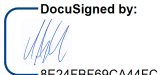




Information Security Management System (ISMS)



Information Security Policy

Client:	BE-terna Ljubljana, BE-terna Zagreb, and BE-terna Belgrade
Project:	ISMS
Version:	3.0
Prepared by:	Prisha Alfiev Justinek, CISO, ciso@be-terna.com
Approved by:	Blaž Strle 
Place & Date:	Ljubljana, 9. 05. 2023

Content

1 Introduction..... 4

1.1 About BE-terna 4

1.1.1 Locations 4

2 Information Security Management System (ISMS)..... 5

2.1 ISMS Scope..... 6

2.1.1 BE-terna ISMS scope 6

2.1.2 Information Security Management System Scope 6

2.2 Activities..... 6

2.3 Information and assets 7

3 Structure of the Information Security Management System 8

3.1 Information Security Objectives..... 8

3.2 Roles and responsibilities 9

4 Framework..... 9

Figures

Figure 1: BE-terna locations..... 4

Figure 2: Information security terms..... 5

Figure 3: Scope of information security in BE-terna..... 6

Figure 4: Activities of BE-terna business processes 7

Figure 5: Digital platforms of BE-terna 7

Figure 6: ISO/IEC 27001:2022 ISMS pillars..... 8

Abbreviations

ISMS – Information security management system

Information Security Policy

Document History

Version	Description	Author	Date
1.0	First Draft	Ines Štefančič, CISO	10.12.2020
2.0	Certification scope, classification and life-cycle of information term added	Ines Štefančič, CISO	05.05.2022
3.0	Renewal of policy based on the new ISO 27001:2022 standard, added scope BE-terna Zagreb and BE-terna Beograd	Prisha Alfirev Justinek, CISO	09.05.2023

1 Introduction

This policy is the core document of BE-terna's ISMS. Here are defined scope, activities, information, and assets of ISMS. Roles and responsibilities regarding information security are defined in chapter 3.2. The ISMS framework is explained and here are listed other topic-specific policies.

1.1 About BE-terna

Empowering businesses for digital success.

We are one of the leading European providers of cloud-based and industry-specific business software solutions.

As a full-service provider we specialize in driving digital transformation and optimizing business processes based on the Microsoft and Infor cloud platforms. We offer and combine best-in-class ERP, CRM, HRM, and data analytics to industry-specific and customer-centric solutions.

Our customers are global corporations and innovative mid-sized companies who strive to gain competitive advantages by using modern, broad, and cloud-based business software applications.

1.1.1 Locations

BE-terna has a strong presence in central Europe with offices in Germany, Austria, Switzerland, Slovenia, Croatia, Serbia, the Netherlands, Denmark, Sweden, and Norway.

Our corporate headquarters are in Innsbruck, Leipzig, Lucerne, Ljubljana and Hørsholm. Our subsidiaries are in Linz, Vienna, Munich, Überlingen, Sindelfingen, Nuremberg, Villingen, Essen, Auerbach, Chemnitz, Erfurt, Maribor, Zagreb, Osijek and Belgrade.

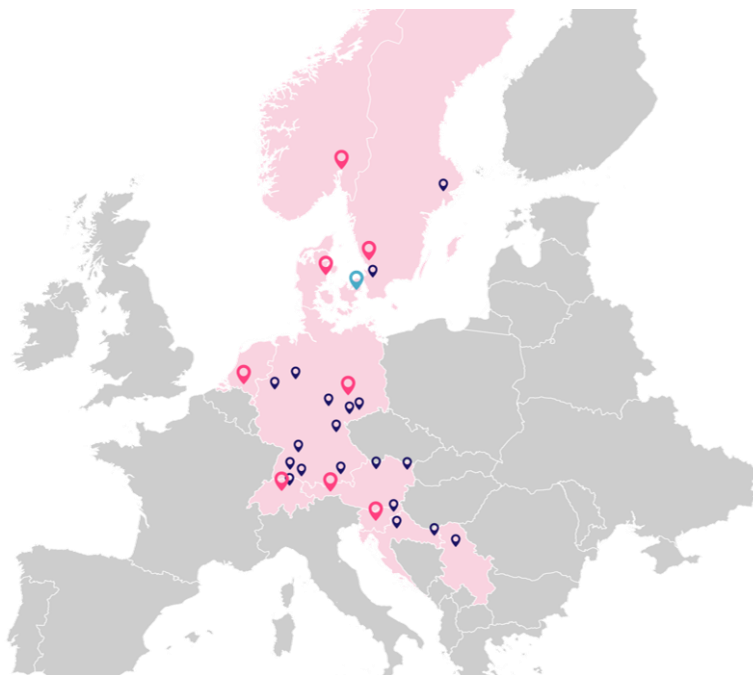


Figure 1: BE-terna locations

2 Information Security Management System (ISMS)

This Information Security Management System is aimed at ensuring:

- Confidentiality,
- Integrity and
- Availability

of information and underlying assets against threats, whether internal or external, deliberate, or accidental, that could affect activities of business processes in BE-terna.

Term	Definition
Information	Knowledge or data that has value for BE-terna or customers.
Assets	Assets on which the information resides and is a resource with economic value that BE-terna owns or controls with the expectation that it will provide future benefit.
Confidentiality	Protection of information so that they are not made available or disclosed to an unauthorized entity.
Integrity	Maintaining the consistency, accuracy, and trustworthiness of information over their entire life cycle.
Availability	Providing accessibility and usability of information upon demand by an authorized entity.

Figure 2: Information security terms

BE-terna manages the Information Security Management System. The Information Security Management System is a set of policies, procedures, guidelines and associated resources and activities, managed by BE-terna with the purpose to protect information assets in scope of this policy.

The approach to BE-terna information security is risk-oriented and conforms to international standards and established good practices. BE-terna information in all forms is protected coherently and commensurately, from its source, through BE-terna, to its recipients; security measures are effective and consistent with classification of these information.

Cyber security is integral part of every service, information system vulnerabilities are remedied as a continuous activity within every process in BE-terna.

Information in all forms within BE-terna are protected coherently and commensurately, from its source, through BE-terna, to its recipients; security measures are effective and consistent with classification of these information.

An information security awareness and education programmes are established to provide employees and contractual workers sufficient training to securely perform their responsibilities. All deviations from the Information Security Management System are controlled by BE-terna ISMS Officers.

BE-terna Information Security Management System follows ISO/IEC 27002 Code of Practice for Information Security Management and ISO 27005 Information Security Risk Management and conforms to ISO/IEC 27001 Information Security Management Systems Requirements.

2.1 ISMS Scope

2.1.1 BE-terna ISMS scope

Development, sales, implementation, and maintenance of software

for companies:

BE-terna d. o. o.
Verovškova ulica 55a
1000 Ljubljana
Slovenia

BE-terna d. o. o.
Strojarska cesta 20
10000 Zagreb
Croatia

BE-terna d. o. o.
Vladimira Popovića 38-40
11070 Novi Beograd
Serbia

2.1.2 Information Security Management System Scope

All information, assets, and activities of business processes in BE-terna are within the ISMS scope, especially:

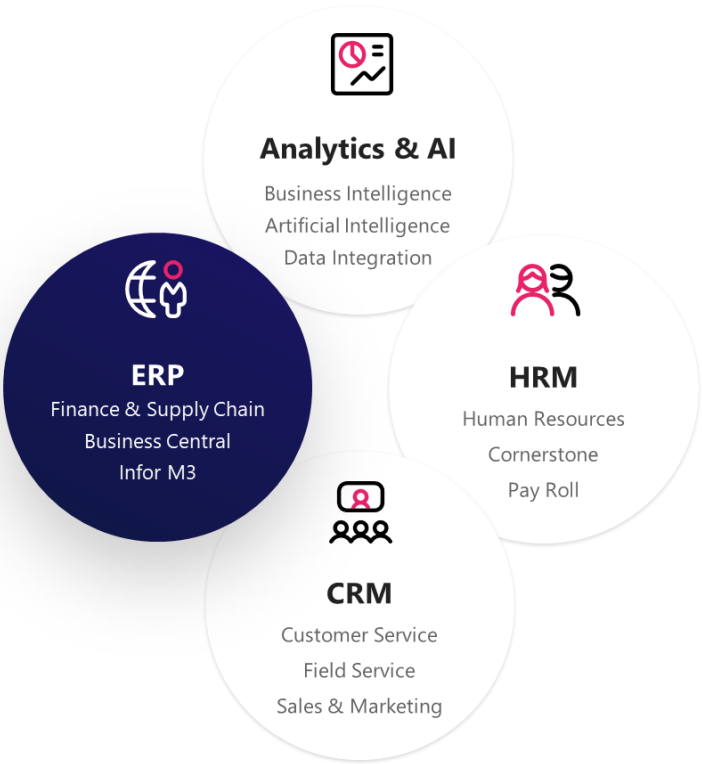


Figure 3: Scope of information security in BE-terna

2.2 Activities

Activities of business processes in BE-terna which are performed for customers are securely managed. In figure 4 below those processes are explained.

