[organization logo]

[organization name]

**INFORMATION SECURITY POLICY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc454535540)

[2. Reference documents 3](#_Toc454535541)

[3. Basic information security terminology 3](#_Toc454535542)

[4. Managing the information security 3](#_Toc454535543)

[4.1. Objectives and measurement 3](#_Toc454535544)

[4.2. Information security requirements 4](#_Toc454535545)

[4.3. Information security controls 4](#_Toc454535546)

[4.4. Business continuity 4](#_Toc454535547)

[4.5. Cloud services 4](#_Toc454535548)

[4.6. Responsibilities 4](#_Toc454535549)

[4.7. Policy communication 5](#_Toc454535550)

[5. Support for ISMS implementation 5](#_Toc454535551)

[6. Validity and document management 5](#_Toc454535552)

# 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 [organization name], as well as relevant external parties.

# Reference documents

* ISO/IEC 27001 standard, clauses 5.2 and 5.3
* ISO/IEC 27017 standard, clause 5.1.1
* ISO/IEC 27018 standard, clauses 5.1.1 and A.9.2
* ISMS Scope Document
* Risk Assessment and Risk Treatment Methodology
* Statement of Applicability
* List of Legal, Regulatory and Contractual Obligations
* [Business Continuity Policy]
* [Incident Management Procedure]

# Basic information security terminology

**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.

# Managing the information security

## Objectives and measurement

General objectives for the information security management system are the following: creating a better market image and reducing the damage caused by potential incidents; goals are in line with the organization's business objectives, strategy and business plans. [job title] is responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by [list job functions which have the appropriate authorization], and approved by [job title] in the Statement of Applicability.

All the objectives must be reviewed at least once a year.

[organization name] will measure the fulfillment of all the objectives. [job title] is responsible for setting the method for measuring the achievement of the objectives – the measurement will be performed at least once a year and [job title] will analyze and evaluate the measurement results and report them to [top management] as input materials for the Management review.

## Information security requirements

This Policy and the entire ISMS must be compliant with legal and regulatory requirements as well as with contractual obligations relevant to the organization and its cloud service customers in the field of information security and protection of Personally Identifiable Information (PII).

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

## 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.

## Business continuity

Business continuity management is prescribed in the Business Continuity Management Policy.

## Cloud services

Cloud services security management is prescribed in the Cloud Security Policy.

## Responsibilities

Responsibilities for the ISMS are the following:

* [job title] is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
* [job title] is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS
* [job title] is responsible for operational security of cloud services as well as for reporting about the cloud services’ security performance to the coordinator of the ISMS
* [top management] 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.
* [job title] 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 reported to [job title]
* [job title] will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when
* [job title] is responsible for ensuring the proper designation of responsibilities to customers, partners, suppliers, and other third parties who have a role in information security management
* [job title] is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management

## Policy communication

[job title] has to ensure that all employees of [organization name], as well as appropriate external parties are familiar with this Policy.

# Support for ISMS implementation

Hereby the [job title or top management body in the scope of the ISMS] 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.

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], 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

Previous versions of this policy must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]