# Incident Response Policy

**Purpose**

This Incident Response Policy aims to define a structured and systematic approach for identifying, responding to, mitigating, and recovering from cybersecurity incidents that could impact the confidentiality, integrity, or availability of the organization's information systems, assets, and data.

**Scope**

This policy applies to all employees, contractors, consultants, temporary staff, and third-party partners interacting with the organization's systems or data. It covers all information systems owned, operated, or managed by the organization.

**Policy Statement**

The organization is committed to protecting its systems and data from cybersecurity threats. To achieve this, we have established an Incident Response Plan (IRP) to promptly and effectively respond to security incidents, minimize impact, and recover operations while preserving evidence for forensic analysis and compliance.

**Definitions**

* **Incident:** Any event that compromises or threatens to compromise the confidentiality, integrity, or availability of organizational systems or data. Examples include malware attacks, unauthorized access, phishing, or data breaches.
* **Incident Response Team (IRT):** A designated group responsible for handling cybersecurity incidents.

**Incident Response Phases**

The organization follows a six-phase approach for incident response:

**1. Preparation**

* An Incident Response Team (IRT) will be established, with defined roles and responsibilities.
* Regular training will be provided to employees and the IRT to ensure awareness and readiness.
* Security tools, monitoring systems, and backup solutions must be maintained and tested regularly.
* A detailed Incident Response Plan (IRP) and playbooks for specific incident types will be developed and reviewed annually.

**2. Identification**

* All employees and contractors are required to report suspected incidents to the IRT immediately.
* The IRT will utilize monitoring tools (e.g., SIEM, IDS/IPS) to detect and confirm incidents.
* Incidents will be classified based on severity (low, medium, high, critical) and documented, including:
	+ Time and date of detection.
	+ Affected systems, users, or data.
	+ Indicators of Compromise (IOCs).

**3. Containment**

* **Short-Term Containment:** Affected systems will be isolated from the network to prevent further damage.
* **Long-Term Containment:** Temporary infrastructure or segmentation will be established to maintain operations during remediation.
* Evidence (e.g., logs and forensic images) will be preserved securely for legal and forensic purposes.

**4. Eradication**

* The IRT will remove malicious files, revoke compromised credentials, and patch vulnerabilities.
* A root cause analysis will be conducted to identify and eliminate all attack vectors.
* Vulnerability scanning and penetration testing will be performed to validate the cleanup process.

**5. Recovery**

* Systems will be restored from secure backups and tested in a controlled environment.
* Heightened monitoring will be maintained during the recovery phase to detect residual threats.
* Full operational capacity will be restored only after validation by the IRT.

**6. Lessons Learned**

* A post-incident review will be conducted within 14 days of resolution to evaluate:
	+ Root cause and timeline of the incident.
	+ Effectiveness of the response.
	+ Areas for improvement.
* Incident reports will be documented and shared with relevant stakeholders.
* Security policies, tools, and training will be updated based on findings.

**Roles and Responsibilities**

1. **Incident Response Team (IRT):**
	* Coordinate and execute all phases of the incident response process.
	* Document actions and maintain a detailed incident timeline.
2. **Employees and Contractors:**
	* Report suspected incidents immediately to the IRT.
	* Follow security protocols and adhere to recommendations during and after an incident.
3. **IT and Security Teams:**
	* Maintain tools for monitoring, detection, and prevention.
	* Conduct regular system updates, backups, and vulnerability assessments.
4. **Executive Leadership:**
	* Provide resources and decision-making support during critical incidents.
	* Ensure compliance with legal and regulatory requirements.

**Incident Classification**

Incidents will be classified into four categories to prioritize response efforts:

1. **Low Severity:** Minor system disruptions or isolated suspicious activity without immediate impact.
2. **Medium Severity:** Events that may degrade performance but do not compromise data or critical systems.
3. **High Severity:** Breaches that affect multiple systems, expose sensitive data, or disrupt critical operations.
4. **Critical Severity:** Widespread disruptions, data loss, or threats to safety requiring immediate escalation to leadership and external parties.

**Incident Reporting**

* All incidents must be reported to the IRT via email, phone, or a designated reporting tool.
* High and critical-severity incidents must be escalated to executive leadership and legal counsel within one hour of identification.

**Communication Protocol**

* **Internal Communication:** The IRT will provide updates to employees and leadership at regular intervals during an incident.
* **External Communication:** The organization's legal and public relations teams will manage all communications with regulators, customers, and the media.
* **Data Breach Notifications:** Notifications will be made to affected parties in accordance with applicable laws (e.g., GDPR, CCPA).

**Compliance**

The organization will adhere to all legal and regulatory requirements for incident reporting, evidence preservation, and data protection. Non-compliance with this policy may result in disciplinary action.

**Review and Maintenance**

* This policy will be reviewed annually or after a major incident to ensure relevance and effectiveness.
* The IRT will maintain a repository of all incident response documentation, including post-incident reports and policy updates.

**Approval**

This policy is approved by the organization's executive leadership and is effective as of [date].