Incident Response Policy

1. Purpose

The purpose of this policy is to establish a structured, consistent, and timely approach to detecting, responding to, and recovering from security incidents. This ensures the protection of organizational assets, data, systems, and reputation, while complying with legal, regulatory, and contractual requirements.

---

2. Scope

This policy applies to:

- All employees, contractors, and third parties with access to organizational systems.
- All IT systems, cloud platforms, applications, and networks operated or managed by the organization.
- All types of incidents including cybersecurity, data breaches, insider threats, physical security breaches, and service disruptions.

---

3. Definitions

- **Incident**: An event that compromises the confidentiality, integrity, or availability of systems, data, or services (e.g., malware infection, unauthorized access, data breach).
- **Major Incident**: An incident with significant business impact (e.g., ransomware attack affecting customer data).
- **Incident Response Team (IRT)**: Designated staff responsible for coordinating incident handling.
- **Forensics**: The practice of collecting, preserving, and analyzing evidence related to an incident.

---

4. Policy Statement

- All incidents **must be reported immediately** through the defined channels.
- Incidents will be classified, prioritized, and escalated based on severity.
- Responses must follow the structured phases of the **Incident Response Lifecycle**: Identification, Containment, Eradication, Recovery, and Lessons Learned.
- Evidence must be preserved for forensic analysis and legal obligations.

- The organization will notify affected parties and regulatory bodies where required by law.

---

5. Incident Response Lifecycle

5.1 Identification & Reporting

- Employees must report suspected incidents immediately to the **IT Security Helpdesk** or via the Incident Reporting Portal.
- Security monitoring tools (SIEM, IDS/IPS, endpoint detection) must log and alert potential incidents.
- Incidents are logged in the **Incident Register** with a unique ID.

🔹 **Scenario Example**:
An employee receives an email that looks suspicious (possible phishing). They forward it to the security team instead of clicking any links. The security team analyzes headers and attachments to confirm it's malicious.

5.2 Containment

- Short-term containment: Isolate affected systems (e.g., disconnect from the network).
- Long-term containment: Apply temporary fixes to prevent further spread while root cause analysis is ongoing.

🔹 **Scenario Example**:
Ransomware detected on a finance department workstation. Immediate containment involves disconnecting the workstation, blocking command-and-control traffic on the firewall, and disabling affected user accounts.

5.3 Eradication

- Remove malicious software, unauthorized accounts, or vulnerabilities.
- Apply security patches or configuration changes to prevent recurrence.

🔹 **Scenario Example**:
Following a malware infection, the IT team uses endpoint detection and antivirus tools to remove the malware and resets affected user credentials.

5.4 Recovery

- Restore systems from clean backups.
- Verify that systems are functioning normally and are secure before reintroducing to production.
- Monitor closely for recurring suspicious activity.

🔷 **Scenario Example**:
A SQL injection attack compromised a customer database. After eradication, the team restores the database from a secure backup, applies WAF rules, and strengthens input validation before putting it back online.

5.5 Lessons Learned

- Conduct a **post-incident review** within 14 days of resolution.
- Document what happened, what worked, what failed, and required improvements.
- Update policies, controls, and employee training accordingly.

🔷 **Scenario Example**:
After a phishing campaign, the organization learns that employees lacked training on identifying spear-phishing. The lessons learned phase leads to mandatory phishing awareness training and better email filtering rules.

---

6. Incident Classification

Severity	Description	Examples	Response Time
Critical	Major data breach, service outage, ransomware	Customer data exfiltrated	Immediate, 24/7 response
High	Unauthorized system access, malware infection	Compromised admin account	1 hour
Medium	Suspicious but limited impact	Failed brute-force attempts	4 hours
Low	Minor policy violation	Unauthorized USB device detected	Next business day

---

7. Roles & Responsibilities

- **Incident Response Team (IRT)**: Lead incident handling, technical containment, and eradication.

- **Chief Information Security Officer (CISO)**: Oversight, external communications, regulatory reporting.
- **Business Unit Leaders**: Assist with impact analysis and communication to staff/customers.
- **Employees**: Report incidents immediately and cooperate during investigations.

---

8. Communication & Escalation

- Internal escalation through IRT chain of command.
- External communication (media, regulators, customers) must only be done by **authorized representatives** (CISO or Communications Manager).
- Breach notifications will comply with applicable laws (e.g., GDPR – 72 hours).

---

9. Training & Awareness

- All employees must complete **annual incident response awareness training**.
- The IRT must participate in **tabletop exercises and simulated incident drills** at least twice per year.

---

10. Policy Compliance

- Non-compliance with this policy may result in disciplinary action up to termination.
- Violations may also result in legal or regulatory consequences.