 Policy

# ****Company Data Retention and Disposal Policy****

## ****1.0 Purpose****

The purpose of this policy is to mitigate threats of non-compliance with regulatory, legal and contractual requirements regarding data retention and disposal policies.

## ****2.0 Scope****

This policy applies to all data assets of Company, whether owned or provided by a third party. Company data assets include, without limitation: Intellectual Property (IP), Personally Identifiable Information (PII) and Personal Health Information (PHI) for employees, customers, other third parties, Business-Sensitive Information (BSI), financial information, other non-public data or information assets deemed the property of Company.

## ****3.0 Roles and Responsibilities****

### ****3.1. Data Owners****

A data owner is a person who is ultimately responsible for the data and information being collected and maintained by their department or division. All data within Company must be assigned a data owner, either directly or indirectly, through their roles and responsibilities in the organization. The responsibilities of the data owners include defining data retention, destruction and/or de-identification (including data de-identification of PII after collection if it is not required) requirements and making sure they are enforced.

### ****3.2. Data User****

A data user is aperson or an entity that interacts with, accesses, uses or updates data to perform a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended and comply with this policy and all policies applicable to such data use.

## ****4.0 Retention of Data****

### ****4.1 Retention of Business-Sensitive and Financial Information****

***Note***: The retention period suggested below is for reference only based on general best practices. Customers are advised to review and update the data/record types and associated retention periods based on their industry and as per applicable legal and regulatory requirements in their specific geography.

Company’s Business-Sensitive and Financial Information shall be retained per the schedule below:

|  |  |
| --- | --- |
| **Data/Record Types** | **Retention Period** |
| Financial Records like Account Payable and Receivable Ledgers | Seven years |
| Financial Statements such as General Ledgers, Chart of Accounts, Stock and Bond Records | Permanent |
| Contractual/ Lease Agreement or any other Legal Documentation | Seven years after expiration |
| Employee Payroll and Insurance Records | Permanent |
| Contractor Payment Records or other Expense Reports | Seven years |
| Invoices - to Customers or from Vendors | Five years |
| Board Meeting Minutes | Permanent |
| Emails – Internal and External | 12 months |
| Electronic Documents | Depends on the subject matter |
| Internal Audit and Risk Assessment Reports | Five years |

### ****4.2 Retention of Personally Identifiable Information (PII) and Personal Health Information (PHI)****

All PII and PHI data shall be retained for as long as there is a business purpose or a legal requirement to do so.

All temporary files containing personally identifiable information must be protected while they exist.

Data de-identification shall be performed before the archival of the data set.

\*\*\*

Policy Conditions for HIPAA:

Company shall retain policies and procedures, assessment records and any documentation required to be maintained by HIPAA for six years from the date of its creation or the date when it last was in effect, whichever is later.

\*\*\*

**4.3 Retention of Customer Data**

All active customer data shall be retained for as long as the customer continues to be an active customer of Company or unless the active customer has requested the deletion of data.

All customer data, after the termination of a contract, must be retained per the contractual agreement between the customer and Company.

Customer data retention policies may be implemented against customer data on an ad-hoc basis as may be agreed between Company and the customer.

\*\*\*

Policy Conditions for PCI DSS:

### ****4.4 Retention of Cardholder Data (CHD)****

Company shall limit the retention of all CHD to a minimum in accordance with the required legal, regulatory and/or business needs. CHD shall only be stored in approved locations and disposed of when no longer required.

\*\*\*

## ****5.0 Data Disposal****

### ****5.1 Customer Data Disposal****

Disposal of customer data will be carried out in accordance with the contractual agreement between Company and the customer. In the absence of any contractual agreement, an automatic script or manual script (for ad-hoc requests) shall be initiated on any Company platform containing customer data. This activates a full hard delete of customer data on the platform.

\*\*\*

Policy Conditions for PCI DSS:

### ****5.2 Disposal of CHD****

Company shall securely delete or dispose of CHD to prevent the data from being recreated or re-rendered. A quarterly process shall be established for identifying and securely deleting stored CHD that exceeds defined retention.

\*\*\*

### ****5.3 Other Data Disposal, Including Company’s Business-Sensitive Information (BSI)****

All electronic documents containing Company’s BSI must be purged upon reaching its retention life span.

All printed material (i.e., hardcopy documents, paper records) must be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, or pulping to ensure personally identifiable information (PII) is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

Company shall securely erase or destroy all temporary files containing personally identifiable information (PII) as per applicable privacy regulations once they are not required.

## ****6.0 Suspension of Disposal in the Event of Litigation or Claims****

In the event Company is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning Company or the commencement of any litigation against or concerning Company, such employee shall inform Management. Any further disposal of documents shall be suspended until Management, with the advice of counsel, determines otherwise. Management shall take such steps as is necessary to promptly inform all staff of any suspension in further data disposal.

A screenshot of a computer

Description automatically generated