**<Your Company Logo>**

**Data Retention and Destruction Policy**

# 

# ***Version Control Table***

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Updated |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

|  |  |
| --- | --- |
| **Date of Next Revision** | **<date>** |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status and at yearly intervals after that.

The version control table will show the published update date and provide a thumbnail of the significant change. CAUTION: the thumbnail is not intended to summarize the difference and is not a substitute for reading the full text.

# 

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_1t3h5sf)

[**Table of Contents 5**](#_2s8eyo1)

[**Purpose 6**](#_3rdcrjn)

[**Scope 6**](#_26in1rg)

[**Policy 6**](#_lnxbz9)

[Reasons for Data Retention 6](#_35nkun2)

[Retention Requirements 6](#_1ksv4uv)

[Data Destruction 7](#_44sinio)

[Disposal of Information Technology Assets 7](#_2jxsxqh)

[Data Retention and Data Destruction procedure 7](#_z337ya)

[**Disciplinary actions 7**](#_3j2qqm3)

[**Change, Review, and Update 8**](#_1y810tw)

[**Responsibility 8**](#_4i7ojhp)

[**Reference 8**](#_2xcytpi)

[**Related Documents 8**](#_1ci93xb)

# 

# Purpose

The purpose of this document is to ensure the company’s guidelines for retaining different types of data.

# Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third party that uses <Company> information assets or information resources and services.

# Policy

## Reasons for Data Retention

* Litigation
* Regulatory compliance requirements
* Data owner requirement
* Security incident investigation

## Retention Requirements

* Operational data can be retained for 1 year;
* Confidential data must be retained as long as the information is needed. Its purpose defines the period of retention for this type of data;
* Critical data including Tax and VAT: critical data must be retained permanently;
* Recruitment details: interview notes of unsuccessful applicants will be held for 3 years after the interview. This personal data will then be destroyed;
* Personal employee data: general employee data will be held for the duration of employment and then for 3 years after the last day of contractual employment. Employee contracts, Candidate CV, Job offer letter, and Onboarding lists will be held for 3 years after the last day of contractual employment;
* Contracts with the clients (NDA, MSA, SoW) must be retained permanently;
* Bank account documentation must be retained permanently;
* Payrolls must be retained for 10 years;
* Visitor logs and CCTV footage are retained for 6 months;
* Electronic systems logs are retained for 90 days.

## Data Destruction

<Company’s> responsibility is to perform proper data destruction techniques upon the expiration of the time frame specified above.

## Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the company’s network communications. When such assets are decommissioned, the following guidelines must be followed:

* Any asset tags or stickers that identify the company must be removed before disposal.
* Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
* At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make methods for data wiping. Alternatively, the company has the option of physically deleting the data unrecoverable.

<Company> explicitly directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to themself or destroying data to cover up a breach of law or company policy.

## Data Retention and Data Destruction procedure

The review of <Company’s> terminated contracts for ensuring that all client data was securely purged conducted once a year.

The review of client information for identifying any information that has exceeded its retention period conducted once a year. There are two types of data retention review procedures:

* Customer data retention review. The project manager can agree on what customer’s data should be destroyed due to the terminated contract. Then the Security Engineer is responsible for assigning the task to purge all related data when IT Operations are accountable for executing the request and engaging other departments if needed.
* Employee data retention review. HR is responsible for the procedure implementation.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 A.8.3.2 Disposal of Media
* ISO 27001 A.8.3.1 Management of Removable Media
* ISO 27001 A.8.2.1 Classification of Information

# Related Documents

* <Company> Data Classification Policy