INFORMATION SECURITY POLICY FRAMEWORK

*Revision:*

*Dated:*

*Classification: INTERNAL*

Table of Contents

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXXXX; 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 XXXXXX

1. Statement from Executive Management 4

2. Introduction 6

2.1 Document Definition 6

2.2 Mission Statement 6

2.3 Objective 6

2.4 Scope 7

2.4.1 Applicability to Employees 7

2.4.2 Applicability to External Parties 7

2.4.3 Applicability to Assets 7

2.5 Document Type Definitions 7

2.5.1 Policy 7

2.5.2 Standard 7

2.5.3 Procedure 7

2.5.4 Terms of Reference 7

2.5.5 Guideline 8

2.6 Related Documents / References 9

3. Policy Statements 10

3.1 Protection of Information by Design and Default 10

3.2 Requirement for Policy Set Documentation 10

3.3 Compliance with Policy & Standard Provisions 10

3.4 Policy & Standard Review Period 10

3.5 Co-Operation with External Organisations 10

3.6 Independent Review of the Information Security Program 11

3.7 Continual Improvement 11

3.8 Information Security Roles & Responsibilities 11

3.8.1 Board of Directors 11

3.8.2 Executive Committee (EXCO) 12

3.8.3 Security Committee (SC) 13

3.8.4 Information Technology (IT) 13

3.8.5 Document Coordinator(s) 14

3.8.6 Internal Audit 14

3.8.7 Data Owner 15

3.8.8 Line Management 15

3.8.9 User 16

3.9 Documentation Development 17

3.10 Policy Format, Naming Convention, & Required Language 18

3.11 Policy & Standard Exceptions 18

3.12 Clear Desk & Clear Screen Policy 18

3.13 Operational Procedures 18

3.14 Change Management 19

3.15 Capacity Management 19

3.16 Segregation of Duties 19

3.17 Information Security in Project Management 20

3.18 Background Checks 20

3.19 Delegation of Information Security Tasking 20

4. Policy Compliance & Enforcement 21

4.1 Compliance Measures 21

4.2 Enforcement 21

5. Glossary / Acronyms 22

5.1 Glossary / Acronyms Table 22

6. Document Management 23

6.1 Document Revision Log 23

6.2 Document Ownership 23

6.3 Document Coordinator 24

6.4 Document Approvers 24

6.5 Document Distribution 24

# Statement from Executive Management

Information security aims to protect information and information assets and ensure business continuity by preventing and minimizing the impact of information security incidents. Information security provides the trusted environment that the The organisation needs to be confident in adopting efficient new ways of doing business. Information security deals with all aspects of information (spoken, written, printed, electronic or any other medium) and information handling (created, viewed, transported, stored or destroyed).

XXXXX (Name of Org) will seek to enhance productivity of the business by reducing the probability of loss through the design and implementation of policies, standards, procedures and guidelines that enhance the protection of business assets.

There are three basic elements to information security that must always be maintained to protect against loss, damage and unauthorized disclosure of information:

* Confidentiality: protecting sensitive information from unauthorized disclosure or interception.
* Integrity: safeguarding the accuracy and completeness of information and computer software.
* Availability: process of ensuring that authorized users have access to information and associated assets when required.

As a modern, forward-looking business, XXXX recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, XXXX has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001:2013 to further strengthen its information security processes.

The operation of this ISMS has many benefits for the business, including:

* Protection of revenue streams and company profitability;
* Ensuring the supply of goods and services to customers;
* Maintenance and enhancement of shareholder value, and;
* Compliance with legal and regulatory requirements.

Commitment to the delivery of information security extends to senior levels of the organisation and will be demonstrated through the information security policy and the provision of appropriate resources to establish and develop the ISMS.

Top management will also ensure that a systematic review of the programme’s performance is conducted on a regular basis to ensure that information security objectives are being met and relevant issues are identified through the audit programme and management processes.

A risk management approach and process will be used which is in line with the requirements and recommendations of ISO/IEC 27001:2013. Risk management will take place at several levels within the ISMS, including:

* assessment of risks to the achievement of our information security objectives;
* regular information security risk assessments within specific operational areas;
* assessment of risk as part of the business change management process, and;
* at the project level as part of the management of significant change.

