<Organization Name>

**Information Security Management System (ISMS) Scope and Context**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |
| **Version** | <Version> |
| **Document Owner** | <Name of CISO/IT Security Lead> |
| **Approved by** | <Name of Approval Authority/Board> |
| **Date Approved** | <Approval Date> |
| **Next Review Date** | <Review Date (typically a year from the approval date)> |
| **Document Classification** | Confidential/Public/Internal Use Only |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

**Table of Contents**

[Introduction 1](#_Toc179735697)

[Organizational Context 1](#_Toc179735698)

[Activities 1](#_Toc179735699)

[Functions 2](#_Toc179735700)

[Services 2](#_Toc179735701)

[Products 2](#_Toc179735702)

[Major Partnerships 3](#_Toc179735703)

[Supply Chains 4](#_Toc179735704)

[Business Objectives and Relevant Policies 5](#_Toc179735705)

[Internal and External Issues 6](#_Toc179735706)

[Internal Issues 6](#_Toc179735707)

[External Issues 7](#_Toc179735708)

[Risk Appetite 8](#_Toc179735709)

[Interested Parties and Their Requirements 9](#_Toc179735710)

[Interested Parties 9](#_Toc179735711)

[Requirements 9](#_Toc179735712)

[Purpose and Scope of the ISMS 10](#_Toc179735713)

[Purpose 10](#_Toc179735714)

[Impact of an Information Security Incident 10](#_Toc179735715)

[Information Security Objectives 11](#_Toc179735716)

[Information Security Priority 11](#_Toc179735717)

# Introduction

The purpose of this document is to define the context and scope of the Information Security Management System (ISMS) for <Organization Name>. The ISMS is designed to safeguard the organization’s information assets against security risks and ensure the confidentiality, integrity, and availability of information.  
  
The scope of this ISMS aligns with the requirements set by ISO/IEC 27001:2022 and will be periodically reviewed and updated based on significant changes to the organization’s business activities or environment.

# Organizational Context

The context of <Organization Name> is outlined based on the external and internal factors influencing the organization and the stakeholders it interacts with.

## Activities

<Organization Name> undertakes a wide range of business activities within its target sector and is constantly developing new products and services to bring to market.

* <Core business operations>
* <Industry sector>
* <Relevant cloud or technology services>
* <Geographical regions of operation>

## Functions

<Organization Name> consists of the following organizational structure.

|  |  |
| --- | --- |
| **Function** | **Description** |
| Sales and Marketing |  |
| Finance and Accounting |  |
| Human Resources |  |
| Operations |  |
| IT and Risk Management |  |
| <Other functions> |  |

## Services

<Organization Name> offers the following major services to its customers.

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Name** | **Service Type** | **Regulatory Impact** | **Service Classification** |
| <Service 1> |  | Yes/ No | Select Service Classification |
| <Service 2> |  | Yes/ No | Select Service Classification |

## Products

<Organization Name> offers the following major products to its customers.

|  |  |  |
| --- | --- | --- |
| **Product Name** | **Description** | **Regulatory Impact** |
| <Product 1> |  | Yes/ No |
| <Product 2> |  | Yes/ No |

## Major Partnerships

<Organization Name> has a policy of forming partnerships with other organizations which complement its own offering and bring increased benefits to its customers.

|  |  |  |
| --- | --- | --- |
| **Organization Name** |  | |
| **Location(s)** |  | |
| **Nature of Partnership** |  | |
| **Affected Products/Services** |  | |
| **Number of Customers Involved** |  | |
| **PII Shared** | Yes/ No | <If yes, the PII data that is shared> |
| **Duration of Partnership** |  | |
| **Other Information** |  | |

*NOTE: If there are several partnerships, add them in the given format*

## Supply Chains

In order to provide the products and services of the <Organization Name> to the customers a number of important supply chain routes are in place.

|  |  |  |
| --- | --- | --- |
| **Products/Services Affected** |  | |
| **Suppliers Involved** |  | |
| **Geography** |  | |
| **Dependencies** |  | |
| **Revenue Impact** |  | |
| **Criticality** | Select Criticality | |
| **PII Impacted** | Yes/ No | <If yes, the PII data that is shared> |
| **Other Information** |  | |

*NOTE: For other products/services also use the given format*

## Business Objectives and Relevant Policies

The purpose of the ISMS is to ensure that <Organization Name> is still able to meet its defined business objectives and comply with its policies.

|  |  |
| --- | --- |
| **Business Objectives** | **Relevant Policy** |
| <Objective related to security> | Information Security Policy |
| <Objective related to growth> | IT Access Control Policy |
| <Objective related to compliance> | Data Privacy Policy |
| <Objective related to operational efficiency> | Acceptable Use Policy |
| <Objective related to risk management> | Incident Management Policy |
| <Objective related to innovation> | Remote Access Policy |
| <Objective related to customer satisfaction> | Business Continuity Policy |
| <Objective related to regulatory compliance> | Vendor Management Policy |
| <Other objectives based on organization needs> | <Other relevant policies based on organization needs> |

# Internal and External Issues

There are a number of internal and external issues that are relevant to the purpose of <Organization Name> and that affect the ability of the ISMS to achieve its indtennded outcomes.

