enforce disciplinary actions if needed. |
| **CISO** | Maintain the IR framework and ensure policy compliance, readiness, and executive reporting. |

**5. Compliance and Enforcement**

Noncompliance with this policy may result in regulatory fines, data loss, reputational harm, or internal disciplinary action. [COMPANY NAME] will audit adherence to this policy and may conduct periodic response drills.

**6. Review and Maintenance**

The CISO is responsible for reviewing this policy annually and following any major incident. Updates must be approved by executive leadership and communicated across the organization.

**7. Acknowledgment and Agreement**

I acknowledge that I have read, understand, and agree to comply with [COMPANY NAME]’s Incident Response Policy. I understand the importance of reporting and responding to incidents in a timely and responsible manner.

|  |  |  |
| --- | --- | --- |
| **Name (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |