Information Security Policy

Table of contents

1. Purpose, scope and target audience of policy

This document defines the organisation's information security policy and thus the overarching objective of the Information Security Management System (ISMS). This document defines the purpose, orientation, principles and general regulations for the ISMS.

The information security policy defined in this document relates to the entire ISMS in accordance to the defined scope of the ISMS.

The users of the document are all employees of the organisation and relevant third parties.

2. Terms of information security

Term	Meaning
Confidentiality	The characteristic that information is not made accessible or disclosed to unauthorised persons, facilities or processes
Integrity	The accuracy and completeness of the information
Availability	The characteristic that information can be accessed and used by an authorised body if required
Information security	Maintaining the confidentiality, integrity and availability of information
Information Security Management System (ISMS)	Management procedure that deals with the planning, implementation, maintenance, review and improvement of information security

3. Importance of information security

3.1. Business objectives

Our mission is to guide companies and entrepreneurs out of the paragraph jungle, so that they are treated fairly and can concentrate on their core business.

Taxy.io develops digital, artificially intelligent software solutions for tax advisors and their employees that are positioned at these two interfaces in order to sustainably improve day-to-day consulting work.

Our mission is to guide companies and entrepreneurs out of the paragraph jungle, so that they are treated fairly and can concentrate on their core business.

3.2. Relevant requirements and interested parties

It is particularly important to us that we fulfil the following requirements:

- Customer requirements
- Contractual requirements
- Legal requirements

We would like to fulfil the requirements and expectations of the following interested parties primarily with the ISMS:

- Customers
- Legislature
- Management Board
- Employees, Investors
- Business Partners

3.3. Information security

Information security is a high priority in line with our business objectives. The objectives for the ISMS are derived from the organisation's business strategy described in section 3.1 and the relevant requirements and interested parties described in section 3.2.

The business success of the Taxy.io GmbH depends on confidential business information that is available and has integrity, which Taxy.io shares with customers, suppliers, cooperation partners and other institutions. Furthermore the ISO 27001 certification is required by (potential) business partners and customers.

3.4. ISMS objectives

The objectives of the information security management system are in particular:

- Fulfilment of all ISO/IEC 27001 requirements, in particular successful (re)certification
- The introduction and regular implementation of ISMS training and awareness-raising measures to increase the information security skills of all employees
- The organisation's overall risk in terms of information security should be at most "medium"
- Checking our suppliers and ensuring that they provide the contractually agreed service.

The objectives of the ISMS are documented and their fulfilment checked in accordance with section 3.5. .

3.5. Planning and reviewing the objectives of the ISMS and their fulfilment

When planning how the objectives of the ISMS should be achieved, the planned measures, resources, responsibilities, time targets and the assessment method for the review must be defined. The points must be documented. The objectives of the ISMS and their fulfilment must be reviewed annually. The person responsible for carrying out the review, analysing the results of the review and preparing a review report for management is the Information Security Officer.

3.6. Information security measures

The organisation commits to comply with the information security requirements as defined in the subject-specific information security policies and ISO/IEC 27001. Suitable information security controls are identified, defined and reviewed within the risk management framework in the risk assessment and risk treatment methodology.

The applicable information security measures, their implementation status and any exceptions are documented in the Statement of Applicability (SOA). Responsible for the SOA is the Information Security Officer. The SOA must be filed in accordance with the chapter "Management of records to this document".

4. Responsibilities

The following responsibilities exist within the ISMS:

Job title	Responsible for
Management Board	the correct implementation and maintenance of the ISMS in accordance with the information security guideline and ensuring that sufficient resources are available for this.
Information Security Officer	coordinating the operation of the ISMS and reporting on its performance.
Information Security Officer	Ensuring that annual reviews of the ISMS and any significant changes are carried out and recorded.
Information Security Officer	the information security awareness of all employees as well as their education and training on the subject of information security.
Asset owner	Ensuring the integrity, confidentiality and availability of the assets or information for which the person is responsible.
All employees	the reporting of information security incidents or vulnerabilities.
Information Security Officer	the handling of information security incidents and vulnerabilities.
Head of Product (business partners / big customers)Data Protection Officer (Data Protection Incidents to authorities)CEO (Investors)	the definition of the information that is communicated to interested parties in the context of information security.

All key responsibilities and recurring tasks in the ISMS are managed and documented by the Task Manager in the Digital Compliance Office (DCO).

In addition to the roles and responsibilities set out in this information security policy, other relevant roles and responsibilities are defined in the topic-specific policies. An overview of the responsibilities in the ISMS, in particular who is responsible for the various tasks:

Who is Responsible, accountable, consulted and informed is listed in the RACI matrix. This must be filed in accordance with the chapter "Management of records for this document".

5. Obligations and responsibilities in the area of information security

Information security is embedded at the highest management level of the organisation. The organisation's management is committed to providing sufficient resources for the implementation and continuous improvement of the ISMS. Continuous improvement is implemented through regular reviews of the processes and specifications by the ISMS. Employees are obliged to report identified non-conformities and suggestions for improvement in accordance with the *Procedure for Corrective Actions*. This should enable all relevant parties involved in the ISMS to achieve the information security objectives and continuously improve the ISMS.

All employees and relevant third parties must be familiar with the organisation's information security policy and the ISMS. All employees must act in accordance with the information security policy, the topic-specific information security policies and all requirements specified by the management. If company policies are violated, disciplinary action may be taken. The management is responsible for communicating the information security policy and emphasising the importance of the ISMS and the company-wide commitment to information security.