# Information Security Policy

## Information Security Management System

**Restricted**

This document contains information that cannot be distributed or reproduced without the written permission of the CEO of QULIX.

**Version 1.2**

Reference code: **QPL ISMS P1 En** | Status: **Approved by CEO** | Confidentiality level: **Public** | Version date: **02.05.2024**


- 1. Introduction
- 2. Purpose, scope and users
- 3. Referenced documents
- 4. Information security management
  - 4.1 Information security principles
  - 4.2 Information security objectives
  - 4.3 Regulatory requirements and contractual obligations
  - 4.4 Information classification
  - 4.5 Supplier relationships
  - 4.6 Protective measures
  - 4.7 Secure development
  - 4.8 Information security continuity
  - 4.9 Incident management
  - 4.10 Compliance, Policy awareness and disciplinary procedures
  - 4.11 Policy review
- 5. Responsibilities
- 6. Validity and document management


# 1. Introduction

This high-level Policy describes how QULIX LLC (hereinafter – the Company) approaches information security. It defines the guidelines, methods, and roles needed to secure the Company's information assets. Special policies, procedures and other local company regulations supplement this Policy and contain detailed requirements.

# 2. Purpose, scope and users

The aims of this Policy are:

- to provide a basis for establishing an acceptable level of information security at the Company and reduce the risks associated with theft, loss, misuse or damage of the Company's information assets by:
  implementing the Information Security Management System (hereinafter – the ISMS) in accordance with the international standard ISO /IEC 27001,
  providing the resources necessary for the operation of the ISMS;
- to make sure that employees, contractors, trainees and interns of the Company (hereinafter referred to as employees), as well as representatives of external parties who have access to the Company's information assets, are aware of and comply with the requirements of the legislation in the field of information security and data protection, understand their responsibilities for protecting the confidentiality, integrity and availability of the Company's information they work with;
- to determine the directions, the implementation of which will allow to create safe and secure information systems and the working environment in general for employees and external stakeholders;
- to protect the Company from liability or damage resulting from improper use of its IT infrastructure;

- to ensure the handling of confidential information of customers and partners of the company at a security level commensurate with the value of this information, including compliance with all contractual obligations related to information security;
- to response to changes in the environment where the Company strives to achieve its information security objectives, initiating a cycle of continuous improvement of the ISMS.

# 3. Referenced documents

- ISO/IEC 27001:2022 standard, clauses 5.2 and 5.3

# 4. Information security management

The Company owns all business information (including intellectual property) and computing resources acquired (received) and put into operation in order to carry out activities in accordance with the legislation and the Company's Articles of Association. This property right applies to licensed and company-developed software, the content of corporate e-mail, corporate paper and electronic documents circulating among employees or on behalf of the Company among external stakeholders. The Company owns owns voice and fax messages transmitted or received using corporate equipment.

## 4.1 Information security principles

The core of the Company's business is the development, implementation and maintenance of IT solutions, consisting of methodology, software and related services. Information and information technology are valuable assets, therefore the Company emphasizes the protection of its information and the information of its customers and partners, implementing an ISMS based on the following main directions (principles):

- information should be classified according to an acceptable level of confidentiality, integrity and availability, as well as applicable legal, regulatory requirements and contractual obligations;
- all persons covered by this Policy must handle information properly in accordance with its classification, fulfill all contractual obligations, as well as special ISMS policies and regulations aimed at complying with these obligations;
- information should be available only to those who have a reasonable right to access information of the appropriate level, therefore, access should be provided on the basis of the least privileges and the need for awareness;
- information should be protected from unauthorized access and processed according to its classification;
- information security should be an integral part of software development and testing processes;
- employees must report violations of this Policy;
- ensuring information security and local regulatory legal acts in this area should be regularly analyzed and revised, including through annual internal audits and penetration testing;
- the Company's ISMS should be evaluated and corrected according to the principles of continual improvement.

This Policy is applicable and communicated to the Company's employees, as well as external stakeholders who interact with the Company's information, and applies to the entire Scope of the Information Security Management System.

## 4.2 Information security objectives

The CEO sets the main objectives for information security and revises them during the regular review of the ISMS by the Company's management.

The Information Security Manager:

- proposes objectives for individual information security controls (or groups of them);
- defines methods for monitoring and measuring the achievement of the objectives;
- takes measurements and analyzes their results at least once a year;
- reports the results of measurements as input materials for review of the ISMS by the Company's management.

Project managers set information security objectives for projects and monitor and measure them in accordance with established methodologies.

## 4.3 Regulatory requirements and contractual obligations

This Policy and the entire Company's ISMS are consistent with the requirements and obligations applicable to the Company such as:

- legislative and regulatory requirements in the field of information security, trade secrets and protection of personal data;
- contractual obligations.

