IT Security Incident Handling Procedure Template

1. Purpose

This document outlines the procedures for identifying, responding to, mitigating, and documenting IT security incidents to minimize their impact and support future prevention efforts.

2. Scope

This procedure applies to all employees, contractors, and systems within the organization involved in information technology processes.

3. Definition

Security Incident: Any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

4. Roles and Responsibilities

Role	Responsibility
Incident Response Team	Coordinate response, investigation, and resolution of incidents
IT Staff	Report and escalate incidents, assist in technical response
All Employees	Identify and report security incidents
Management	Oversee process and provide resources

5. Incident Handling Procedure

1. **Identification**
   - Detect potential security incidents through system monitoring or reports from staff.
   - Document the initial details of the incident (date, time, reporting party, affected systems).

2. **Containment**
   - Limit the spread and impact of the incident (disconnect affected devices, disable accounts, etc.).
   - Preserve evidence for analysis.

3. **Eradication**
   - Identify the root cause and remove the threat from the environment.

4. **Recovery**
   - Restore affected systems and services to normal operation.
   - Monitor for signs of weakness or recurrence.

5. **Lessons Learned**
   - Conduct a post-incident review to analyze response effectiveness and update procedures if necessary.

6. Incident Reporting

All incidents must be reported to the IT Security Team via the official incident reporting channel within 24 hours of detection.

7. Documentation

Maintain records of all reported incidents, actions taken, communications, and lessons learned.

8. Review and Update

This procedure should be reviewed annually or after a major incident to ensure its effectiveness and accuracy.

9. References

- Organizational Information Security Policy
- NIST Special Publication 800-61: Computer Security Incident Handling Guide

10. Approval

Name	Position	Date	Signature