## Internal Issues

With regard to the <Organization Name> business itself, there are a number of relevant internal issues.

|  |  |
| --- | --- |
| **Internal Issue** | **Impact on ISMS** |
| Organizational Structure |  |
| Resource Availability |  |
| Employee Relations and Knowledge |  |
| <Other internal issues> |  |

These general internal issues will be considered in more detail as part of the risk assessment process.

## External Issues

With regard to the external environment in which <Organization Name> operates, there are a number of relevant external issues.

|  |  |
| --- | --- |
| **External Issue** | **Impact on ISMS** |
| Legal and Regulatory Requirements  *(Ex:* *GDPR, local privacy laws)* |  |
| Economic Factors  *(Ex:* *industry growth, competition)* |  |
| Technological Trends  *(Ex:* *AI, cloud computing advancements)* |  |
| Political Influences  *(Ex:* *Government Instability)* |  |
| Social Considerations  *(Ex:* *Social Attitudes)* |  |
| Environmental Causes  *(Ex:* *flood, earthquake)* |  |
| <Other internal issues> |  |

These general external issues will be considered in more detail as part of the risk assessment process.

## Risk Appetite

The ISMS is designed to address the significant risks identified concerning the information security of <Organization Name>.The organization’s risk appetite defines how it will identify, assess, and manage these risks based on its willingness to accept potential outcomes.

In general terms the organization’s appetite for risk may be said to be Low/Moderate/High.

|  |  |
| --- | --- |
| **Low** | The organization prefers to avoid risk where possible and invests significant resources in reducing or mitigating residual risks through highly effective information security measures. This is suitable for organizations with low tolerance for potential security breaches or financial loss. |
| **Moderate** | The organization is willing to accept reasonable levels of risk while implementing adequate controls and measures to minimize any adverse outcomes. This is suitable for organizations that balance risk and reward, ensuring critical risks are managed while allowing some flexibility. |
| **High** | The organization is willing to accept significant risks to achieve strategic goals and considers the potential rewards as justifiable. Security measures are applied based on the potential benefits, and a certain degree of risk is inherent in the business approach. |

# Interested Parties and Their Requirements

## Interested Parties

An interested party is defined as a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

|  |  |  |
| --- | --- | --- |
| **Interested Party** | **Type** | **Description** |
| Employees | Internal |  |
| Customers | External |  |
| Suppliers | External |  |
| Regulators | External |  |
| <Other Stakeholders> | Select Type |  |

## Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **Interested Party** | **Requirement Reference** | **Information Security Requirements** | **Source/Link to supporting documents** |
| Employees |  | *(Ex. Access control, proper use of information assets)* | *(Ex. Minutes of Annual General Meeting dd/mm/yyyy)* |
| Customers |  | *(Ex. Data confidentiality, integrity, availability)* |  |
| Suppliers |  | *(Ex. Secure data exchange, contractual compliance)* |  |
| Regulators |  | *(Ex. Compliance with standards like GDPR, ISO 27001)* |  |
| <Other Stakeholders> |  | *Describe requirements for other stakeholders* |  |

# Purpose and Scope of the ISMS

## Purpose

The purpose of the ISMS is to:

1. Understand the organization’s needs and the necessity for establishing information security management policy and objectives.
2. Implement and operate controls and measures for managing the organization’s overall capability to manage information security incidents.
3. Monitor and review the performance and effectiveness of the ISMS.
4. Continually improve the organization’s information security based on objective measurement.

This purpose applies to the scope of the ISMS as defined below.

## Impact of an Information Security Incident

The potential impact of an inability to perform normal business processes will be shown in one or more of the following key areas.

|  |  |  |
| --- | --- | --- |
| **Impact** | **Applicable** | **Explanation of Relevance to the Organization** |
| Loss of sales revenue | Yes/ No |  |
| Risk to life on health and safety grounds | Yes/ No |  |
| Inability to meet legal obligations | Yes/ No |  |
| Breach of contractual obligations | Yes/ No |  |
| Loss of business opportunity | Yes/ No |  |
| Fines and other penalties | Yes/ No |  |
| <Other Stakeholders> | Yes/ No |  |

## Information Security Objectives

Based on the requirements and issues set out in this document, the following major objectives are set for information security.

|  |  |
| --- | --- |
| **Objective Number** | **Objective Description** |
| <Objective 1> |  |
| <Objective 2> |  |

### Information Security Priority

|  |  |
| --- | --- |
| **Objective Number** | **Objective Description** |
| Protecting confidential information | Ensure information is protected from unauthorized access. |
| Ensuring availability | Ensure critical business information is available to authorized users. |
| Maintaining data integrity | Ensure customer data is accurate and not altered without authorization. |