Information Security Policy

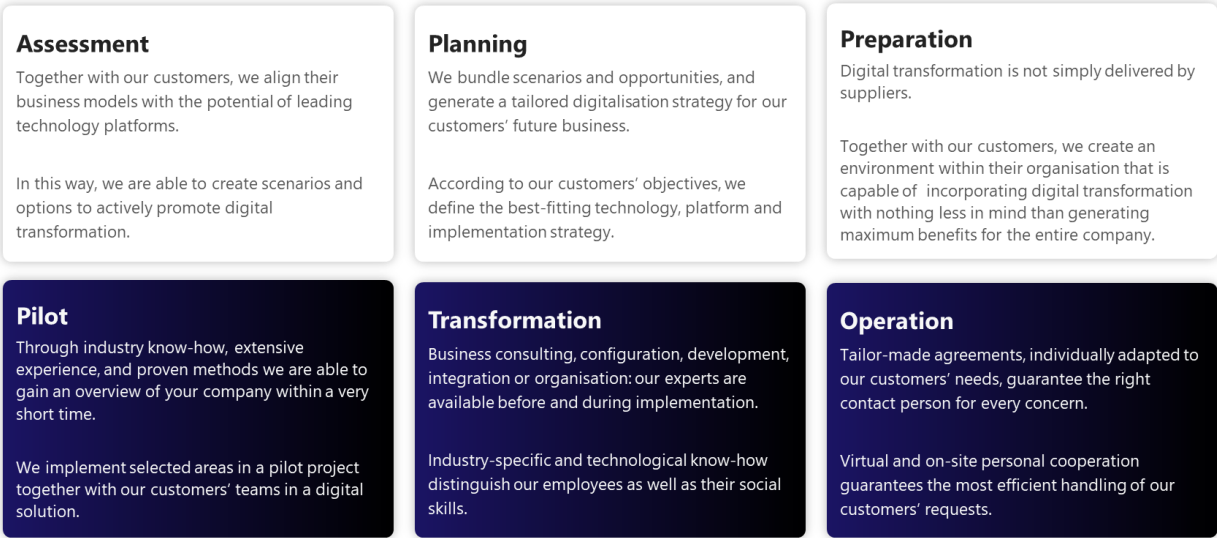


Figure 4: Activities of BE-terna business processes

2.3 Information and assets

Information and assets of BE-terna are focused on services provided within digital platforms such as Business Central, Augmented / Virtual Reality, Analytics & AI, Power Platform, Human Resources, Field Services, Sales & Marketing, Customer Engagement, Project Operations, Supply Chain and Financials.

