Data Management Policy

|  |  |
| --- | --- |
| Owner |  |
| Approver |  |
| Last Reviewed |  |

Scope: All [Company Name] Information Systems

**Roles and Responsibilities Policy**

**Classification Highly Confidential Confidential Private**

**Public**

**Data Handling**

**APPENDIX A  Internal Data Retention Procedure APPENDIX B  Data Retention Additional Guidance**

# Roles and Responsibilities

[Company Name] Personnel  [Company Name] personnel are responsible for protecting the information and devices under their control, understanding and complying with [Company Name]ʼs Information Security policies, and reporting any suspicious system activity to management and the Security team (security team contact).

Data Owner  This is an individual, organization, or entity that determines the value and classification of the data and associated system(s) assigned to them and provides appropriate disclosure, distribution, and protection requirements. The Data Owner has primary responsibility for the data assigned to them whether it is in their custody or in the custody of others. System owners are responsible for data within their systems.

# Policy

[Company Name] classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Information systems and applications shall be classified according to the highest classification of data that they store or process.

For AI guidelines and data, please refer to:

[Company Name] Guidelines for Use of AI Tools

# Classification

To help [Company Name] and its employees easily understand requirements associated with different kinds of information, the company has created four classes of data.

# Highly Confidential

Highly confidential data consists of the most sensitive business information that requires the highest level of scrutiny to ensure limited access to only authorized [Company Name] Personnel. Highly confidential data includes all customer data submitted to [Company Name]ʼs service Event Data).

# Confidential

Confidential data includes [Company Name] proprietary information requiring thorough protection; access is restricted to employees with a “need-to-knowˮ based on business requirements. Examples include:

 Company financial and banking data  Employee PII

 Salary, compensation and payroll information  Strategic plans

 Incident reports

 Risk assessment reports

 Technical vulnerability reports  Authentication credentials

 Secrets and private keys

 Proprietary source code  Litigation data

# Private

Private data includes data that can only be distributed outside the company with approval. This is default for all company information that is not “highly confidentialˮ or “confidentialˮ unless stated otherwise. Examples include:

 Internal policies

 Legal documents

 Meeting minutes and internal presentations  Contracts

 Internal reports  Slack messages

 Internal email records

# Public

Public data includes all data which can be freely distributed outside [Company Name] or is publicly available. Examples include:

 Marketing materials  Product descriptions  Release notes

 External facing policies

 Business contact information

# Data Handling

## Highly Confidential Data Handling

Highly confidential data is subject to the following protection and handling requirements:

 Access for non-pre approved roles requires documented approval from the data owner

 Access is restricted to specific employees, roles and/or departments

 Systems with Highly Confidential data shall not allow unauthenticated or anonymous access

 Highly Confidential Customer Data shall not be used or stored in non-production systems/environments

 Highly Confidential data shall be encrypted in transit over public networks  Backups with Highly Confidential Data shall be encrypted

 Highly Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CDʼs, or DVDʼs

 Hard drives and mobile devices used to store Highly Confidential information must be securely wiped prior to disposal or physically destroyed

 Transfer of Highly Confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

## Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

 Access is restricted to users with a need-to-know based on business requirements

 Systems with Confidential data shall not allow unauthenticated or anonymous access

 Transfer of confidential data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner

 Paper records shall be securely stored and disposed

 Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed

## Private Data Handling

Private data is subject to the following protection and handling requirements:  Access is restricted to users within the organization.

 Transfer to people or entities outside of the company shall only be done when accompanied by a business/legal need.

## Public Data Handling

 No special protection or handling controls are required for public data. Public data may be freely distributed.

## Data Retention

Access, retention, and disclosure of any customer data processed by or stored by [Company Name] is additionally controlled by [Company Name]ʼs [Privacy Policy](https://sentry.io/privacy/) and its customer agreements, including [Terms of Service](https://sentry.io/terms/).

[Company Name] data records must be held in compliance with all applicable legal, regulatory, and contractual requirements; including those related to international regulation.