We would encourage all employees and other stakeholders in our business to ensure that they play their part in delivering our information security objectives.

Sincerely,

Signed.

Chief Executive Officer

# Introduction

## Document Definition

This document is a Policy.

For a full description of document type, see [Document Type Definition](#_Document_Type_Definitions)s below.

## Mission Statement

Policies, Standards, Procedures, and Guidelines are the primary way in which the Board and Executive Committee’s (EXCO) direction and expectations are translated into specific, measurable, and testable goals and objectives. They are a critical component of governance at XXXX as they provide the structure and rules around which the organisation, and all subsidiary organisations, must operate. The Security Committee (SC) has been established to create, maintain, and govern Information Security (IS) Policies, Standards, Procedures, and Guidelines. The SC is responsible for communicating these documents to all applicable partners, joint ventures and subsidiaries, as well as distributing them and/or making them accessible to XXXX’s Employees (including consultants, contractors, and other applicable 3rd party vendors and partners).

## Objective

The objective of the Information Security Policy is to protect the The organisation’s information assets from accidental or intentional loss, disclosure, attack or misuse. All reasonable measures shall be taken to ensure that:

* The The organisation’s information remains confidential;
* The integrity of information is maintained;
* The The organisation’s requirements for the availability of information and the systems used to process information are met;
* Accountability for information is maintained, and;
* All appropriate regulatory and legislative requirements are met in full.

The Information Security Policy sets out supporting policies and standards intended to help the The organisation achieve these objectives.

Compliance with this Information Security Policy is necessary to ensure business continuity, and minimise business damage by preventing the occurrence, and minimising the impact, of information security incidents.

This Policy is based partly on the ‘*International Organisation for Standardisation and International Electro-Technical Commission (ISO/IEC) 27002 Standard, Information Technology - Security Techniques - Code of Practice for Information Security Controls*’. It is further supported by XXXX’s Information Security Policies set listed out in *XXXX-OTH-ALL-001 - Master Records Register.*

## Scope

### Applicability to Employees

XXXX refers to XXXXXX as well as its applicable partners, joint ventures and subsidiaries (where/if applicable). This Policy applies to all Employees including temporary Staff, members of the Board of Directors, external partners/vendors, third parties 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 and facilities globally owned by XXXX, or where XXXX has custodial responsibilities.

## Document Type Definitions

The primary documents that support this Information Security Policy are Polices, Standards, and Procedures. These are defined below.

### 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.

### Terms of Reference

A Term of reference defines the purpose and structures of a project, committee, meeting, negotiation, or any similar collection of people who have agreed to work together to accomplish a shared goal.

### 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.

## Related Documents / References

* *Risk Management Policy*
* *XXXX-PO-ALL-004 - Data Classification Policy*
* *XXXX-STD-ALL-001 - IS Documentation Standard*
* *XXXX-OTH-ALL-001 - Master Records Register*
* *XXXX-PRC-ALL-025 - Policy Exception Procedure*

# Policy Statements

## Protection of Information by Design and Default

It is the Policy of XXXX that information in all its forms: written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

## Requirement for Policy Set Documentation

All supporting Policies, Standards, and Procedures must be documented and must be made available to individuals responsible for their implementation and compliance. All activities identified by the Policies and Procedures must also be documented in appropriate record format (defined in Standard or Procedure).

## Compliance with Policy & Standard Provisions

All business processes and information systems implemented after the effective date of these policies are expected to comply with the provisions of all related Policies and Standards. Existing systems are expected to be brought into compliance as soon as practical.

Information System Owners will work in conjunction with Internal Audit to ensure that information systems are managed, maintained, and processing in a manner that supports compliance with all security requirements.

## Policy & Standard Review Period

All documentation must be reviewed at least annually, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape.

Alternative Policy review timings to be determined by the XXXX Board or Executive Management where applicable.

Alternative Standards review timings to be determined by the XXXX Standard Owner.

## Co-Operation with External Organisations

Contact with relevant external authorities for security purposes must be maintained by the Information Security Committee (SC). This includes law enforcement, Information Service Providers, regulatory bodies, telecommunications companies, trade organizations, specialist security advisors and any other external organization. All communications between XXXX and third-party enforcement agencies must be maintained in confidence.

## Independent Review of the Information Security Program

The SC or the EXCO must initiate an independent review of all relevant aspects of the XXXX Information Security Program at least annually, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape to ensure the continuing suitability, adequacy and effectiveness of the organisation’s approach to managing inherent risks.

The review must:

1. assess opportunities for improvement and the need for changes to the approach to security, including the Policy, Standards and/or control objectives;
2. be carried out by individuals independent of the area under review. These individuals can be internal or 3rd parties, but must demonstrate that they have appropriate skills and experience;
3. be recorded and reported to the SC and the EXCO. These records must be maintained, and;
4. incorporate recommendations for corrective actions.

## Continual Improvement

XXXX policy with regard to continual improvement is to:

* continually improve the effectiveness of the information security program and ISMS;
* enhance current processes to bring them into line with industry good practices and standards;
* maintain ISO/IEC 27001:2013 certification;
* increase the level of proactivity with regard to information security;
* make information security processes and controls more measurable in order to provide a sound basis for informed decisions;
* review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data, and;
* obtain ideas for improvement via regular meetings and other forms of communication with interested parties, internal and external.

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

## Information Security Roles & Responsibilities

### Board of Directors

The Board of Directors are accountable for:

1. defining the business goals to be supported and enabled by the Information Security Program;
2. being ultimately accountable for the maintenance of the Confidentiality, Integrity and Availability of XXXX information and infrastructure assets[[1]](#footnote-2);
3. being accountable for all applicable regulatory and statutory compliance requirements;
4. demonstrating commitment to the continuous improvement, suitability, adequacy and effectiveness of the XXXX Information Security Management System (ISMS);
5. the provision for, and ongoing support to, the XXXX Security Committee;
6. setting of Information Security Policy;
7. setting of Information Security Risk appetite;
8. oversight of Information Security performance, and;
9. to review, rule on, and track IS Policy exception requests.

### Executive Committee (EXCO)

The Executive Committee are responsible for:

1. setting Information Security objectives in-line with business goals, to be reviewed annually or when updated to reflect significant changes to business goals, or the prevailing threat landscape;
2. the implementation of all Policies related to the maintenance of the Confidentiality, Integrity and Availability of XXXX information and infrastructure assets[[2]](#footnote-3), and the enforcement of them;
3. maintaining compliance with applicable regulatory and statutory compliance requirements;
4. the continuous improvement, suitability, adequacy and effectiveness of the XXXX Information Security Management System (ISMS), and;
5. day to day support of the XXXX Security Committee.

The Executive Committee consists of:

* CEO
* Executive Director, Business Development
* Chief Operations Officer (COO)
* Chief Financial Officer (CFO)
* Chief Risk Officer (CRO)
* Head of Internal Audit
* Head of Operations
* Head of Legal
* Head of Treasury
* Head of Compliance
* Head of HR (Human Resources)
* Head of BD (Business Development)
* Head of IT (Information Technology)

### Information Security Committee (SC)

The primary functions of the SC are:

1. to address “at risk” behaviour or performance counter to the XXXX Information Security Policy Set;
2. to set and review IS strategy and vision to align it with the business;
3. review key IS risks in relation to their progress and risk impact.
4. Review of the IS Risk Register to ensure risks are been mitigated
5. to coordinate the creation and communication of IS Policies and Standards;
6. to review/approve Policy Coordinator’s recommendation on the IS Policies and Standards;
7. to provide oversight for communication of IS Policies to all interested parties (internal and/or external), educate the user community, and make them easily accessible;
8. to oversee IS Change Control, and;
9. perform annual performance evaluations of XXXX ISMS objectives, and an annual IS strategy review with Executive Committee

Refer to the Security Committee Terms of Reference (TOR) for details on composition and responsibilities.

With the support of the EXCO, the SC will coordinate the creation and maintenance of XXXX’s Information Security Policies and Standards and ensure that they are appropriately approved, communicated to, and understood by all appropriate parties. Additional Standards, Guidelines, and Procedures may be developed by departmental leadership to meet unique technology, regulatory, legal, or commercial requirements. These supplementary documents must comply with this Information Security Policy Framework and must be submitted to the SC for review and approval.

