SecOps® Solution

Data Breach Response Policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new policy or an updated version of this one.*

1. Overview

A data breach response plan outlines an organization's course of action in the case of a data breach. It describes what constitutes an information security and cybersecurity incident, who is involved in the plan and how to reach them, as well as what to do in the event of a breach and what to do thereafter.

2. Purpose

This policy's objective is to give you a way to let the proper departments know if you suspect someone of stealing, exposing, or breaching Fordham Protected Data or Fordham Sensitive Data (including unlawful access, use, or disclosure).

The goal of posting a data breach response policy is for <ORGANIZATION NAME> information security to pay close attention to data security and data. Security lapses and how an <ORGANIZATION NAME> openness, trust, and integrity-based culture should react to such behavior. <ORGANIZATION NAME> Information Security is dedicated to defending <ORGANIZATION NAME> partners, employees, and customers from individuals' wrongful or harmful activities, whether they do so consciously or inadvertently.

3. Scope

This policy is applicable to anyone who collects, accesses, maintains, distributes, processes, safeguards, stores, uses, transmits, discards, or otherwise handles personally identifiable information (PII) or Protected Health Information (PHI) of members of <ORGANIZATION NAME>. Any agreements with vendors will contain language similar that protects the fund.

4. Policy

All access to a resource will be terminated as soon as a theft, data breach, or expose containing <ORGANIZATION NAME> protected data or sensitive data is discovered.

© 2022 SecOps® Solution and/or its affiliates. All rights reserved. SecOps® Solution Confidential

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed.
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Theft, security breach, or exposure will be reported to the Executive Director. IT will examine the breach or expose it jointly with the assigned forensic team to identify the underlying cause.

Work with Forensic Investigators

As provided by <ORGANIZATION NAME> cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan

Work with <ORGANIZATION NAME> communications, legal and human resource departments to determine how to notify the following parties about the breach: a) internal employees, b) the public, and c) those directly affected.

5. Ownership and Responsibilities

- Sponsors - Members of the <ORGANIZATION NAME> community who have primary responsibility for maintaining a specific information resource are known as sponsors. Any <ORGANIZATION NAME> executive may name sponsors as part of their administrative duties, or by the information itself being sponsored, collected, developed, or stored.

© 2022 SecOps® Solution and/or its affiliates. All rights reserved. SecOps® Solution Confidential

- The Executive Director or the Director, of Information Technology (IT) Infrastructure designates a member of the <ORGANIZATION NAME> community as the information security administrator, and this person is responsible for providing administrative support for the implementation, supervision, and coordination of security procedures and systems with regard to particular information resources in consultation with the appropriate Sponsors.
- Users include virtually all members of the <ORGANIZATION 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 Executive Management will preside over the Incident Response Team, which will be made up of representatives from the following departments: IT Infrastructure, IT Application Security, Communications, Legal, Management, Financial Services, and Human Resources.

6. Enforcement

Any < ORGANIZATION 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.

7. Definition and Terms

Protected Health Information (PHI) - Under US law any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered.

8. Revision History

Version	Date	Description
1.0	09-12-2022	Initial Policy

© 2022 SecOps® Solution and/or its affiliates. All rights reserved. SecOps® Solution Confidential