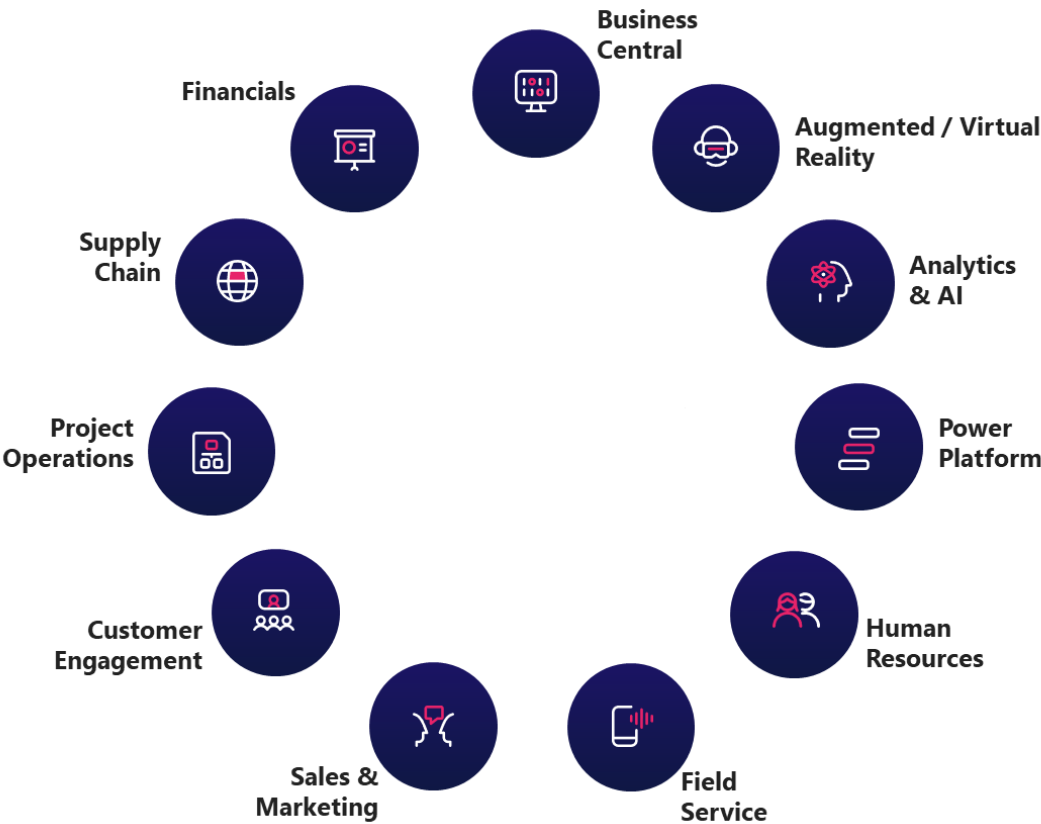


Figure 5: Digital platforms of BE-terna

3 Structure of the Information Security Management System

The Information Security Management System includes all aspects of information security that are presented in the information security policies, based on 4 key pillars of ISO/IEC 27001:2022, these are: organization, people, physical and technological controls.



Figure 6: ISO/IEC 27001:2022 ISMS pillars

3.1 Information Security Objectives

- **Information security policies**

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

- **Organization of information security**

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

- **Human resource security**

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

- **Asset management**

Objective: To identify organizational assets and define appropriate protection responsibilities.

- **Access control**

Objective: To limit access to information and information processing facilities.

- **Cryptography**

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

- **Physical and environmental security**

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

- **Operations and cyber security**

Objective: To ensure correct and secure operations of information processing facilities.

- **Communications and cyber security**

Objective: To ensure the protection of information in networks and supporting information processing facilities.

Information Security Policy

- **System acquisition, development, and maintenance**

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle.

- **Supplier relationships**

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

- **Information and cyber security incident management**

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

- **Business continuity management**

Objective: Information security continuity shall be embedded in the organization's BCM systems.

- **Compliance**

Objective: To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements in the lifecycle of information from creation to archiving or deletion.

3.2 Roles and responsibilities

The Company's management shall bear the overall responsibility for ensuring an appropriate level of information security by the introduction of appropriate technical and organisational measures in business processes to ensure integrity, confidentiality, and availability of information.

The Company's management shall be responsible for proving compliance with ISO/IEC 27001:2022.

The Company's management may transfer responsibilities, duties, and powers to staff members by authorisations. BE-terna managers at all levels are responsible for the implementation of the Information Security Management System and for ensuring employee and contractual workers' adherence to the policies, procedures, and guidelines. All employees and contractual workers are, according to their functions and authorities, responsible for abiding the Information Security Policy.

The COO has appointed regional chief information security officer (CISO) to advise the Company's management about planning, organising, and executing measures to ensure confidentiality, integrity, availability and resilience of processing systems and solutions. The COO has also appointed regional data protection officer (DPO).

4 Framework

The Information Security Policy Framework is defined by a set of security policies:

- Information management
- IT Asset management
- Access management
- System development life cycle
- Change management
- Log management

Information Security Policy

- IT Service management
- Teleworking
- Cryptography
- HR Management
- Physical security
- Business continuity management
- Incident Management
- Risk management

Each policy is structured as follows:

- Introduction
 - Scope
 - Applicability
 - Basic principles
- Responsibilities
- Requirements
- Implementation guidance

Basic principles and requirements in Information Security Policies are part of the Information Security framework that is binding regarding collecting, storing, processing, and sharing of information in all activities and assets in the business processes within the scope. Implementation guidance is intended to assist in meeting the requirements.