Standard Operating Procedure (SOP): Incident Reporting for Breaches or Unauthorized Access

This SOP establishes clear procedures for **incident reporting for breaches or unauthorized access** to ensure timely detection, documentation, and response to security incidents. It outlines the steps for identifying, reporting, and escalating breaches or unauthorized access attempts, assigns responsibilities to relevant personnel, and emphasizes maintaining accurate records to support investigation and mitigation efforts. The goal is to protect sensitive information, maintain system integrity, and uphold organizational security standards.

1. Purpose

To provide a standardized approach for reporting, documenting, and responding to incidents involving breaches or unauthorized access to systems and information.

2. Scope

This SOP applies to all employees, contractors, and third-party users who have access to the organization's information systems and data.

3. Definitions

- **Breach:** Unauthorized access, acquisition, or disclosure of sensitive or confidential data.
- **Unauthorized Access:** Any access to systems, networks, or data by individuals who do not have explicit permission.
- **Incident:** Any event that compromises the confidentiality, integrity, or availability of information systems.

4. Responsibilities

Role	Responsibilities
All Staff	Identify and report suspected breaches or unauthorized access incidents immediately.
IT Helpdesk	Receive, log, and escalate reported incidents as per escalation matrix.
Incident Response Team	Investigate, document, and remediate reported incidents. Coordinate with stakeholders as needed.
Management	Review incidents, ensure appropriate actions are taken, and provide updates to executive leadership.

5. Procedure

1. **Incident Identification:**
    - Recognize signs of potential breaches, such as unauthorized login attempts, unusual system behavior, missing files, or alerts from security tools.
2. **Immediate Reporting:**
    - Report incidents to the IT Helpdesk or designated authority using the established incident reporting channels (e.g., phone, email, ticketing system).
    - Provide all relevant details, including date/time, system(s) affected, nature of the incident, and any actions already taken.
3. **Incident Logging:**

    - IT Helpdesk logs the incident in the incident management system, assigning a unique reference number.
4. **Initial Assessment and Escalation:**
    - Incident Response Team conducts a preliminary assessment to determine the severity and potential impact.
    - Escalate to management and/or specialized teams as prescribed in the escalation matrix, based on severity and impact.
5. **Containment and Investigation:**
    - Take immediate steps to contain the breach (e.g., revoke access, isolate affected systems).
    - Incident Response Team investigates to determine the root cause, scope, and affected assets/data.
6. **Communication:**
    - Notify affected stakeholders and external parties (if required, e.g., regulators), following organizational protocols.
7. **Documentation:**
    - Maintain accurate and detailed records of the incident, actions taken, and evidence collected to support any forensic investigations.
8. **Mitigation and Remediation:**
    - Implement fixes to mitigate risks and prevent recurrence. Restore affected services and strengthen controls as necessary.
9. **Closure and Review:**
    - Incident Response Team conducts a post-incident review to identify lessons learned and update policies/SOPs as needed.

6. Record Keeping

- All incident reports and investigation documents must be stored securely, with access limited to authorized personnel.
- Records must be retained in accordance with organizational policy and applicable regulations.

7. Related Documents

- Incident Response Plan
- Access Control Policy
- Data Protection Policy
- Escalation Matrix

8. Revision History

Version	Date	Description	Author
1.0	2024-06-14	Initial SOP Creation	Policy Team