Incident Response Policy Sample

---

1. Purpose

The purpose of this policy is to define the requirements and responsibilities for detecting, responding to, and reporting information security incidents at [Organization Name].

2. Scope

This policy applies to all employees, contractors, vendors, and third-party service providers who access, use, or manage [Organization Name]'s information systems or data.

3. Definitions

- **Incident:** Any actual or suspected event that may threaten the confidentiality, integrity, or availability of information or information systems.
- **Incident Response Team (IRT):** The group of individuals responsible for responding to incidents.

4. Policy Statement

All incidents must be reported immediately to the IRT for investigation and resolution following the procedures defined below.

5. Incident Response Phases

1. **Preparation:** Establish and maintain an incident response capability.
2. **Identification:** Detect and determine whether an incident has occurred.
3. **Containment:** Limit the scope and impact of the incident.
4. **Eradication:** Remove the root cause and affected elements.
5. **Recovery:** Restore and validate system functionality.
6. **Lessons Learned:** Review the incident and improve response processes.

6. Roles and Responsibilities

Role	Responsibility
All Staff	Report suspected or actual incidents promptly.
IRT	Classify, investigate, and respond to incidents.
IT Department	Support technical investigation and remediation.
Management	Ensure compliance and oversight.

7. Reporting Procedure

1. Report the incident to IRT via email: *incident@[organization].com* or phone: *[number]*.

2. Provide details including date, time, description, and affected systems or data.
3. IRT will acknowledge and begin investigation within one business day.

8. Policy Review

This policy shall be reviewed annually and updated as necessary.

9. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination.