DATA HANDLING & RETENTION POLICY

*Revision: r1.0*

*Effective Date:*

*Classification: INTERNAL*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX Limited; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX Limited.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Data Handling & Destruction 4

2.2 Data Retention 4

2.3 Data Asset Information 4

2.4 Storage Instance Minimisation 4

2.5 Data Masking 5

2.6 Requests for Data Asset Access 5

2.7 Data Asset Logging & Monitoring 5

2.8 Data Leakage Prevention 5

2.9 Data Destruction 5

3. Policy Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 6

4. Exception Process / Glossary 7

4.1 Exception Process 7

4.2 Glossary / Acronyms 7

5. Document Management 8

5.1 Document Revision Log 8

5.2 Document Ownership 8

5.3 Document Coordinator 8

5.4 Document Approvers 8

5.5 Document Distribution 8

6. Appendix A - Table of Data Stores 9

6.1 Record of Assets 9

7. Appendix B - Role Access 10

7.1 Record of Role Access 10

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Objective

The objective of this policy supplemental is to detail all data storage and role access requirements for data at classification levels Internal, CONFIDENTIAL and RESTRICTED.

Most regulatory compliance programs require organisations to not only keep track of the data they have, but to justify its retention beyond an established business need and to ensure use and processing of the data is within the regulatory requirements. Access to this data must be equally well tracked, and these ‘privileged access’ credentials assigned only to named individuals.

## Scope

### Applicability to Employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all Employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001- Information Security Policy Framework*
* *XXXX-POL-ALL-004 - Data Classification Policy*
* *XXXX-PRC-ALL-003 - Data Backup & Media Handling Procedure*
* *XXXX-STD-ALL-011 Data Handling, Retention and Destruction Standard*

# Policy Statements

## Data Handling & Destruction

All XXXX data assets must be handled in compliance with the *XXXX-STD-ALL-011 Data Handling, Retention and Destruction Standard. This covers the processing, use and security of data in XXXX*

## Data Retention

Every instance of data retention as it relates to Internal, CONFIDENTIAL or RESTRICTED must be fully justified against one or more of the following (not all inclusive):

* Local, Regional, or National Law;
* Industry specific regulations or compliance; and/or
* Client and partner dependent service level agreements

## Data Asset Information

For each instance of data storage, the following information must be included at a minimum;

|  |  |
| --- | --- |
| * *Data Store Name:* | Either the database table, or commonly accepted name of the stored data entity |
| * *System Name:* | The hostname or the commonly accepted name of the storage system |
| * *System Location:* | Physical location of system |
| * *Data Type:* | i.e. cardholder data, personally identifiable information, intellectual property |
| * *Data Classification:* | Confidential or Restricted |
| * *Retention Period:* | How long (in months) the data is to be retained |
| * *Business Justification / Applicable Regulation:* | Full justification for the retention of the data, and details of any Industry / Government regulation with which the information asset must comply |
| * *Data Owner:* | Name of Data Owner |
| * *Data Custodian:* | Name of data custodian to whom the Data Owner has delegated functional responsibility for a data asset |

## Storage Instance Minimisation

The default for storage of Confidential or Restricted data assets is a ‘single instance’, with security controls in place per the *XXXX-POL-ALL-005 Data Handling and Retention Policy*

Request for multiple instances must be approved by the Data Owner in writing and recorded as a separate data asset.

## Data Masking

Where possible, access to Confidential or Restricted should be masked, truncated, or in some other way minimised.

## Requests for Data Asset Access

All requests for access to Internal, Confidential or Restricted data assets must be formally recorded, approved by the Data Owner, and recorded as a form of ‘Privileged Access’.

## Data Asset Logging & Monitoring

All access to / use of Internal, Confidential or Restricted data assets must be recorded with individual’s name or system username, and date/time stamps.

## Data Leakage Prevention

Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

## Data Destruction

For every data asset that has exceeded the retention period, documented evidence must be available from the Data Owner that the destruction has taken place in accordance with the *XXXX-STD-ALL-011 Data Handling, Retention and Destruction Standard.*

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| For a selection of XXXX information assets, obtain evidence that the data storage is officially recorded. | * Information asset (e.g., application) inventory listing, including asset owners * Output from asset management tools / systems * Output from risk assessment (e.g. GRC, DLP) tools |
| For a selection of XXXX information assets, obtain evidence that access requests are formally approved by the Data Owner. | * Role Access Log * Help desk request logs |
| For a selection of XXXX information assets, obtain evidence that any data storage past its retention period has been securely destroyed. | * Information asset (e.g., application) inventory listing, including asset owners * Output from asset management tools / systems |
| For a selection of XXXX information assets that have been destroyed, obtain documented evidence from Data Owner. | * Information asset inventory listing from each asset owner |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| XXXX | XXXX |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Policy is owned by YYYY.

## Document Coordinator

This Policy is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

The distribution of this document is to all staff

# Appendix A - Table of Data Stores

## Record of Assets

In the absence of a suitable asset management system, the following table will suffice if it is appropriately labelled and protected:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Store Name** | **System Name** | **System Location** | **Data Type** | **Data**  **Classification** | **Retention Period** | **Business Justification / Applicable Regulation** | **Data Owner** | **Data Custodian** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

# Appendix B - Role Access

## Record of Role Access

In the absence of a suitable user management system, the following table will suffice if it is appropriately labelled:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Asset** | **Requestor** | **Read / Write**  **Access?** | **Data Masking** | **Business Justification** | **Temp or Perm?** | **Exp.** | **Data Owner** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |