INFORMATION SECURITY DOCUMENT MANAGEMENT STANDARD

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*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 Employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Standard Statements 4

2.1 Definitions 4

2.2 Procedural Documents 4

2.3 Responsibilities 4

2.4 Development of Procedural Documents 5

2.5 Templates 6

2.6 Document title and version control 6

2.7 Publication 6

2.8 Monitoring 7

2.9 Review 7

2.10 Policy Intranet Site 7

2.11 Primary Attributes 7

3. Standard Compliance & Enforcement 9

3.1 Compliance Measures 9

3.2 Enforcement 9

4. Exception Process / Glossary 10

4.1 Exception Process 10

4.2 Glossary / Acronyms 10

5. Document Management 11

5.1 Document Revision Log 11

5.2 Document Ownership 11

5.3 Document Coordinator 11

5.4 Document Approvers 11

5.5 Distribution 11

# Introduction

## Document Definition

This document is a Standard.

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

## Objective

This document sets out XXXX system for the development, implementation and management of procedural documents such as policies, standards, procedures and guidelines. The policy provides information and guidance in the form of procedural documents to ensure that policies, procedures and processes are carried out in the correct way. The procedural documents must be accurate, up to date, readable, always fit for purpose and available to relevant staff. Procedural documents may define best practice, latest standards or regulations, or new legislation.

## Scope

### Applicability to Employees

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

### Applicability to External Parties

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

### Applicability to Assets

This Standard 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-002 - Acceptable Use Policy*
* *XXXX-POL-ALL-004 - Information Classification Policy*

# Standard Statements

## Definitions

* **Consultation**: A process by which stakeholders are requested to provide comment on a draft document. It is advisable for an author to consult relevant stakeholders before a document is submitted for approval and clarify their input in the version control.
* **Publication:** When the term publication is referred to, this means the document is posted onto the XXXX’s intranet/shared folders to ensure availability for all staff.
* **Review:** Most procedural documents will require a review annually to ensure it is still relevant, still reflects local practice and complies with any new recommendations or legislation.
* **Version Control:** The process used for tracking the development of a document is called version control. The XXXX uses a version number to track the development of her documents and an incremental number is used together with the change description.

## Procedural Documents

**Policy**

A Policy is a set of directional statements and requirements aiming to protect corporate values, assets and intelligence. Policies serve as the foundation for related Standards, Procedures, Processes, and Guidelines.

**Standard**

A Standard is a set of practices and benchmarks employed to comply with the requirements set forth in the Policies. A Standard should always be a derivation of a Policy, as it is the second step in the process of an organisation’s Policy propagation.

**Procedure**

A Procedure is a set of step-by-step instructions for implementing Policy requirements and executing Standard practices.

**Guideline**

A Guideline is a non-mandatory best practice guide designed to help all employees understand some of the more difficult IT concepts. e.g. choosing a strong password.

## Responsibilities

* **Executive Management**

The Executive Management is responsible for:

Seeking assurance that the systems for the development and management of procedural documents are robust and effective.

* **Security Committee**

The Security Committee is responsible for:

Ensuring the XXXX has a system for the management and timely publication of an appropriate Procedural Management System

Ensuring a timely review process is implemented to ensure procedural documentation is updated as per the guidance.

Escalating any shortfalls in policy requirement to the Executive Management

* **CISO/Document Coordinator**

The Information Security Officer/Document Coordinator is responsible for:

Ensuring the process for the development and management of XXXX procedural documents is robust.

Providing reports on the status of policies as required

Maintaining and improving the XXXX’s process for procedural document development and management.

Ensuring that a robust archiving system for procedural documents is in place.

Ensuring the publishing approved procedural documents on the Trust’s Intranet/Shared folders.

Communicating to staff when new or revised procedural documents have been published.

Providing guidance to authors regarding the development of procedural documents

Maintaining a registry of procedural documentation

Make changes and adjustments to documents, disseminate and sends for approval at the next approval at the next review date

Alerting authors of procedural documents that their review dates are approaching.

* **Author**

The author is responsible for:

Identifying when a document is required and ensuring if follows the agreed practice and procedure

Ensuring the content and details of the procedural document are accurate, meet best practice and national guidance, and conform to relevant legislation.

Ensuring that the appropriate template is used and completed.

Consult with stakeholders in the development of the document.

Follow the agreed approval process and gain approval from the necessary specialists

Maintaining and updating the document control report.

Ensuring the document is archived in the relevant department or team procedural document archive.

Reviewing the document at the agreed interval.

Arranging for the withdrawal of the document if required

* **Line Managers**

Line managers are responsible for:

Ensuring their staff are aware of relevant procedural documents relating to their roles and responsibilities.

Implementing the procedural documents for the areas in which they apply.

* **Approving Officers**

Approving Information security policies is vested with the CEO, but this can be delegated to the Security Committee

## Development of Procedural Documents

When the need for a procedural document is identified, the author will use the relevant template which is published on the XXXX’s intranet in the policy hub section of the intranet.

