SOP Template: Incident Reporting and Breach Response Protocols

This SOP details the **incident reporting and breach response protocols**, including procedures for identifying and documenting incidents, timely reporting to relevant authorities, investigation and analysis of breaches, containment and mitigation measures, communication strategies, and post-incident review and corrective actions. The goal is to ensure a structured and efficient response to incidents and breaches, minimizing impact and preventing recurrence.

1. Scope

This SOP applies to all employees, contractors, and relevant stakeholders involved with handling sensitive information and IT systems.

2. Definitions

Term	Definition
Incident	An event that may compromise the integrity, confidentiality, or availability of information or systems.
Breach	Confirmed unauthorized access, disclosure, alteration, or destruction of sensitive information.
Incident Response Team (IRT)	Designated group responsible for managing incident response procedures.

3. Responsibilities

- **All Staff**: Promptly report suspected or actual incidents.
- **IRT**: Assess, manage, document, and resolve incidents and breaches.
- **Management**: Support, allocate resources, and review post-incident recommendations.

4. Procedures

4.1 Identification and Documentation

1. Identify unusual or suspicious activity related to systems or data.
2. Document essential details:
    - Date and time of detection
    - Description of the incident
    - Systems and data involved
3. Log incident in the Incident Register.

4.2 Reporting

1. Immediately report incidents to the IRT via designated communication channels.
2. If applicable, notify external authorities as per legal/regulatory requirements.
3. Record all notifications in the Incident Register.

4.3 Investigation and Analysis

1. IRT assesses and categorizes the incident (e.g., low, medium, high severity).
2. Collect forensic evidence while maintaining chain-of-custody.
3. Determine root cause and impact.
4. Document findings and update incident records.

4.4 Containment and Mitigation

1. Isolate affected systems to prevent further impact.
2. Apply immediate mitigation actions (e.g., password resets, access revocation).
3. Monitor effectiveness and adjust measures as needed.
4. Record all containment activities.

4.5 Communication

1. Notify impacted parties and stakeholders.
2. Coordinate public communications, if needed, with authorized representatives.
3. Maintain logs of all communications related to the incident/breach.

4.6 Post-Incident Review and Corrective Actions

1. Conduct a post-incident review meeting to evaluate response steps.
2. Identify lessons learned and areas for improvement.
3. Implement corrective and preventive actions.
4. Update security policies and training as needed.
5. Close incident in the Incident Register when all actions are complete.

5. Records and Documentation

- Incident Register
- Investigation reports
- Communications logs
- Post-incident review documentation

6. Review

This SOP shall be reviewed annually or after a significant incident or breach, whichever occurs first.