Within this context, the main role of XXXX’s SC is to provide final review and recommendations for changes and updates to Information Security documentation.

### Information Technology (IT)

General responsibilities include:

1. Management of the XXXX IT risk assessment and management program(s);
2. Providing security expertise and support for all systems and users;
3. Advising Data Owner in the security controls appropriate to an asset’s Information Classification;
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation;
5. Specifying controls and communicating the control requirements to the Data Owners and users of the information;
6. Educating Data Owners, or other owners of IS relevant assets, with comprehensive information about security controls affecting system users and application systems;
7. Overseeing the implementation, administration and maintenance of the The organisation’s technical security infrastructure in line with approved policies and standards;
8. Enforcing compliance with security policies and standards across their processes and operations,
9. Reporting regularly to the SC on the status with regards to information security;
10. Performing security assessments;
11. Monitoring, investigating and analysing security breaches;
12. Ensuring staff receive on-going training and awareness in information security, and;
13. Undertaking an annual review of this policy, considering all of the following:

* Feedback from other areas of the The organisation
* Results of independent reviews and audits
* Changes to the business model of the The organisation
* Trends relating to threats and vulnerabilities
* Reported information security incidents
* Recommendations made by relevant authorities

### Document Coordinator(s)

The Document Coordinator(s) are responsible for working with management, Data Owners, and end users to develop and implement all types of security documentation, and controls. All are subject to the approval and must be presented in the format specified in the *STD-001 - IS Document Management Standard*. The current document coordinators are the Head of IT and the Information Security Officer.

General responsibilities include:

1. To be functionally responsible for the creation and maintenance of Information Security (IS) Policies and Standards for submission to the SC for approval;
2. To be functionally responsible for communication of their individual IS Policies to all interested parties (internal and/or external), educate the user community, and make them easily accessible;
3. Approval of documentation storage location, and media type (both soft and hard-copy);
4. Management of documents of external origin;
5. Monitor and maintain the accuracy of their documentation, and;
6. Ensure documentation is recorded in the *ZBL-OTH-ALL-001 - Master Documents Register*

### Internal Audit

Among many other functions, the Internal Audit is responsible for

1. Internal Audit would provide third line assurance reviews on the effectiveness of the The organisation’s policies and controls with a reporting line to the Board
2. Ensuring periodic audits of the organisation’s departments and information security management system are carried out.

### Data Owner

Data Owners within the organisation shall be responsible for the identification, implementation and maintenance of controls that are commensurate with the value of the information assets they own and the risks to which they are exposed.

Responsibilities of the Data Owner include:

1. Knowing the information for which she/he is responsible for;
2. Assigning Information Classification Level as per *XXXX-POL-ALL-004 - Data Classification Policy*;
3. Ensuring appropriate procedures and controls are in effect to protect the Confidentiality, Integrity, and Availability of the information assets;
4. Releasing information as authorised by EXCO for use and disclosure using procedures that protect the privacy of information;
5. Maintaining operational procedures that support the Information Security Policies and Standards as appropriate;
6. Reporting promptly, the loss or misuse of XXXX information in line with the XXXX-POL-ALL-012 - Incident Response Policy;
7. Monitor and manage the performance of Third Parties against information quality and security targets and compliance to this policy and supporting standards, and;
8. Initiating corrective actions when problems are identified.

### Line Management

XXXX Line Management are Employees who supervise other Employees, consultants, and/or contractors. Each Line Management is responsible for overseeing their team’s use of information, including:

1. Reviewing and approving all requests for changes to their team’s access authourisation;
2. Initiating security change requests to keep their team’s security records and accesses current with their positions and job functions;
3. Ensure and review that staff reporting to them are complying with information security policies and programs in the discharge of their job responsibilities
4. Shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
5. Promptly informing appropriate parties of team member’s terminations and transfers, in accordance with termination procedures;
6. Revoking physical access to terminated Employees, i.e., confiscating keys, changing combination locks, etc.;
7. Providing Employees with the opportunity for training needed to properly use XXXX computer systems;
8. Reporting promptly the loss or misuse of XXXX information and physical assets (e.g. ID badges, laptops), and;
9. Initiating corrective actions when problems are identified.

