Standard Operating Procedure (SOP)
Incident Reporting and Breach Response Protocol

This SOP details the **incident reporting and breach response protocol**, outlining the procedures for timely identification, documentation, and reporting of security incidents and breaches. It includes steps for immediate containment, investigation, communication with stakeholders, and implementation of corrective actions to mitigate risks and prevent recurrence. The protocol ensures compliance with legal and organizational requirements, promotes transparency, and supports continuous improvement in security management.

1. Purpose

To establish a standard process for the identification, reporting, management, and resolution of security incidents and breaches within the organization.

2. Scope

This SOP applies to all personnel, contractors, and third parties who have access to organizational information systems and data.

3. Definitions

Term	Definition
Incident	An event that compromises the confidentiality, integrity, or availability of information assets.
Breach	A confirmed incident where unauthorized access to data has occurred.
Containment	Actions taken to limit the impact and spread of an incident or breach.

4. Responsibilities

- **All Staff:** Report any suspected or confirmed incidents or breaches immediately.
- **IT/Security Team:** Lead investigation, containment, eradication, and recovery processes.
- **Management:** Ensure compliance, review incident reports, and approve corrective actions.
- **Legal/Compliance:** Advise on regulatory notification requirements and support communication efforts.

5. Procedure

1. **Identification**
   - Monitor systems for signs of incidents or breaches.
   - Report suspected incidents to the designated incident response contact/team.
2. **Reporting**
   - Document the date, time, nature, and potential impact of the incident.
   - Use the Incident Report Form (see Appendix A) to standardize submissions.
3. **Containment**
   - Initiate immediate actions to contain the incident (e.g., isolate affected systems, revoke credentials).
   - Escalate to IT/Security Team for major incidents or confirmed breaches.
4. **Investigation**
   - Determine the scope, root cause, and impact of the incident.
   - Gather and preserve evidence following chain-of-custody procedures.
5. **Eradication and Recovery**
   - Remove threats and restore systems to normal operation.
   - Monitor for signs of residual or recurring issues.
6. **Communication**
   - Inform affected stakeholders and, if applicable, regulatory authorities in accordance with legal requirements.
   - Provide status updates as necessary.
7. **Review and Corrective Actions**
   - Conduct a post-incident review to assess response effectiveness.
   - Implement corrective actions to improve policies, controls, and staff training.
8. **Documentation and Reporting**

- Maintain detailed records of the incident and response actions.
- Submit final incident report to management and file for audit purposes.

6. Compliance

All incident response activities must adhere to applicable legal, regulatory, and contractual requirements, and align with organizational policies on information security and privacy.

7. Continuous Improvement

Lessons learned from incidents and breach responses must be used to enhance security awareness, update response protocols, and strengthen organizational defenses.

Appendix A: Incident Report Form (Template)

Field	Description
Date and Time of Incident	
Reporter Name & Contact	
Description of Incident	
Systems/Data Affected	
Initial Actions Taken	
Suspected Cause	
Impact	
Additional Comments	