Data Classification Policy

1 Overview

The purpose of this Guideline is to establish a framework for classifying institutional data based on its level of sensitivity, value and criticality to SproutLoud as required by SproutLoud's Information Security Policy. Classification of data will aid in determining baseline security controls for the protection of data.

2 Applies To

This Policy applies to all employees (full-time and part time) and third-party providers of SproutLoud as well as any other affiliate who is authorized to access SproutLoud's Data.

3 Definitions

Confidential Data is a generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with sensitive data.

A Data Steward is a senior-level employee of SproutLoud who oversees the lifecycle of one or more sets of Institutional Data.

Institutional Data is defined as all data owned/licensed by SproutLoud or uploaded by users in the Sproutloud application.

Non-public Information is defined as any information that is classified as Private or Restricted Information according to the data classification scheme defined in this Guideline.

Sensitive Data is a generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with confidential data.

4 Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to SproutLoud should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications:

A.	**Restricted Data**
	Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to SproutLoud, its Clients or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data.
B.	**Private Data**
	Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to SproutLoud, its Clients or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.
C.	**Public Data**
	Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to SproutLoud, its Clients and its affiliates. Examples of Public data include press releases, product documentation and publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Classification of data should be performed by an appropriate Data Steward. Data Stewards are senior-level employees of SproutLoud who oversee the lifecycle of one or more sets of Institutional Data.

5 Data Collections

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of an employee's name, address and social security number, the data collection should be classified as Restricted even though the employee's name and address may be considered Public information.

6 Reclassification

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to SproutLoud.

This evaluation should be conducted by the appropriate Data Steward. Conducting an evaluation on an annual basis is encouraged; however, the Data Steward should determine what frequency is most appropriate based on available resources. If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification.

If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

7 Calculating Classification

The goal of information security, as stated in SproutLoud's Information Security Policy, is to protect the confidentiality, integrity and availability of Institutional Data. Data classification reflects the level of impact to SproutLoud if confidentiality, integrity or availability is compromised.

Unfortunately there is no perfect quantitative system for calculating the classification of a particular data element. In some situations, the appropriate classification may be more obvious, such as when federal laws require SproutLoud to protect certain types of data (e.g. personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide. It is an excerpt from Federal Information Processing Standards (FIPS) publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

As the total potential impact to SproutLoud increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the Information Security Office for assistance.

8 Appendix A - Predefined Types of Restricted Information

The Information Security Office and the People and Organizational Development Department have defined several types of Restricted data based on state and federal regulatory requirements. The following table applies to data stored within the SproutLoud infrastructure and its internal operations. They're defined as follows:

1.	**Authentication Verifier**

	An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals using a password manager like LastPass. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to: ● Passwords ● Shared secrets ● Cryptographic private keys
2.	**Employee/Customer Financial Information**
3.	**Electronic Protected Health Information ("EPHI")**
	EPHI is defined as any Protected Health Information ("PHI") that is stored in or transmitted by electronic media. For the purpose of this definition, electronic media includes: ○ Electronic storage media includes computer hard drives and any removable and/or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. ○ Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, an extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, private networks and the physical movement of removable and/or transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via

	electronic media because the information being exchanged did not exist in electronic form before the transmission.
4.	**Federal Tax Information ("FTI")**
	FTI is defined as any return, return information or taxpayer return information that is entrusted to SproutLoud by the Internal Revenue Services. See Internal Revenue Service Publication 1075 Exhibit 2 for more information.
5.	**Payment Card Information**
	Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements: • Cardholder name • Service code • Expiration date • CVC2, CVV2 or CID value • PIN or PIN block • Contents of a credit card's magnetic stripe
6.	**Personally Identifiable Records**

	Personally Identifiable Records are defined as any Records that contain name and one or more of the following personal identifiers: • Name of the employee/client • Social security number • A list of personal characteristics that would make the employee/client's identity easily traceable • Any other information or identifier that would make the employee/client's identity easily traceable
7.	**Personally Identifiable Information**
	For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements: • Home/physical address • E-mail address • Social security number • State-issued driver's license number • State-issued identification card number • Financial account number in combination with a security code, access code or password that would permit access to the account • Medical and/or health insurance information
8.	**Protected Health Information ("PHI")** PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium. PHI is considered individually identifiable if it contains the first name, first initial and last name and one or more of the following identifiers:

	• Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code) • All elements of dates (except year) related to an individual including birth date, admission date, discharge date, date of death and exact age if over 89) • Telephone numbers • Fax numbers • Electronic mail addresses • Social security numbers • Medical record numbers • Health plan beneficiary numbers • Account numbers • Certificate/license numbers • Vehicle identifiers and serial numbers, including license plate number • Device identifiers and serial numbers • Biometric identifiers, including finger and voice prints • Full face photographic images and any comparable images • Any other unique identifying number, characteristic or code that could identify an individual
9.	**Controlled Technical Information ("CTI")**
	Controlled Technical Information means technical information related to proprietary technology developed by SproutLoud for its services and application offerings.

9 Appendix B - Predefined Types of Information Related to Subcontractor Use and Data Security Policy

The following document outlines SproutLoud's Information Security Office views on the data provided to Subcontractors. The following table outlines meaningful classifications that should be viewed in contacts with SproutLoud's Subcontractor Use and Data Security policy:

NOTE: In the event additional data data points grow beyond what is listed below, this appendix will be updated to reflect such data and data re-classified. This applies especially to any data points that come under PHI or PII as per Appendix A.

1.	**Restricted-MSP Data:** In context of storage/processing/transfer within SproutLoud application and/or shared with a service provider for fulfillment of marketing tactics.
	Restricted Data is classified as a combination for First Name, Last name or First Initial and Last name in combination with any of the following: ● Medical Record Data ● Financial/Insurance Account numbers ● Username/Passwords
2.	**Private-MSP Data:** In context of storage/processing/transfer within SproutLoud application or shared with a service provider for fulfillment of marketing tactics.
	Private Data is classified as a combination for First Name, Last name or First Initial and Last name and Address/Phone/Email in combination with any of the following: ● Invoices and Payment receipts ● Device identifiers and serial numbers ● Client account or policy numbers of its customers
3.	**Public-MSP Data:** In context of storage/processing/transfer within SproutLoud application or shared with a service provider for fulfillment of marketing tactics. Any or all of this data is public and can be purchased from a thid-party provider for a fee.
	Public Data is classified as a combination for First Name, Last name or First Initial and Last name in combination with any of the following: ● Physical Address

	• Public facing Agent/Contractor Certificate/license numbers • Email address • Phone number • Fax Number • Website URL • Facebook/Twitter/Instagram or any social handle

Revision History

Date of Change	Responsible	Summary of Change	Version ID
11/2018	Anjan Upadhya	Initial Release	1.0
09/2019	Anjan Upadhya	Added Appendix B	1.1