SOP Template: Reporting and Documentation of Security Incidents

This SOP details the procedures for **reporting and documentation of security incidents**, including immediate incident reporting guidelines, proper documentation practices, investigation protocols, communication channels, confidentiality requirements, and follow-up actions. The aim is to ensure timely and accurate reporting to enhance security measures, support incident analysis, and maintain comprehensive records for accountability and future prevention.

1. Purpose

To establish a consistent and effective process for the immediate reporting, thorough documentation, investigation, and analysis of security incidents.

2. Scope

This SOP applies to all employees, contractors, and relevant stakeholders involved in the reporting, management, and response to security incidents.

3. Definitions

Term	Definition
Security Incident	An event that may compromise the confidentiality, integrity, or availability of information, systems, or assets.
Incident Report	Documentation detailing the facts, status, and resolution of a security incident.
Incident Response Team (IRT)	Designated individuals responsible for incident management and resolution.

4. Procedures

1. **Immediate Incident Reporting**
    - Upon identifying or suspecting a security incident, **immediately notify** the Incident Response Team (IRT) via designated communication channels (e.g., hotline, email, ticketing system).
    - Provide initial details: date/time, description, affected systems, and actions taken (if any).
    - Do not attempt to alter, delete, or remediate evidence unless directed by the IRT.
2. **Documentation Practices**
    - Complete a Security Incident Report using the approved template (see Appendix A).
    - Ensure all relevant details (who, what, when, where, how) are included and factual.
    - Attach relevant logs, screenshots, and supporting documents.
3. **Investigation Protocols**
    - The IRT will conduct a preliminary assessment and classify the incident severity.
    - Assign responsibilities for investigation, evidence collection, and coordination.
    - Document investigation steps, findings, and resolution measures.
4. **Communication Channels**
    - Internal: Use secure channels for sharing incident information (e.g., encrypted email, secure portals).
    - External: Communicate with third parties (vendors, regulators) only as authorized.
5. **Confidentiality Requirements**
    - Restrict access to incident information to authorized personnel only.
    - Do not disclose details outside required channels without explicit approval.
6. **Follow-Up Actions**
    - Conduct a post-incident review to determine root cause and impact.
    - Develop and implement corrective and preventive actions as necessary.
    - Update relevant policies, controls, and awareness training to address lessons learned.

5. Roles and Responsibilities

Role	Responsibilities

All Employees	Report suspected or actual security incidents as per this SOP.
Incident Response Team	Coordinate incident response, investigation, documentation, and follow-up.
IT Department	Assist with technical investigation and system restoration.
Management	Review incidents and approve policy or procedural changes.

6. Record Keeping

- All incident reports and related documentation must be retained for a minimum of **2 years** or as required by law/regulations.
- Store incident records securely with restricted access.

7. Review and Update

- This SOP shall be reviewed annually or following a major incident to ensure effectiveness and relevance.

Appendix A: Security Incident Report Template

Incident Number	
Date/Time Reported	
Reporter Name/Contact	
Description of Incident	
Affected Systems/People	
Actions Taken	
Evidence Collected	
Incident Severity	
Investigation Summary	
Resolution/Follow-up Actions	
Approved By	
Date Closed	