

INTEGRATED MANAGEMENT SYSTEM POLICY

ISO/IEC 27001, ISO 22301, ISO/IEC 20000-1 i ISO 55001

The Management of KONČAR – Digital d.o.o. (hereinafter referred to as the Company) is committed and determined to: apply all applicable requirements of international standards ISO/IEC 27001, ISO 22301, ISO/IEC 20000-1 and ISO 55001, continuously improve their suitability, adequacy, and effectiveness, and define and monitor the achievement of set objectives to minimize the risk of adverse events, while ensuring compliance with national legislation across all business processes and relationships with stakeholders.

These Policies apply without exception to all processes within the Company and serve as a framework for the implementation, maintenance, and continuous improvement of the relevant systems. Adherence to the principles and rules established in this Policy, as well as applicable laws and regulations, is mandatory for all employees and is also expected from business partners and all other stakeholders.

The Company's goal is to operate in accordance with professional standards and internationally recognized norms, ensuring and maintaining an appropriate position in global markets for itself and other companies within the KONČAR Group whose services the organization uses.

The policy of the Information Security Management System (ISMS), Business Continuity Management System (BCMS), Service Management System (SMS) and Asset Management System (AMMS) forms the foundation and blueprint for establishing ISMS/BCMS/SMS (hereinafter referred to as the Integrated Management System - IMS) and setting the framework for decision-making, strategy selection, tactics, and direction for achieving IMS objectives.

By adopting this Policy, the Company continues to build a framework for enhancing organizational resilience and readiness for continuous and secure service provision, thereby ensuring the fulfillment of its business mission - delivering products and services to end customers, identifying and meeting stakeholder expectations, safeguarding reputation, and protecting other Company values.

The Policy is expressed in the context of Management Statements as their intent, and serves as a framework for defining and setting all other Company objectives.

In line with the Company's commitment to the optimal functioning of the established systems, this policy is available to all employees, business partners, and other stakeholders on the Company's website and intranet. Any violation of this policy forms the basis for various forms of responsibility.

Statement of Service Management System (SMS) Policy

The ultimate goal is to define all services within the scope, in the "from-to" matrices, and reduce the likelihood of service interruptions delivered by the Company to customers and end users. In the event of an interruption, the intention is to build the organization's capacity to continue business services within a defined timeframe and ensure the necessary resources for full recovery.

In this context, the Company will:

- Develop close relationships with clients
- Actively participate in identifying and articulating client requirements
- Ensure a high level of satisfaction with business requirements in the services offered
- Provide the necessary training and education on solutions to maximize benefits during use and operation
- Ensure independence in work and service use through training and education
- Use the most advanced technical solutions and compatibility with various platforms
- Take care of the security of clients and service-related information
- Ensure that capacity and service change requests are adequately addressed
- Ensure high availability and service continuity
- Regularly review service and improvement requirements
- Monitor compliance with ISO/IEC 20000-1 requirements.

Statement of Business Continuity Management System (BCMS) Policy

The ultimate goal is to reduce the likelihood of business interruptions for the Company. In the event of an interruption, the intention is to build the organization's capacity to continue operations within a defined and/or acceptable timeframe and ensure the necessary resources for full recovery.

In this context, the Company will:

- Establish, maintain, and manage processes necessary for business continuity and the protection of human life, information, and dependent assets involved in the delivery of critical business services and related activities
- Actively manage changes to maintain focus on the most critical activities and assets
- Develop a consistent and proactive approach to identifying potential disruptive events that could harm its digital services and associated valuable assets, reducing the likelihood and/or impact if the risk materializes
- Align business processes with existing incident management practices, improve communication among participants, and contribute to the overall response to disruptive events and incidents
- Identify responsible bodies within Končar Digital for the design and operation of crisis management processes to protect valuable assets and the company's reputation
- Fulfill all legal, regulatory, contractual obligations, and interests of key stakeholders

- Introduce and expand business continuity concepts within Končar - Digital and embed them into existing values and behavior culture through an effective awareness-raising program
- Define a framework for developing comprehensive and effective business continuity plans for services
- Develop, implement, apply, manage, test, and improve business continuity plans for key products/services, processes, and assets
- Maintain a focus on continuous evaluation of products/services to ensure human safety, continuity, and effective business recovery
- Enable effective communication, training, education, and awareness programs for employees and other relevant stakeholders within the business continuity management system
- Ensure the achievement of business continuity management system objectives and the execution of business continuity plans within the agreed MAO/MTPD (maximum acceptable outage/maximum tolerable period of disruption)
- Monitor compliance with ISO 22301 requirements.

Statement of Information Security Management System (ISMS) Policy

We recognize that information security within our Company can have a significant impact on the safety of people and property, the natural environment, product quality, financial performance, and the Company's reputation. Therefore, we are committed to taking all necessary measures and actions to elevate information security to a level recognized by international standards and professional practices.

In line with this, we are determined to protect information assets in terms of integrity, confidentiality, and availability, conduct business ethically, and maintain a secure working environment. Our goal is to permanently maintain the achieved level of information security.

We will achieve the set objectives through good organization, continuous training, and care for the professional and personal development of our employees, with particular attention to systematically monitoring, evaluating, and improving all business processes, especially those affecting information security.

In achieving the set goals, we will pay special attention to the needs of business partners, our employees, local communities in which we operate, the broader society, and society as a whole, as well as the preservation and protection of the natural environment.

Statement of Asset Management System (AMMS) Policy

The asset management system is focused on the processes, rules, functions, and environment within which KOD manages key tangible and intangible assets related to the development, delivery, and support of PROZA and MARS solutions. Acting according to the provisions of the Policy implies support in optimizing the efficiency of assets contained within the open digital platform and modular architecture solutions intended for the company's clients.

In this context, the Company will:

- Establish, manage, and improve the processes, mechanisms, decisions, and functions necessary for a manageable asset management system (AMMS) at KOD
- Primarily treat the open digital platform and modular architecture solutions expressed in the PROZA and MARS products
- Actively participate in asset management throughout its life cycles, from creation to decommissioning
- Appoint responsible personnel who will, with due diligence and prescribed guidelines, manage the defined asset portfolio to maximize its effectiveness
- Manage assets in line with the interests of the company's key stakeholders and in the direction of achieving its defined goals
- Establish processes and educate personnel to manage assets in a dynamic environment, under the growing influence of climate factors, and within the new concept of using "green" energy or renewable resources
- Establish a consistent methodological approach to active risk management over assets, which includes the active treatment of threat elimination
- Ensure processes for adequate incident management over assets and change management processes resulting from regular planned or emergency changes
- Ensure high availability and continuity of assets in development, personal, and client production environments on platforms
- Develop a proactive approach to asset management, budgeting processes, and timely asset engagement to maximize the effectiveness of project implementation and regular business processes
- Ensure the fulfillment of all legal, regulatory, contractual obligations, and stakeholder needs
- Actively promote the AMMS system, education, and improve communication with key personnel
- Establish advanced communication processes with key stakeholders and clients to maximize customer satisfaction and the performance of engaged assets
- Regularly review system provisions, eliminate non-conformities, improve processes, and make decisions that will result in the achievement of system goals.

Overall responsibility for the implementation of the SMS/BCM/ISMS/AMMS Policies (IMS Policies) remains with the ISO Function and the Management of Končar Digital. All employees and third parties within the IMS are expected to act in accordance with it. Any violation of the IMS Policy may be considered a breach of contractual obligations.

Zagreb, 29.06.2024.

Stjepan Sučić, CEO