Once data is no longer needed, it shall be securely disposed or archived as according to data deletion standards defined within this policy. Data owners, in consultation with legal counsel, may determine retention periods for their data. Retention periods shall be documented in the Data Retention Matrix in Appendix B to this policy. Additional retention policies developed subsequently (i.e. department- specific) will be maintained in the [Company Name] internal repositories and linked within Appendix B.

## Data Deletion

Data classified as confidential or highly confidential shall be securely deleted when no longer needed. [Company Name] shall assess the data and disposal practices of third-party vendors in accordance with the Vendor Management Policy. Only third-parties who meet [Company Name] requirements for secure data disposal shall be used for storing and processing confidential or highly confidential data.

[Company Name] shall ensure that all confidential and highly confidential data is securely deleted from company devices prior to, or at the time of disposal.

Customers are able to delete their own Event Data and additionally request deletion of data from [Company Name].

## Labeling

Labeling sources of information according to their direct classification level in the company is not mandatory due to the potential risk that may arise from clearly indicating the importance of information.

However, confidential and highly confidential information documents must be marked as "Restricted."

Owners of information assets are responsible for classifying information assets and labeling their containers. Legal and Compliance can periodically verify compliance with the company's requirements by initiating internal audits.

|  |  |
| --- | --- |
| **Information storage** | **Required labels** |
| Electronic and printed documents | The label must be present on every page of the document. |
| Emails | Mark an email when sending confidential information. |
| External media | External data carriers intended for long-term storage of information must be marked. |
| Information assets received from third parties | Information the company receives from third parties that cannot be classified is considered information for internal use and is not subject to special marking. Except when this information includes company information so that it is easily identifiable and requires labeling. |

## Data Protection

[Company Name] shall hold annual data awareness and data privacy trainings to ensure data protection standards and best practice are communicated across the organization.

## Review

Management shall review data retention requirements during the annual review of this policy.

## Legal

Under certain circumstances, [Company Name] may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by [Company Name] legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to review with [Company Name]ʼs legal counsel to evaluate continuing requirements and scope.

## Data Anonymization

Data processed by the supplier will not be combined with other data sets to increase the identifiability of a data subject.

## Exceptions

Requests for an exception to this policy must be submitted to the ISMS Committee for approval.

## Violations and Enforcement

Any known violations of this policy should be reported to the Legal Counsel. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

## Standard

The following areas of the ISO/IEC 270012013 standard are addressed by this document:

* 1. Asset management
     1. Information classification
        1. Classification of information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** | **Approved by** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# APPENDIX A – Internal Data Retention Procedure

For more practical day to day guidelines, please refer to:

[Company Name] Rules for Handling Customer Data

[Company Name]ʼs Engineering Operations team is responsible for setting and enforcing the data retention and disposal procedures for [Company Name] systems which manage data.

## Customer Accounts:

 Event data is tied to the customerʼs organization. Any customer event data which has been backed up will be inaccessible, but will be deleted at 90 days.

 Customer registration data (email, organization details) shall be deleted upon request. Organization details are able to be deleted by the user.

**APPENDIX B – Data Retention Additional Guidance**

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Data** | **Description** | **Classification** | **Retention Guidance** |
| Usage Data | Metadata gathered on the usage of the [Company Name] service.  i.e - how often did a customer click on x function. | Confidential | Retain at a minimum for as long as customer continues to use [Company Name] services or has an account with [Company Name]. |
| Customer Registration Data | Customer data used to sign up for [Company Name], i.e. email, name, billing information.  Separate from customer  event data. | Confidential | Retain at a minimum for as long as customer continues to use [Company Name] services or has an account with [Company Name]. |
| Event Data | Data sent from customers to [Company Name] for monitoring and analysis. | Highly Confidential | 90 days unless the customer account is deleted.  If customer organization account is deleted, within 24 hours of organization deletion. |
| Employee Data | [Company Name] Employee PII | Confidential | Retain for the duration of employment + minimum 6 years after employment. |
| Financial Data | Internal financial data i.e. Accounts Payable/Receivable Ledgers, Financial Statements. | Confidential | Minimum 7 years |