Special ISMS policies and other local regulations adopted in accordance with this Policy provide details on the applicable regulatory requirements and establish the way contractual obligations are fulfilled.

## 4.4 Information classification

All information in the Company is classified in accordance with legal requirements, its significance, criticality and sensitivity to unauthorized disclosure or change with the assignment of an appropriate access level. The access level of information is regularly reviewed by the owners of information assets.

## 4.5 Supplier relationships

The Company's suppliers of goods and services, as well as other counterparties who have access to the Company's information assets, must:

- comply with this Policy;
- comply with the established requirements for suppliers;
- ensure adequate protection of information when accessing the Company's information assets, at the location of the Company or remotely, including when subcontracted with other organizations.

The following conditions must be met by providers of cloud services and data transfer (processing) services:

- it is expected that the services used by the supplier to process the Company's sensitive data will be certified to comply with the ISO/IEC 27001 standard or similar. Compliance with the standards is considered the best way for the supplier to prove that it takes information security into account when providing services;
- requests for exceptions to these rules are reviewed by the CEO.

## 4.6 Protective measures

Information security at the Company is ensured through the selection and implementation of information security controls (protective measures). The selected controls and their implementation status are monitored by the Information Security Manager, and their effectiveness is assessed during review of the ISMS by the Company's management.

## 4.7 Secure development

The Company has established and adheres to the requirements for ensuring information security in software development, as well as for the security of development and testing environments.

## 4.8 Information security continuity

The Company uses information security continuity procedures based on the methodology of the Business Continuity Management System.

## 4.9 Incident management

If the Company's employees or external stakeholders become aware of an information security incident involving an information asset of the Company or its client, they must report it in accordance with the established procedure. The Information Security Manager provides a rapid response to incident reports, conducts their investigation, initiates the implementation of corrective actions.

## 4.10 Compliance, Policy awareness and disciplinary procedures

All employees, as well as external stakeholders:

- are properly familiarized with this Policy, as well as special policies, procedures and other local legal acts of the Company in the field of the ISMS;
- undertake to comply with the ISMS requirements when interacting with the information assets of the Company and its customers.

Information security breaches committed by employees are subject to the Company's disciplinary procedures.

## 4.11 Policy review

This Policy, special policies, procedures and other local ISMS legal acts of the Company are regularly reviewed and updated to ensure that they are consistent with changes in legislation, organizational structure of the Company, contractual obligations and other elements of the environment whe re the Company strives to achieve its information security objectives. If necessary, the Information Security Manager develops additional rules to regulate problem domains.

# 5. Responsibilities

The CEO of the Company:

- accepts the Company's obligations to comply with applicable information security requirements and continually improve the ISMS;
- demonstrates leadership and commitment to these obligations by
    - ensuring the conformity of this Policy and the established information security objectives with the Company's strategy,
    - supporting the integration of the ISMS into other Company's processes,
    - ensuring the availability of resources necessary for the operation of the ISMS,
    - informing employees about the importance of effective information security management and the conformity to the ISMS requirements,
    - taking measures to ensure that the ISMS achieves all objectives,
    - supporting the efforts of employees to ensure the effectiveness of the ISMS,
    - promoting continual improvement of the ISMS and supporting the demonstration of leadership by all other persons performing significant managerial functions in the Company within their area of responsibility;
- determines which information security issues will be communicated to which of the interested parties (both internal and external), by whom, when and in what order;
- analyzes the suitability (acceptability), adequacy (compliance with requirements) and effectiveness (degree of achievement of the set goals) of the ISMS on a special meeting of the Company's management at least once a year or more often in case of any major change in the environment where the Company strives to achieve its information security objectives.

The CTO is responsible for organizing and securing development and test processes and environments.

The Information Security Manager:

- is responsible for ensuring the compliance of the Company's ISMS with the requirements of the international standard ISO/IEC 27001;
- monitors the implementation and executes, if he or she is responsible in a particular case, the measures approved by the Company's management, aimed at ensuring the required level of information security;
- coordinates ISMS processes, creates and updates the necessary documents and records;
- prepares an ISMS operation report for the Company's management review, documents minutes of this meeting;
- together with the HR Manager, organizes training and awareness programs for the Company's employees in the field of information security.

Project managers are responsible for organizing and ensuring information security in all projects (external and internal).

The protection of integrity, availability, and confidentiality of information assets is the responsibility of the owner of the corresponding asset.

# 6. Validity and document management

This document is valid as of 02.05.2024.

The owner of this document is the Information Security Manager, 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:

- the 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 Company;
- ineffectiveness of ISMS implementation and maintenance;
- unclear responsibilities for ISMS implementation.