Information Security Policy And Scope

ISO 27001:2023 Section	Document Section
4.3 Determining the scope of the information security management system	1.
4.4 Information security management system	(All)
5.1 Leadership and commitment	8.
5.2 Policy	2.
5.3 Organizational roles, responsibilities and authorities	8.

Summary

The Information Security Policy describes the scope of the Information Security Management System (ISMS), its documented procedures and a description of their interactions.

1. Scope

The policy described in this document outlines the framework to manage information security in *<your company name>*.

This policy applies to all employees, contractors, and third-party vendors of [Organization Name] who have access to electronic and physical information systems and data.

2. Policy Statement

<your company name> commits to maintaining the confidentiality, integrity, and availability of all its information assets. This is achieved through:

- Implementing a comprehensive Information Security Management System (ISMS) compliant with ISO/IEC 27001:2023 standards.
- Regularly assessing the information security risks and implementing the appropriate measures to mitigate identified risks.
- Ensuring that information security is an integral part of all IT and business processes.
- Providing ongoing training and support to all staff to ensure they understand their roles and responsibilities in safeguarding sensitive information.
- Regularly reviewing and updating the ISMS to address new security challenges and business changes.

3. Information Security Principles

- Confidentiality: Ensuring that information is accessible only to those authorized to have access.

- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorized users have access to information and associated assets when required.

4. Risk Management

The organization will regularly carry out risk assessments to identify, evaluate, and address risks associated with information security.

5. Incident Management

A structured approach will be followed to handle security breaches or incidents, which includes incident reporting, investigation, and mitigation strategies to prevent future occurrences.

6. Compliance

Compliance with this policy will be monitored and reviewed as part of the ongoing performance evaluation process. Violations of this policy will result in disciplinary action, which may include termination and legal action, depending on the severity of the breach.

7. Policy Review

This policy will be reviewed annually or in response to significant organizational or technological changes to ensure its continuing suitability, accuracy, and effectiveness.

8. Organizational Roles, Responsibilities and Authorities

> Describe the roles of the people in your company. Typically this is done by drawing an organigram (you could use draw.io for that). Or, you just use a table like below.
>
> Minimum requirement information: required qualification and description of tasks related to QMS process involvement If applicable, add: report / authority, access rights, etc.

Role	People
CEO	Steve Jobs
CTO	Steve Wozniak
ISO	Oliver Eidel

All C-level roles (CEO, CTO, CMO) are referred to as the Management. Management is generally responsible to endorse and support the Information Security Policy by providing the necessary resources and authority to implement it.

The Information Security Officer (ISO) is responsible for maintaining the ISMS and ensuring the policy is implemented, monitored, reviewed, and updated.

All Employees are required to adhere to this policy and report any security breaches or incidents to the designated authority.

Required qualification for this role:

- Fluent in German and English language
- Training in the field of information security management