It is intended that the author will populate the template detailing the process or procedure that is locally used. Then pass the document to the stakeholders for comment, once the comments have been received the author will amend the policy and arrange for approval at a relevant group or committee.

The document needs to be written in plain English with no jargon.

Wherever a procedure can be illustrated as a flowchart this should be included to provide a clear process without lengthy explanation and words.

When the document has been approved it can be sent to the IT/Information Security team who will publish the document and confirm this has been done to the author.

An implementation plan should accompany a policy sent to a group or committee for approval. This plan should detail how the author intends to let the XXXX’s Staff know that the policy/procedural document is now available.

Documents should be written in plain English with little use of abbreviations and acronyms. Abbreviations and acronyms should only be used if they have been written in full the first time they are referred to or explained in the abbreviation explanation section of the document.

Most Standard Operating Procedures or Procedures can be illustrated as a flowchart showing the procedures, this will negate the requirement for a full document.

Job titles should be used rather than individual names.

Sub processes should be added as appendices.

The title of the document should reflect what the document is for. Titles should not start with policy or guideline.

## Templates

Templates are available on the XXXX's Intranet in the policy hub section. There are several templates available:

Policy Template

Standard Template

Procedure Template

The templates are the corporate style of Calibri Size 11 font.

## Document title and version control

When a document is first written as a draft the version numbering should start as 0.1, with each subsequent revision given in sequential order. Once the document has been approved and is ready for publishing it will be given the next whole number, such as 1.0.

## Publication

Once a document has been approved, the author will send a copy to the IT/Information Security team for publication on the XXXX’s intranet site on policy hub

The latest version of a procedural document will be available to staff on the XXXX’s intranet site.

The document will be published as a PDF by the IT/Information Security Team and a listing will be posted on the front page of the policies site of the most recently published documents.

## Monitoring

The author will need to identify what form of monitoring will be used to enable assessment of compliance. Monitoring may take the form of audits, reports, feedback, results of complaints or incidents, sample surveillance, spot checking, documented observations, or feedback.

A document can be revised to reflect minor changes and changes that do not changethe structure of the document such as departmental changes.

This can be recorded on the document control report, but the document can be published with the revision until the review date without going through the full approval process.

## Review

The Information Security Officer/ Document Coordinator will remind the author 3 months before the policy is due for review. If no response is received and escalation process will be implemented, where the line manager will be asked if the policy is still required or can it be removed.

Procedural documents must be reviewed at least annually to ensure they are still relevant.

The author will review the document and consult with the Stakeholders prior to arranging for approval at the relevant group or committee, prior to re-publishing.

## Policy Intranet Site

Procedural documents are published on the XXXX's intranet site under the Policy hub section

The Information security team will ensure relevant information security procedural documents are always maintained in this site with support from IT.

## Primary Attributes

The table below describes the basic attributes of documentation

|  |  |
| --- | --- |
| **Section** | **Description** |
| Document Name | A user-friendly name that gives an indication as to the content |
| Document Number | Unique number, obtained from the **Error! Unknown document property name.** |
| Revision | Whole number for major change (e.g. rX.0), decimal changes for minor changes (e.g. rX.1), incremented from previous revision |
| Document Status | DRAFT, RELEASED, APPROVED, OBSOLETE |
| Effective Date | Date from which the current (RELEASED) revision is effective |
| Document Type | Identifies and defines the document type (e.g., Policy (POL), Standard (STD), Procedure (PRC), Guideline (GDL), etc.) |
| Scope & Objective | States the policy’s objectives and goals and describes the policy’s impact within XXXX’s organisational structure and enterprise environment |
| Applicability to employees, External Parties, and/or Assets | Defines the applicability of the document to XXXX’s employees (employees, consultants, contractors) and external parties/entities, and assets if applicable) |
| Related Documents / References | Identifies related documents to the topic or referenced within the Policy / Standard / Guideline plus others as stated above |
| Policy / Standard / Guideline Statements | States the specific Policy / Standard / Guideline requirements that meet the document’s objectives |
| Compliance Measures | Provides recommended compliance measures and example evidence that can be used to review compliance with the Policy / Standard / Guideline statements |
| Enforcement | Provides legal language regarding enforcement of the Policy / Standard / Guideline in question |
| Exception Process | Provides a reference to the XXXX exception procedure in the event that a deviation to the Policy is requested |
| Glossary / Acronyms | Provides definitions for acronyms and technical terminology |
| Document Management | Defines the document Revision History, Authorship / Ownership / Approvers / Coordinators, and Effective Date |

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. 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** |
| The number of up to date information security policy set hosted in policy hub | * Percentage of procedural documents hosted compared to total number of required policy set documents |
| Retrieving of policy set templates | * Ensure Policy set templates are hosted on the intranet and easily accessible to staff |
| Training of staff on the use of policy templates | * Ensure evidence of training records for staff on use of the required templates |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards 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 Standard 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

|  |  |
| --- | --- |
| IT | Information Technology |

# Document Management

## Document Revision Log

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

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

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

## Distribution

The Document Owner controls distribution of this document. The distribution is to all staff: