SOP Template: IT Security Incident Response Workflow

This SOP defines the **IT Security Incident Response Workflow**, detailing the process for identifying, reporting, analyzing, mitigating, and documenting cybersecurity incidents. It ensures timely detection of threats, effective containment of breaches, coordinated communication among stakeholders, and continuous improvement through post-incident reviews. The goal is to minimize damage, protect organizational assets, and maintain compliance with security policies and regulations.

1. Purpose

To establish a standardized workflow for managing IT security incidents, ensuring efficient response, minimizing impact, and documenting lessons learned.

2. Scope

This SOP applies to all employees, contractors, systems, and data within the organization impacted by or involved in the process of responding to IT security incidents.

3. Definitions

Term	Definition
Security Incident	An event indicating a possible breach or violation of information security policies or standard security practices.
Incident Response Team (IRT)	Group responsible for responding to and managing security incidents.
Mitigation	Actions taken to contain, eradicate, and recover from a security incident.

4. Roles and Responsibilities

Role	Responsibilities
IT Security Team	Monitor threats, lead investigations, coordinate mitigation, and document incidents.
Incident Response Team (IRT)	Activate response plan, communicate status, and conduct post-incident reviews.
All Employees	Report suspected incidents promptly to the IT Security Team.
Management	Support incident response, allocate resources, and communicate with stakeholders.

5. Workflow Steps

1. **Identification**
   - Monitor security logs, alerts, and user reports for abnormal activity.
   - Recognize and verify potential security incidents.
2. **Reporting**
   - Report suspected incidents immediately via designated communication channels (e.g., email, hotline).
   - Log incident details: date, time, description, systems involved.
3. **Assessment & Classification**
   - IRT assesses impact, scope, and severity.
   - Classify incident (e.g., data breach, malware, DoS, unauthorized access).
4. **Containment**
   - Implement short-term actions to limit damage.
   - Isolate affected systems if necessary.
5. **Eradication & Mitigation**
   - Remove threats from affected systems.
   - Apply patches, change passwords, and eliminate vulnerabilities.
6. **Recovery**

    - Restore systems and operations to normal.
    - Monitor for recurrence of the incident.
7. **Communication**
    - Notify stakeholders as appropriate (management, legal, regulators).
    - Maintain records of all communications.
8. **Documentation**
    - Document all actions taken, findings, and results.
    - Store reports securely for compliance and review purposes.
9. **Post-Incident Review**
    - Conduct root cause analysis and evaluate response effectiveness.
    - Update policies, procedures, and controls based on lessons learned.

6. Escalation Matrix

Incident Severity	Escalation Path
Low	IT Security Team
Medium	Incident Response Team, Management
High/Critical	IRT, Executive Management, Legal/Compliance, External Authorities (if required)

7. References

- Organizational Information Security Policy
- NIST SP 800-61: Computer Security Incident Handling Guide
- ISO/IEC 27035: Information Security Incident Management

8. Revision History

Date	Version	Description	Author
2024-06-01	1.0	Initial SOP Template Release	IT Security Team