### User

A User is any person who has been authorised to read, enter, or update XXXX information. A user of information is expected to:

1. Comply with the XXXX Acceptable Use Policy;
2. Comply with other XXXX Information Security Policies and Standards relevant to their job functions (current ‘released’ revisions only);
3. Comply with security controls established by the Data Owner(s);
4. Keep personal authentication devices (e.g. passwords, Remote Access Authentication PINs, etc.) confidential;
5. Report promptly unauthorised access, the loss or misuse of XXXX information and physical assets (e.g. ID badges, laptops), and;
6. Submit Policy, Standard, and Procedure change requests as necessary.

## Documentation Development

Where documentation does not already exist, the SC may assemble a group of subject matter experts or other necessary resources to review and comment on the feasibility of specific Policies and Standards. Each document will be presented in a prescribed format, described in the ‘Policy Format, Naming Convention, & Required Language’ section below.

Each Policy and Standard document will undergo a detailed preliminary review and approval from the appropriate SMEs and relevant Policy Coordinator(s). Once the preliminary review and approval is completed, a final sign-off will be provided by a member of the Executive Committee for standards and policies approved by the board.

When a Policy is approved, the Policy Coordinator will oversee coordination of the communication and training initiative(s) regarding the new Policy with IT and HR or other relevant areas and publish it for the end user community.

The table below lists the processes and responsible parties for new IS Policy, Standard, and Guideline development.

| **Processes** | **Responsibility** |
| --- | --- |
| 1. Identify need for a specific Policy, Standard, or Guideline, submit topic to the SC | All |
| 1. Assign, if necessary, a sub-committee of subject matter experts (e.g., technical) to develop or review documentation drafts for feasibility determination. This sub-committee will report to the SC on additional considerations, recommended changes, etc. | Policy Coordinator  Subject Matter Experts |
| 1. Research, develop, and review documentation drafts | Policy Coordinator  Subject Matter Experts |
| 1. Review and adjust documentation based on sub-committee input or comments | Policy Coordinator |
| 1. Finalise draft, submit documentation draft to SC for approval | Policy Coordinator |
| 1. Review draft. Approve, or return it to the Policy Coordinator for revisions | SC/EXCO/Board |
| 1. If approved, implement Policy through publication, training, and enforcement of the policy/standard/guideline | SC  Policy Coordinator |
| 1. Track, monitor, and resolve any exceptions to the approved Policies and Standards | Line Management  Internal Audit |
| 1. In accordance with the defined timeline, review the documentation for accuracy and applicability | Policy Coordinator |
| 1. Monitor Information Security Policy and Standard compliance | Policy Coordinator  Internal Audit |

## Policy Format, Naming Convention, & Required Language

A standard template will be used in the creation of all Information Security Policies, and for the related Standards, Procedures and Guidelines. A full description is outlines in *XXXX-STD-ALL-001 - IS Documentation Standard*.

## Policy & Standard Exceptions

In the event that a business area or department is unable to comply with an approved Policy or Standard, an exception may be requested and submitted to the document’s Coordinator for initial review and onward presentation with recommendations to the SC and other interested parties for Board approval. A full description of this process is outlined in *XXXX-PRC-ALL-025 - Policy Exception Procedure.*

An exception also allows for non-compliance with a Policy or Standard for either approved time period, or indefinitely. This may be caused by technical limitations within an application or system, the result of a fundamental change to a business process or be in-line with specific business goals. In the case of an exception, a member of the Executive Committee must formally accept the risk and retain accountability for non-compliance and risk treatment.

## Clear Desk & Clear Screen Policy

This policy is to ensure that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended

## Operational Procedures

At a minimum, the following operational procedures must be developed, documented, and distributed to relevant XXXX Employees and contractors in line with the XXXX-POL-ALL-004 - Data Classification Policy:

* the installation and configuration of information systems (platform and application);
* processing and handling of information assets both automated and manual;
* back-ups;
* change control management;
* vulnerability management & patching;
* instructions for handling errors or other exceptional conditions;
* support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;
* output and media handling instructions;
* system restart and recovery procedures;
* collection of audit-trail and system log information;
* monitoring procedures for XXXX assets, and;
* monitoring and review procedures for third party providers.

## Change Management

Any changes to the organisation, business processes, information processing facilities or systems that affect information security must be controlled.

The following change controls must be in place for any major change requests:

* description of change including designation of importance (e.g. minor, or major change);
* planning and testing of change(s);
* assessment of the potential impacts, including information security impacts, of such changes;
* formal approval procedure;
* verification that information security requirements have been met;
* communication of change details to all relevant persons;
* fall-back procedure or equivalent, and;
* description of audit capability and audit trail retention.

All relevant documentation must be updated as a result of any changes to XXXX systems.

## Capacity Management

A capacity management plan must be documented for critical information systems.

The plan should include:

* System tuning and monitoring parameters;
* Detective controls to alert on threats to production systems, and:
* Projections of future capacity requirements.

## Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of XXXX’s assets.

Where this is not possible, detailed mitigating controls must be prepared and approved as a Policy Exception by the Security Committee.

Where practical, the initiation of an event should be separate from the authorization.

The possibility of collusion must be considered in the design and implementation of information security controls.

## Information Security in Project Management

Information security must be built into the XXXX project management method to ensure that information security risks are identified and addressed as part of a project. This applies to projects of any sort.

The following requirements will be integral to all project plans:

* information security objectives are included;
* an information security risk assessment is conducted;
* information security is part of all phases;
* information security implications should be reviewed regularly in all projects, and;
* responsibilities for information security should be defined and allocated to specified roles defined in the project management method.

## Background Checks

Background verification checks will be conducted on all candidates for employment and shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirement(s), the information classification to be accessed, and the perceived risks.

## Delegation of Information Security Tasking

Any individual with information security responsibilities may delegate to others, but the overarching accountability must reside with the original individual.

Where information above classification Internal may be at risk, permission to delegate must be received from the Data Owner.

# Policy Compliance & Enforcement

## Compliance Measures

Compliance with this Policy Framework is enforced through the validation of Compliance Measures relevant to each individual Policy and Standard derived from it. Internal Audit and Information Security are responsible for ensuring compliance with this Information Security Framework and the associated information security policies.

## 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.

# Glossary / Acronyms

## Glossary / Acronyms Table

|  |  |
| --- | --- |
| Information System Assets | Information, regardless of classification, stored, processed, owned or transmitted by XXXX that has tangible and intangible value to the organisation, owned markets and joint ventures, or that must be secured under applicable legal requirements. This includes information in all forms (physical, electronic, intellectual, and sound) as well as the physical media and or systems upon or within which the information is stored, processed or transmitted. |
| Information Security Policy Set | The Information Security Policy Set is comprised of those documents and publications that have been approved, and which detail requirements for information security globally. |
| SC | Security Committee |
| EXCO | Executive Management Committee |
| IS | Information Security |
| ISMS | Information Security Management System |
| Accountability | Cannot be delegated and represents the highest form of responsibility. For example, the CEO can delegate responsibility for IT security, but will always be held ultimately responsible. |
| Responsibility | Assigned to those responsible for getting things done, and usually assigned to department head level, or an overarching committee or steering group. For example, the CEO can delegate responsibility for IT security, but will always be held ultimately responsible. Cannot be delegated. |
| Functional Responsibility | Those responsible for performing the actual functions. For example, a department leader can be responsible for creating and distributing relevant polices, but can delegate the drafting to a policy coordinator. |
| Production Systems | Any XXXX Information Asset that directly supports the generation of revenue or transmit, process or store information. |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
| Sep 2023 | [First] [Last] | 1.0 | First release. |

## Document Ownership

This Policy is owned by the Board of Directors.

## Document Coordinator

This Policy is coordinated by the CISO.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name / Title** | **Signature** | **Date** |
| Board of Directors |  | dd-mm-yyy |
| Executive Management |  | dd-mm-yyy |
| Board of Directors |  | dd-mm-yyy |

## Document Distribution

The Document Coordinator controls distribution of this document. The distribution is all staff and relevant third parties

1. Responsibility delegated to the EC [↑](#footnote-ref-2)
2. Functional responsibility delegated to the SC [↑](#footnote-ref-3)