DATA CLASSIFICATION POLICY

*Revision: r1.0*

*Effective Date: dd-mm-yyyy*

*Classification: INTERNAL*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX; 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.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to all employees (contract, termed & permanent). 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 4

2. Policy Statements 5

2.1 Data Ownership 5

2.2 Assigning Classifications 5

2.3 Information Classification Levels 5

2.3.1 PUBLIC 5

2.3.2 INTERNAL 6

2.3.3 CONFIDENTIAL 6

2.3.4 RESTRICTED 6

2.3.5 Data Classification Summary Table 7

2.3.6 Electronic Information Access Matrix 8

2.4 Minimum Classification 8

2.5 Information Release 8

2.6 Information Control 8

2.7 Delegation and Accountability 8

2.8 Data Custodian 9

2.9 Data Collection / Groups 9

2.10 Labelling & Handling 9

2.11 Periodic Classification Reviews 9

2.12 Periodic Retention Reviews 9

2.13 Human Resources Classification 9

2.14 Privileged Access Reviews 9

3. Policy Compliance & Enforcement 10

3.1 Compliance Measures 10

3.2 Enforcement 10

4. Exception Process / Glossary 11

4.1 Exception Process 11

4.2 Glossary / Acronyms 11

5. Document Management 12

5.1 Document Revision Log 12

5.2 Document Ownership 12

5.3 Document Coordinator 12

5.4 Document Approvers 12

5.5 Document Distribution 12

# 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 is to provide information security requirements for classification of XXXX information assets.

In the context of this Policy, “data asset” and “information asset” are used interchangeably.

An information asset is a definable piece of data, regardless of format, which is recognized as valuable to the organization. Information assets may include but are not limited to all forms and types of business proprietary information/content, customer related information, financial, strategies and processes, analytics, innovation, legal and all employees /personnel data.

In order to provide more appropriate levels of protection to information assets, data must be classified according to the risks associated with its storage, processing, use, transmission or destruction. Consistent use of this data classification policy will facilitate more efficiency for data owners to classify data and assign appropriately security levels relevant to each information asset.

## Scope

### Applicability to all employees (contract, termed & permanent).

XXXX refers to XXXX Ltd 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-005 - Data Handling and Retention Policy*
* *XXXX-POL-ALL-006 - Data Backup and Recovery Policy*
* *XXXX-PRC-ALL-003 -* *Data Backup & Media Handling Procedure*

# Policy Statements

## Data Ownership

Every information system must have a Data Owner.

The Data Owner is the person responsible for, or dependent upon, the business process associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

## Assigning Classifications

The Data Owner must ensure that the classification of information is assigned and properly indicates its business value and level of sensitivity and criticality to the organisation.

## Information Classification Levels

Information owned, used, created or maintained by XXXX must be classified into one of the following four categories:

* PUBLIC
* INTERNAL
* CONFIDENTIAL
* RESTRICTED

### PUBLIC

PUBLIC data is information that may or must be open to the general public. It is defined as information with no existing local, regional, national, or international legal restrictions on access or usage. Public data, while subject to XXXX disclosure rules, is available to all employees and all individuals or entities external to the corporation.

Examples of PUBLIC Data include:

* Publicly posted press releases
* Publicly available marketing materials
* Publicly posted job announcements
* Adverse media reports on open media
* General information offered on Internet sites that does not require a contract, sign-on, etc.

Disclosure of PUBLIC data must not violate any pre-existing, signed non-disclosure agreements.

### INTERNAL

INTERNAL Data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorised access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. INTERNAL Data is information that is restricted to personnel designated by XXXX, who have a legitimate business purpose for accessing such data.

Examples of INTERNAL Data include:

* Training Manuals
* Corporate / Company Newsletters
* Organisational Charts
* Corporate Policies
* Business Information Report, List Products etc
* Sales presentations
* Free downloaded product manuals
* Licensed data
* Customer Validation Reports
* Samples and/or Proof of Concepts with customers, vendors, suppliers, etc.

### CONFIDENTIAL

CONFIDENTIAL Data is information protected by XXXX policies or contractual language. CONFIDENTIAL data is sensitive in nature and access is restricted. Disclosure to parties outside of XXXX must be authorised by appropriate management or covered by a binding confidentiality agreement.

Examples of CONFIDENTIAL Data include:

* Research and Competitive Analysis Data;
* Supplier Relationship Information;
* Applications Portfolio;
* Client Statements of Work (SoW) and Contracts

### RESTRICTED

RESTRICTED Data is information protected by statutes, regulations, XXXX policies or contractual language. RESTRICTED Data is sensitive in nature and access is restricted. Disclosure is limited to individuals on a “need-to-know” basis only. Disclosure to parties outside of XXXX must be authorised by appropriate management or covered by a binding confidentiality agreement. In addition, RESTRICTED Data is information that may:

* Give XXXX a competitive advantage
* Could compromise the privacy of individuals
* Might be detrimental to XXXX interests if its disclosure was unrestricted

Examples of XXXX Data include:

* Personnel and Medical Files
* Customer Credit Card or Other Financial Information
* Corporate Strategic and Marketing Plans
* Trade Secrets
* Product Development Plans, Recipes, Specifications
* Sales and other Financial Results
* Regulatory Reports
* Any data belonging to a XXXX customer that may contain Personally Identifiable Information (PII), or Sensitive Personal Information (SPI)

### Data Classification Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| **CLASSIFICATION** | **LABELLING** | **HANDLING** | **EXAMPLES** |
| **Restricted**   * High Value * Strict Legal Requirements * High Sensitivity * High Criticality to the organization | Restricted | * Restricted refers to the most sensitive business information * Information is restricted to be seen and handled by nominated personnel only * All information in this category should be labelled as Restricted * Confidentiality of this information shall be maintained at the highest level * Password protect information * Removeable media should only be used to store this information if it is encrypted * Destroy any printouts * Do not discuss in public | * Trade secrets * Card Holder Data * Customer information * Core Banking Application (and supporting systems) Information * Financial statements * Business design principles * Strategic plans * Intellectual property of the organisation * Passwords, ATM PIN * Security parameters * Software license key * Authorization codes * Audit Report * Merger and acquisition plans, etc. |
| **Confidential** | Confidential | * Information that cannot be released to any persons outside of the restricted permissions set * Removeable media should only be used to store this information if it is encrypted * Destroy any printouts * Do not discuss in public * Only transmit via email with approval and encryption in place. * Shred all paper copies | * Employee personal records (HCM Files) * Customer personally identifiable information * Project documents * Operational reports of various departments * Audit tools and software, software logs * System documentation and organizational records |
| **Internal** | Internal | * Information that cannot be released to any person outside of XXXX without approval * All XXXX personnel have access to internal information with the permissions that have been set on the Bank’s IT system. | * Policy manuals * Standard operating procedures * Internal circulars * Internal correspondence and memos * XXXX's telephone directory * Training materials * Intranet / web portals, etc. |
| **Public**  Low Value  Few Legal Requirements  Low Sensitivity  Low Criticality to the organization | Public | * Information that may be released to the public, that does not benefit a competitor, negatively impact XXXX or does not breach any confidentiality. * Information that may be published in any public forum without constraints either enforced by law or discretionary. * By default all information is classified as Public unless otherwise classified. | * Service brochures * Advertisements * Job opening announcements * Press releases * Declared/published financial results etc. |

### Electronic Information Access Matrix

| **CLASSIFICATION** | **STAFF** | **VENDORS** | **THIRD PARTIES** |
| --- | --- | --- | --- |
| **Restricted** | * Information Owners. * Executive management and SBU Heads. | Except on legal advice. | Except on legal advice. |
| **Confidential** | * Information owners. * Information processors within the scope of their function. * Subject of information. | Where duly signed NDA exits. | Except on legal advice. |
| **Internal** | Full Access | Where duly signed NDA exits. | Except on legal advice. |
| **Public** | Full Access | Full Access | Full Access |

## Minimum Classification

All information must be assumed INTERNAL unless classified otherwise.

## Information Release

The Data Owner must communicate the information classification when the information is released outside of the department and / or XXXX locations.

## Information Control

The Data Owner controls access to his / her information and must be consulted when access is extended or modified.

## Delegation and Accountability

If the Data Owner delegates the responsibility of data protection to a Data Custodian, the Data Owner must retain full accountability for the security of the information.

## Data Custodian

The Data Custodian must maintain the protection of data according to the information classification associated to it by the Data Owner.

The Data Custodian role is delegated by the Data Owner and is usually Information Technology personnel.

## Data Collection / Groups

Data Owners 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.

## Labelling & Handling

XXXX (UK) Limited INTERNAL, CONFIDENTIAL, and RESTRICTED information must be labelled, handled, stored, transmitted (internally or externally), and ultimately reclassified or destroyed, in a manner that prevents inadvertent disclosure or compromise.

All individuals employed by XXXX have the responsibility to protect the confidentiality, integrity, and availability of information assets, irrespective of the medium on which the data resides (i.e. electronic, paper or other physical form etc.).

## Periodic Classification Reviews

Information asset classifications must be reviewed by the Data Owner at least every year or when necessary based on business need.

## Periodic Retention Reviews

Information asset retention must be reviewed by the Data Owner at least every year and any exceptions treated according to the *XXXX-PRC-ALL-003 - Data Backup & Media Handling Procedure*.

## Human Resources Classification

By default, all data and documents from Human Resources are classified as Confidential, unless otherwise stated so by Human Resources

## Privileged Access Reviews

Access to data assets classified as INTERNAL, CONFIDENTIAL and RESTRICTED is deemed ‘Privileged Access’ and continued access must be reviewed on a yearly basis by the Data Owner.

# 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, verify evidence of data ownership. | * Information asset (e.g., application) inventory listing, including asset owners * Output from asset management tools / systems * Output from risk assessment (e.g., Governance, Risk and Compliance – GRC) tools |
| For a selection of XXXX information assets, obtain evidence of documented information classifications. | * Information asset (e.g., application) inventory listing, including asset owners * Output from asset management tools / systems * Output from risk assessment (e.g., Governance, Risk and Compliance – GRC) tools |
| For a selection of XXXX information assets, verify that information labeling and handling requirements are implemented. | * Evidence assets and information are labelled with the right criticality and appropriately handled. * Management reviews and audits that showed unlabelled assets and information |
| For a selection of XXXX information assets, obtain evidence that information classifications are reviewed on a periodic basis. | * Physical sign-off of asset inventory listing * Electronic sign-off via asset inventory, GRC tools, email, etc. |

## 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

|  |  |
| --- | --- |
| Intellectual Property | Ideas and/or creations of the mind, including but not limited to inventions, designs, processes, symbols, names, images, and designs used in commerce. |
| PII | Personally Identifiable Information |
| SPI | Sensitive Personal Information |
| PCI DSS | Payment Card Industry Data Security Standard |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
| dd-mm-yyyy |  | r1.0 | Approval by Executive Committee and aligning restricted document treatment with standards |

## Document Ownership

This Policy is owned by the Executive Committee

## Document Coordinator

This Policy is coordinated by the CISO

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
| Executive Committee |  | dd-mm-yyyy |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff