

1. Purpose, Scope and Users

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

This Policy is applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of **Insert Company Name** as well as relevant external parties.

2. References

- ISO 27001:2013 Clauses 5.2 and 5.3
- Information Security Scope
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- List of Legal, Regulatory and Contractual Obligations
- Incident Management Procedure

3. Definitions

Confidentiality:

characteristic of the information by which it is available only to authorized persons or systems.

Integrity:

characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Availability:

characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security:

preservation of confidentiality, integrity and availability of information.

Information Security Management System:

part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

ISMS:

Information Security Management System

4. Managing the information security

4.1 Objectives and measurement

To ensure the continued suitability and effectiveness of information security within **Insert Company Name**, a number of measurable objectives have been established. These objectives shall be monitored and reviewed as part of the ongoing measurement and metrics activities, and the Management Review process. These objectives include:

Insert Objectives and Measurements as per example below:

A **business objective** is a detailed picture of a step you plan to take in order to achieve a stated aim. These need to be **SMART** (Simple, Measurable, Attainable, Relevant/Realistic, Time-bound) in order for the business to know what progress it has made towards achieving the objective.

Objectives	Measurement
To protect the integrity and confidentiality of business and customer information.	<ul style="list-style-type: none"> The number of security incidents relating to the loss of data or breaches of integrity and confidentiality. Changing risk profile.
To protect the organization's information assets from theft, abuse, misuse and any form of damage.	<ul style="list-style-type: none"> The number of security incidents relating to the loss/theft of equipment. Instances of non-compliance with policies and procedures.
To establish responsibility and accountability for information security in the organization.	<ul style="list-style-type: none"> Staff awareness activities. Internal audit ensuring staff awareness and compliance.
Ensuring the availability of Insert Company Name's information systems and applications during routine operations and also in crisis situations.	<ul style="list-style-type: none"> Number of incidents relating to service availability. Success of disaster recovery testing.

The **Insert position of authority** is responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by the Information Security Officers and approved by **Insert position of authority** in the Statement of Applicability. All the objectives must be reviewed at least once a year.

Insert Company Name will measure the fulfilment of all the objectives. The **Insert position of authority** is responsible for setting the method for measuring the achievement of the objectives – the measurement will be performed **at least once a year** and the Information Security Officers will analyse and evaluate the measurement results and report them to **Insert position of authority** as input materials for the Management review.

4.2 Information security requirements

This Policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to the organization in the field of information security, as well as with contractual obligations.

A detailed list of all contractual and legal requirements is provided in the List of Legal, Regulatory and Contractual Obligations.

4.3 Information security controls

The process of selecting the controls (safeguards) is defined in the Risk Assessment and Risk Treatment Methodology.

The selected controls and their implementation status are listed in the Statement of Applicability.

4.4 Responsibilities

Responsibilities for the ISMS are the following:

- **Insert position of authority** is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- **Insert position of authority** are responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS
- **Insert position of authority** must review the ISMS at least once a year or each time a significant change occurs and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS
- Information Security Officers will implement information security training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- all security incidents or weaknesses must be managed according to the Incident Management Procedure.
- Information Security Officers will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when
- Information Security Officers are responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management

4.5 Policy communication

Information Security Officers have to ensure that all employees of **Insert Company Name** as well as appropriate external parties are familiar with this Policy.

5. Support for ISMS implementation

Hereby the **Insert position of authority** declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

6. Validity and document management

This document is valid as of **Insert Date**.

The owner of this document is **Insert position of authority** who must check and, if necessary, update the document **at least once a year**.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of employees and external parties who have a role in the ISMS, but are not familiar with this document
- non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organization
- ineffectiveness of ISMS implementation and maintenance
- unclear responsibilities for ISMS implementation

WWISE
WORLD WIDE INDUSTRIAL & SYSTEMS ENGINEERS
SAMPLE DOCUMENT