Data Breach Response Policy

1.0 Purpose

This policy establishes the framework and objectives for the organization's data breach response process. It defines the scope of applicability, outlines procedures for suspected or confirmed breaches, clarifies roles and responsibilities, sets standards for incident prioritization, and mandates reporting, remediation, and feedback mechanisms. The purpose is to ensure a coordinated, effective, and timely response to protect the organization's data, personnel, and stakeholders. This policy must be effectively communicated and readily accessible to all personnel involved in data privacy and security protection.

The organization is committed to maintaining a culture of openness, trust, and integrity. This includes a proactive approach to data security and a structured response to potential breaches. This policy aims to protect the organization, its employees, partners, and associated individuals from harm resulting from unauthorized data access or disclosure, whether intentional or unintentional.

2.0 Background

Any individual who suspects that a theft, breach, or unauthorized exposure of the organization's Protected Data or Sensitive Data may have occurred has an immediate obligation to report the incident. Reports should describe the circumstances and be submitted promptly through the designated internal channels (e.g., IT Help Desk email, dedicated phone line, or internal reporting portal). These reporting channels are actively monitored by the designated Information Security personnel or team responsible for initiating investigations. All reports will be investigated to determine if a data breach or exposure has occurred. Confirmed incidents will trigger the established Incident Response Procedure.

3.0 Scope

This policy applies to all employees, contractors, vendors, and partners who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle sensitive or protected information, including Personally Identifiable Information (PII) and Protected Health Information (PHI), on behalf of the organization. Agreements with third-party vendors must include provisions requiring adherence to comparable data protection and breach notification standards.

4.0 Policy: Incident Response Protocol

4.1 Incident Confirmation and Initial Response

Upon confirmation of a theft, data breach, or exposure involving Protected or Sensitive Data, immediate steps will be taken to contain the incident, including isolating affected systems and

revoking access where necessary to prevent further unauthorized activity.

4.2 Incident Response Team Activation

The designated Executive Leader (e.g., Executive Director, Chief Information Security Officer) will activate and chair an Incident Response Team (IRT) to manage the breach or exposure event. The core IRT will be composed of representatives from relevant departments, including:

* IT Infrastructure
* IT Applications / Information Security
* Legal Counsel
* Communications / Public Relations
* Finance (if financial data is impacted)
* Member/Customer Services (if member/customer data is impacted)
* Human Resources
* The business unit(s) directly affected or responsible for the compromised system/data.
* Additional members as deemed necessary by the IRT Chair based on the nature and scope of the incident.

4.3 Investigation and Analysis

The IRT, potentially supported by internal IT and designated external forensic specialists (often coordinated through cyber insurance providers), will conduct a thorough investigation. The objectives are to:

* Determine the root cause of the breach or exposure.
* Identify the specific types of data involved.
* Ascertain the extent of the impact, including the number of individuals and/or organizations potentially affected.
* Assess the scope and severity of the incident.

4.4 Communication Strategy

The IRT, in collaboration with Legal, Communications, and Human Resources departments, will develop and execute a strategic communication plan. This plan will address necessary notifications to:

* Internal personnel
* Regulatory bodies (as required by law)
* Affected individuals
* The public, if deemed necessary.

5.0 Ownership and Responsibilities

* **Data Sponsors:** Individuals or departments with primary responsibility for overseeing specific information resources. Sponsors are typically designated based on administrative roles or their function in collecting, developing, or managing data.

*   **Information Security Administrator/Team:** Designated personnel responsible for the administrative implementation, oversight, and coordination of security procedures and systems, acting in consultation with Data Sponsors.
*   **Users:** All members of the organization community (including staff, contractors, consultants, etc.) with authorized access to information resources. Users are responsible for adhering to security policies and reporting suspected incidents.
*   **Incident Response Team (IRT):** Chaired by Executive Management, this cross-functional team is responsible for managing the response to confirmed data breaches as outlined in section 4.2.

6.0 Enforcement

Violations of this policy by organizational personnel may result in disciplinary action, up to and including termination of employment, subject to applicable laws and internal procedures. Violations by third-party partners may lead to remediation actions, including termination of contracts or network access.

7.0 Definitions

*   **Breach:** The unauthorized acquisition, access, use, or disclosure of Protected Data or Sensitive Data that compromises its security or privacy.
*   **Encryption:** The process of converting data (plain text) into a coded format (ciphertext) requiring a specific key or password for decryption, enhancing data security.
*   **Information Resource:** The data and information assets managed by the organization or its units.
*   **Personally Identifiable Information (PII):** Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information.
*   **Protected Health Information (PHI):** As defined under applicable laws (e.g., HIPAA in the US), information relating to health status, healthcare provision, or payment for healthcare that can be linked to a specific individual.
*   **Protected Data:** A collective term referring to PII and/or PHI requiring specific security measures.
*   **Plain Text:** Data that is not encrypted.
*   **Safeguards:** Technical, administrative, and physical controls implemented to protect information resources from threats and minimize security risks.
*   **Sensitive Data:** Data classified by the organization as requiring protection due to its confidential nature, including but not limited to Protected Data.

Revision #3
Created 28 August 2024 16:59:58 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery