“Your Company Name”
Data Breach Response Policy

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

“Your Company Name” Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how “Your Company Name”’s established culture of openness, trust and integrity should respond to such activity. “Your Company Name” Information Security is committed to protecting “Your Company Name” 's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Background

This policy mandates that any individual who suspects that a theft, breach or exposure of “Your Company Name” protected data or “Your Company Name” sensitive data has occurred must immediately provide a description of what occurred via e-mail to “person in your company” and “second person” or by calling “telephone number”. This e-mail address, phone number, are monitored by the “Your Company Name” ’s Executive and IT team lead. 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 Security Administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information of “Your Company Name” customers.

3.0 Policy Confirmed theft, data breach or exposure of “Your Company Name” Protected data or “Your Company Name” Sensitive data

As soon as a theft, data breach or exposure containing “Your Company Name” Protected data or “Your Company Name” Sensitive data is identified, the process of removing all access to that resource will begin.

The President 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 President

Confirmed theft, breach or exposure of “Your Company Name” data

The President will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by “Your Company 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.

Communication plan.

“Your Company Name” communications, legal and human resource departments will decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

3.2 Ownership and Responsibilities
Roles & Responsibilities:

- Vendors - Vendors are those members of the “Your Company Name” community that have primary responsibility for maintaining any particular information resource. Vendors may be designated by any “Your Company Name” Executive in connection with their administrative responsibilities, or by the actual collection, development, or storage of information. An example is AWS.
- Information Security Administrator is that member of the “Your Company Name” community, designated by the President 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 Vendors .

- Users include virtually all members of the “Your 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 Executive Management and shall 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; Human Resources.

4.0 Enforcement

Any “Your 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 their network connection terminated.

5.0 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).

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

Protected data - See PII

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, 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 data - Data that is encrypted or in plain text and contains PII data. See PII above.

6.0 Revision History

Version	Date of Revision	Author	Description of Changes
1.0	July 1, 2022		Initial version

1.0			