ISMS Information Security Policy

Status:	Published
Version:	7.0
Date:	2026-05-08
Project:	QMS
Authors:	Tomasz Puk (TOPU1)

Contents

Introduction

This Policy describes the Information Security Management System (ISMS) in Centra Technology, hereinafter referred to as the Organization. The purpose of the policy is to establish the principles and define the requirements for the protection of information processed in the Organization, the secure processing of personal data, and the provision of IT services at a specified level.

This Policy is the top-level document in the information security hierarchy; it defines the purpose, scope, and references concerning other documents, roles, and activities that comprise the ISMS. The Organization has adopted the requirements of both the ISMS ISO 27001:2022 standard and the PIMS EU: General Data Protection Regulation as the basis for the introduction and certification of the Information Security Management System.

This Policy is a top-level document that references or introduces other ISMS documentation. This Policy shall be treated as Public information and can be shared with all interested parties or published on the Internet.

Purpose

The Information Security Management System consists of the daily activities of Users working for or cooperating with the Organization. In this Policy, we present the objectives of the ISMS adopted by the ISMS Top Management (corresponding to the Management Board) and the goals the Organization intends to achieve, e.g.:

1. Comprehensive and professional information security management in the Organization.
2. Secure and lawful processing of Personally Identifiable Information (PII, personal data).
3. Building awareness and competence among the Users involved in the Organization's activities concerning their impact on information security.
4. Fulfilling legal requirements in terms of security and privacy.
5. Development of an ISMS compliant with the requirements of the ISMS ISO 27001:2022 standard and its continuous improvement.
6. Implementation of technical and organizational security measures adopted by the Organization.
7. Strengthening the image of the Organization as a provider of secure IT services.

Scope of the Policy

This Policy applies to all persons in the Organization, including persons assigned the ISMS Member role, as well as to entities providing services for the benefit of the Organization. All these persons are hereinafter referred to as Users.

1 Declaration of the Management

The ISMS Top Management is aware that the management of information security is an important element of the Organization's operations. Information security management includes the following elements:

1. Establishment of policies and work standards.
2. Education of Users.
3. Information security risk management.
4. Hardware and ICT assets management.
5. Access management.
6. Application of cryptographic security measures.
7. Ensuring the physical safety of the Organization’s premises.
8. System operations.
9. Communication security.
10. Acquisition management.
11. Supplier management.
12. Incident management.
13. Business continuity management.
14. Compliance and monitoring.

Given the above, the ISMS Top Management has established this Policy to identify the ISMS objective, reference other ISMS documentation, and introduce the main roles engaged in the ISMS setup and operations.

The ISMS Top Management has decided that the Information Security Management System certification scope statement shall be defined as:

"***Development, service delivery, and support services in a SaaS manner for the e-commerce platform.***"

2 Objectives of the Information Security Management System

The ISMS Top Management has set the following high-level objectives of the ISMS:

1. Ensuring the confidentiality, availability, and integrity of the information processed within the Organization in all its physical locations.
2. Ensuring secure and lawful processing of Personally Identifiable Information (PII) in the Organization.
3. Ensuring the Organization's compliance with applicable laws, regulations, and contractual requirements with a special focus on PIMS EU: General Data Protection Regulation.
4. Identifying and providing the resources necessary for effective security management.
5. Ensuring that the Organization’s operations and information protection measures are based on risk management principles.
6. Implementation and maintenance of security measures adopted in the ISMS ISO 27001:2022 Statement of Applicability.
7. Prompt identification and handling of security incidents and events.
8. Continuous improvement of the Information Security Management System in the Organization.

Information security objectives specific to a given year are documented in the ISMS Information Security Objectives folder.

3 Scope of the Information Security Management System

The Information Security Management System covers the following areas of the Organization's activities:

1. The ISMS covers the following Organization units and physical locations:
    a. **Headquarter - Centra Technology AB**
        a. Address: Torsgatan 26, 113 21 Stockholm
        b. VAT: SE556768105001
    b. **Polish subsidiary - Centra Technology Polska Sp. z o.o.**
        a. Address: Pl. Jana Pawła II 14, 50-043 Wrocław
        b. VAT: PL5273028939
    c. **UK subsidiary - Centra Technology UK Limited**
        a. Address: The Record Hall, 16-16A Baldwin's Gardens, London EC1N 7RJ, United Kingdom
        b. Company Registration Number: 15169844
    d. **Virtual Organization** - As the Organization uses both employees and contractors working remotely, this group of people is managed as a “virtual organization” structure. It means they provide standard services but from remote/home office locations.

2. The ISMS covers all roles in the units mentioned above.
3. All Centra Platform services and modules are covered by the ISMS and with a particular focus on:
    a. The **Centra Platform** comprises two main modules:
        a. **Direct to Consumer (DTC)**.
        b. **Wholesale**.
4. All Centra Platform-related services provided to customers are within the scope of the ISMS as well.

More details about the hierarchy of the Organization can be found in the ISMS Organization Context.

The Information Security Management System **does not cover**:

1. The way customers manage information and security aspects of the Centra Platform. This is due to the fact such activities are outside of the Organization's jurisdiction and shall be managed under an ISMS implemented on the client side.
2. The information security and privacy controls implemented within suppliers' ICT infrastructure remain under the responsibility of the respective suppliers. Nevertheless, the Organization defines legal, organizational, and technical requirements for suppliers through applicable agreements, supplier evaluation, and supplier management processes.

4 Division of Roles and Responsibilities

Everybody in the Organization is responsible for its part of the information security and privacy management. The Organization identified the leading Roles from the ISMS perspective and listed some of them in the table below. The detailed descriptions and responsibilities of each role can be found in each role definition in the Roles section of ins2outs.

