Data Breach Notification Procedure Document

Document Owner: IT Security Manager
Version: 1.0
Date: 2024-06-30

1. Purpose

The purpose of this procedure is to provide a structured approach for responding to data breaches, ensuring prompt notification to all relevant parties and compliance with applicable legal and regulatory requirements.

2. Scope

This procedure applies to all employees, contractors, and third-party vendors who handle or process personal data or confidential information within the organization.

3. Definition

A **data breach** is any incident that results in unauthorized access, disclosure, alteration, or destruction of personal or sensitive data.

4. Procedure

1. **Identification and Reporting:**
    - Any employee who detects a data breach must report it immediately to the IT Security Manager.
    - Use the Data Breach Report Form to provide details of the incident.
2. **Assessment:**
    - The IT Security Manager assesses the scope, type, and impact of the breach.
    - Document all findings and determine whether personal or sensitive data is involved.
3. **Containment and Eradication:**
    - Immediate steps must be taken to contain the breach and prevent further unauthorized access.
4. **Notification:**
    - If notification is required, inform affected individuals and regulatory authorities within the stipulated timeline.
    - Provide clear information on the nature of the breach, the data involved, and recommended steps for affected parties.
5. **Investigation and Documentation:**
    - Conduct a thorough investigation and document the cause and response actions.
6. **Review and Improvement:**
    - After resolving the incident, review the procedures and update them as necessary to prevent future breaches.

5. Roles and Responsibilities

- **IT Security Manager:** Lead breach response, coordinate notifications, document incident.
- **All Staff:** Report suspected or confirmed breaches.
- **Management:** Ensure procedures are followed and resources are allocated as needed.

6. Communication

Communications about the breach must be accurate, clear, and provided only by authorized personnel.

Important Notes

- Timely notification can help mitigate the impact and potential fines related to data breaches.
- Legal requirements for breach notification may vary by jurisdiction and type of data.
- Maintaining up-to-date contact details for key personnel and regulatory authorities is essential.
- Regular training and awareness for employees can reduce the risk of breaches.