Incident Response Plan (IRP)

This Incident Response Plan (IRP) defines how the organization detects, responds to, and recovers from cybersecurity incidents. The goal is to minimize damage, reduce recovery time, and comply with legal and regulatory requirements.

1. Purpose

To establish a structured and systematic approach for identifying, handling, and resolving security incidents such as malware infections, unauthorized access, data breaches, and system outages.

2. Scope

Applies to all employees, contractors, and systems handling organizational data. Covers internal and external incidents, including cloud-based environments and third-party vendors.

3. Incident Categories

Incidents are classified into the following types:

Unauthorized access

Malware or ransomware infection

Data leakage or exfiltration

Denial of service (DoS) attacks

Insider threat activity

4. Response Phases

4.1 Preparation

Train staff, deploy monitoring tools, and maintain updated contact lists and IR documentation.

4.2 Detection & Analysis

Monitor logs, SIEM alerts, and user reports. Validate incidents and determine impact.

4.3 Containment

Isolate affected systems (e.g., disconnect from the network) to limit damage.

4.4 Eradication

Remove malware, unauthorized users, and fix vulnerabilities.

4.5 Recovery

Restore systems from backups and monitor for re-infection or issues.

4.6 Lessons Learned

Conduct post-incident reviews and update the IRP and controls as needed.

5. Roles & Responsibilities

- Incident Response Manager: Oversees incident handling and communications.
- Security Analyst: Investigates alerts and triages incidents.
- IT Operations: Assists with containment and system restoration.
- Compliance Officer: Ensures legal, regulatory, and privacy obligations are met.
- Communications Lead: Handles internal and external notifications.

6. Communication Plan

All incidents must be reported via the Security Incident Form or SOC hotline. Communications must be clear, timely, and documented. High-severity incidents require executive notification within 1 hour.

7. Reporting & Documentation

Each incident must be logged in the incident tracking system with the following information:

- Date/Time detected
- Systems affected
- Root cause
- Response actions taken
- Recovery time
- Impact and resolution

Effective Date: June 1, 2025

Policy Owner: Incident Response Manager

Review Date: Annually or post-incident