Role	Summary	High-level responsibility
ISMS Top Management	The role represents a person or a group responsible for managing the Organization at its highest level.	Responsibility for establishing the Information Security Management System, defining objectives, and providing resources for its operations and improvements.

ISMS Member	The role of an ISMS Member is the most generic role in the information security context in the Organization. It applies to every person working for the Organization under either a B2B or employment contract.	Responsibility for implementing information security in daily activities of the Organization's operations.
ISMS IT Administrator	A person or group of persons who are responsible for generic ICT administration, maintenance, and operations of IT assets and resources in the Organization.	Overall responsibility for managing the security of common ICT assets and ICT infrastructure and executing operations activities on those assets.
ISMS SysOps	A person or group of persons who, on behalf of the Product Team, manages technical activities such as environment installation, configuration management, and service provision for clients' environments only.	Overall responsibility for managing security, privacy, and ICT infrastructure and executing operations activities on the clients' environments.
ISMS Release Manager	A person or group of persons who, on behalf of the Product Team, manages the technical deployment process for clients' environments only.	Overall responsibility for managing security, privacy, and ICT infrastructure and executing operations activities on the clients' environments.
ISMS R&D Engineer	A person or group of persons who takes part in the Research and Development phase of a product.	Overall responsibility for the Research and Development phase of a product with access only to the research-and-development environments.
ISMS DevOps	A person or group of persons who, on behalf of the Research and Development team, manages technical activities such as environment installation and configuration	Overall responsibility for architecting, managing security, privacy, ICT infrastructure, specification of installation, and deployment activities

	management for the Research and Development environments only.	(tools configuration) on the research-and-development-level environments.
Line Manager	A person supervising the work of a department or group of people	Responsible for leading, educating, and supervising a group of ISMS Members who report to a manager with respect to ISMS and PIMS.
ISMS Information Security Officer	The role represents a person or a group of people responsible for the definition and supervision of an information security management system in the Organization.	Overall responsibility for the definition, implementation, and operations of the Information Security Management System in the Organization.
ISMS Internal Auditor	This role is responsible for carrying out information security management system audits within the Organization.	Overall responsibility for planning, executing, and communicating outcomes of both internal and external audits.

Table. ISMS Roles.

5 System Definition

The Organization defined its ISMS on the ins2outs platform, which is used to manage system documentation and both documents and records related to the operation of the ISMS. The approach to managing this documentation is described in the ISMS Control of System Documents Procedure.

The following list presents the primary ISMS documents and policies.

Document	Purpose

ISMS ISO 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
PIMS EU: General Data Protection Regulation	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
ISMS ISO 27001:2022 Statement of Applicability	This document describes how the Organization implements security measures identified in Annex A of the ISO 27001:2022 standard.
ISMS Organization Context	This document describes the internal and external organization context required to properly define an Information Security Management System.
ISMS Information Security Policy	The Information Security Policy is the top-level document in the hierarchy of the Information Security Management System in the Organization.
ISMS Information Classification Policy	This policy defines information categories and their labeling in the Organization.
ISMS Acceptable Use Policy	This Policy defines the acceptable use of resources/assets/information in the Organization.
ISMS External Communication Policy	This Policy defines the rules of communication within the Organization and with its external environment.
ISMS Access to Network and Network Services Policy	This Policy regulates the Users' access to networks and network services.
ISMS Access Control Policy	This policy defines the main rules of managing access control in the Organization.

ISMS Information Transfer Policy	This policy defines the requirements for the secure transfer of information.
ISMS Password Management Policy	This Policy defines the requirements for creating, maintaining, and deleting passwords in the Organization.
ISMS Policy on the Use of Cryptographic Controls	This Policy regulates the use of cryptographic controls and cryptographic keys in the Organization.
ISMS Backup Policy	This policy defines the rules for defining, making, and checking backups.
ISMS Mobile Devices Policy	This Policy regulates the use of mobile devices in the Organization.
ISMS Suppliers Management Policy	This Policy defines the rules for managing Information Security in relations with suppliers.
ISMS Clean Desk and Clean Screen Policy	This policy defines the rules for managing documentation and information in employees' environments.
ISMS Secure Development and Delivery Policy	This policy defines the approach to managing a product/service information security and privacy along its full product life cycle (PLC), including development and service delivery.

Table. System definition.

6 Compliance with Legal Requirements

The Organization declares that the ISMS helps it to achieve compliance with legal requirements. The legal regulations and standards implemented in the Organization are listed in the Normative Sources with a special focus on PIMS EU: General Data Protection Regulation and other data privacy regulations.

The Organization applies special protection measures to the following categories of information (this list is not exhaustive):

1. Legally protected secrets, processed within the Organization, including:
    a. Protected and Confidential information.
2. Personally Identifiable Information (PII, personal data).
3. Intellectual property and legal assets of the Organization, customers, and other entities.
4. Customers' information is protected as specified in individual agreements.

7 Scope of Dissemination

All Users must become familiar with the contents of this document and accept this Policy. The document may be shared with all other entities providing services to the Organization, as well as the authorities and public bodies to present the Organization's information security management system approach. From that perspective, this policy should be treated as a Public document.

Policy Compliance

The Organization will verify compliance with this Policy using a variety of methods, such as the review of user policy acceptance in the ins2outs system, documentation reviews, video monitoring, IT tool reports, internal audits, and feedback to the policy owner.

Policy Non-Compliance

Non-compliance with this policy may result in the initiation of disciplinary proceedings against the persons responsible for the infringement, which may result in termination of the agreement or contract.

Document Hash

0cb8f62fa34ebad4d925ac3ece8cf6c61ce209870919d2b0e8f30c3c755b0302