|  |  |
| --- | --- |
| Data Breach Response Policy | Icon  Description automatically generated |

**Last Update**: *September 2020*

# Purpose

<Company Name>’s Data Breach Response Policy (DBRP) sets forth the plans and procedures to prepare for and respond to a data breach (or the suspicion a data breach has occurred). It establishes and designates the members of the Breach Response Team, as well as includes the organizational framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach. It is intended to provide guidance on whether and how to provide notification and services to those individuals. The purpose of this policy is to ensure that <Company Name> responds in a timely, consistent and appropriate manner to suspected and confirmed breaches to protect <Company Name>’s information and assets and to minimize harm to individuals and entities that may be affected by the breach. The DBRP is also intended to promote consistency in the way <Company Name> prepares for and responds to a breach by establishing baseline requirements and procedures, and promote a culture of openness, trust and integrity in the way it manages and responds to a breach incident.

# Background

In fulfilling its mission, <Company Name> collects and maintains personally identifiable information (PII) about customers, employees, officers and directors of financial institutions. <Company Name> is responsible for protecting this PII from loss, theft or compromise (“breach”). Failure to adequately protect this PII, as well as to report a breach in a timely manner, could cause significant financial, reputation, or other harm to individuals, the Corporation, or other affected stakeholders.

# Scope

The DBRP is a component of <Company Name>’s overall Incident Response Plan. The Policy applies to a breach of PII in any format (electronic, paper or verbal). This policy applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of <Company Name> members. Any contracts or agreements with third-party vendors will contain language similar that protects <Company Name>.

If any individual suspects that a theft, breach or exposure of <Company Name> protected data or <Company Name> sensitive data has occurred, the Information Security Administrator and Executive Directors must be notified immediately. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will initiate the Data Breach Response process.

# Definition of a data breach

For the purposes of this policy, <Company Name> defines a data breach as an incident that occurs when information held by <Company Name> is lost or subjected to unauthorized access, modification, disclosure, or other misuse or interference. In this Plan, the terms “data” and “information” are used interchangeably and should be taken to mean both data and information.

# Policy

When a data breach has occurred or is suspected to have occurred, <Company Name> will initiate the following process. However, it should be noted that there is no single method of responding to a data breach, and in some cases the following steps may need to be modified. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved and using that risk assessment to decide the appropriate course of action.

## Identify

As soon as a theft, data breach or exposure containing <Company Name> protected data or <Company Name> sensitive data is reported, it must be identified and confirmed.

This will be conducted by the Information Security Administrator and members of the IT Department and the Incident Response Team.

<Company Name> will form an incident response team to handle the breach or exposure. The Incident Response Team should be compromised of personnel with the necessary skills and authority to undertake the response process for their respective department. These departments should include, but are not limited to, IT Security, Data Privacy, Legal, Finance, and Communications.

## Contain

The Incident Response Team will take immediate steps to contain the breach, which may include:

* Stopping unauthorized practices
* Recovering records
* Shutting down a system that has been breached
* Revoking or changing computer access privileges
* Addressing weaknesses in physical or electronic security
* Alerting building security

## Assess

The Incident Response Team, along with applicable forensic investigators, will complete a full data breach assessment that will determine how the breach or exposure occurred; the types of data involved; the number of internal and external individuals and/or organizations impacted; and an analysis of the breach or exposure to determine the root cause.

## Notification and Communication

The Incident Response Team will complete a Data Breach Assessment Report to Executive Management. The Information Security Administrator will work with <Company Name>’s executive management team, and communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public and c) those directly affected.

## Policy roles and responsibilities

Roles and responsibilities are as follows:

* Sponsors are those members of the <Company Name> community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any <Company Name> executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
* Information Security Administrator is a member of the <Company Name> community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
* Users include virtually all members of the <Company Name> community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
* The Incident Response Team shall be chaired by the Executive Director or Information Security Administrator and include, but will not be limited to, the following departments or their representatives: IT infrastructure, IT application security, communications, legal, management, financial services, member services and human resources.

# Enforcement

Any <Company Name> personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have its network connection terminated.

# Terms & Definitions

**Encryption or encrypted data:** The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

**Plain text:** Unencrypted data.

**Hacker:** A slang term for a computer enthusiast — i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

**Protected Health Information (PHI):** any information about health status, provision of health care, or payment for health care that is created or collected by a medical or healthcare provider or under U.S law is a “Covered Entity” (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

**Personally Identifiable Information (PII):** Any data that could potentially identify a specific individual or distinguish or trace and individual’s identity, either alone or when combines with other information that is linked or linkable to a specific individual.

**Protected data:** See PII and PHI.

**Information resource:** The data and information assets of an organization, department or unit.

**Safeguards:** Countermeasures and controls put in place to avoid, detect, counteract or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

**Sensitive dat**a: Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

**Incident**: An incident refers to an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. [For purposes of this policy, an “incident” includes all suspected or known (confirmed) breaches.]

**Breach:** A breach refers to the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for another than authorized purpose.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of Revision | Author | Description of Changes |
| 1.0 |  |  |  |