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.

SproutLoud 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 SproutLoud's established culture of openness, trust and integrity should respond to such activity. SproutLoud Information Security is committed to protecting SproutLoud's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of SproutLoud Protected data or SproutLoud Sensitive data has occurred must immediately provide a description of what occurred via e-mail to dataprivacy@sproutloud.com to reach our Data Protection Officer (DPO), who is also currently our Chief Technology Officer. This e-mail address is monitored by the SproutLoud security team that 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 follow the appropriate procedure in place.

3.0 Scope

This policy applies to any breach of data surrounding Personal Information in accordance with our Privacy Policy found here: www.sproutloud.com/legal/privacy.

4.0 Process on confirmed theft, data breach or exposure of SproutLoud Protected data or SproutLoud Sensitive data

As soon as a theft, data breach or exposure containing SproutLoud Protected data or SproutLoud Sensitive data is identified and confirmed, the process of removing all access to that resource will begin.

The DPO 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 (if applicable)
- Communications
- Member Services (if Member data is affected)
- People & Organizational Development (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

Confirmed theft, breach or exposure of SproutLoud data

The DPO will be notified of the theft, breach or exposure. The team will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

Depending on the severity of the breach, the DPO will make a determination whether to include a forensic investigation, as provided by SproutLoud 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 SproutLoud communications, legal and POD departments to decide how to communicate the breach to: a) internal employees, b) Clients, and c) those directly affected within 3 business days of confirmation of the incident.

5.0 Ownership and Responsibilities

- *Information Security Administrators* are SproutLoud employees designated by the DPO within the Information Technology (IT) Infrastructure, who provide 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 SproutLoud 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 DPO and shall include, but will not be limited to, the following departments or their representatives: IT-SRE, IT-DevOps; IT-Development; Client Relationship Manager; Legal; Executive Management; and POD.

6.0 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).

Protected Health Information (PHI) - Under US law is 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 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 and PHI

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 or PHI data. See PII and PHI above.

7.0 Revision History

Version	Date of Change	Responsible	Summary of Change
1.0	12/2017	James Aggrey	Initial Release
1.1	05/05/2018	Anjan Upadhya	Updates per GDPR
1.2	06/02/2020	James Aggrey	Updated name of HR
1.3	07/20/2021	Anjan Upadhya	Updated POD in other areas and added language for communication timeframe in the event of a breach.