NAKA

POLICY ON ENSURING QUALITY, INFORMATION SECURITY MANAGEMENT AND BUSINESS CONTINUITY

POL

DATE
01. 07. 2025

VERSION
3.0

COMPANY
NAKA GLOBAL Ltd. / Letališka cesta 33F / Ljubljana, Slovenia

Document Information

Document Name:	Policy on Ensuring Quality, Information Security Management and Business Continuity
Document Reference:	POL
Confidentiality Level:	Public
Status:	Final version
Version:	3.0
Date of Adoption:	01. 07. 2025
Authors:	Luka Planinc, Timotej Polach, David Mirosavljević
Administrator:	David Mirosavljević, Head of Quality
Reviewed by:	Tamara Starič Petrović, Head of Business Compliance
Adopted by:	Dejan Roljić, Director

Document history

Version	Date of Adoption:	Status:
1.0	03. 05. 2021	Final version
2.0	21. 06. 2021	Final version
2.1	12. 06. 2024	Final version – correction of the point of integrity and authenticity
2.2	05. 06. 2025	Final version - Company correction and editorial corrections
3.0	01. 07. 2025	Final version - Amendments due to the introduction of BCMS

Data confidentiality and copyright

1 Policy on Ensuring Quality, Information Security Management and Business Continuity

With regard to the vision of the Company and with regard to the level of awareness and responsibility for the implementation of the systems for the quality management, information security management and business continuity management (hereinafter: **the Management System**), the management of the Company has adopted this Policy of Ensuring Quality, Information Security Management and Business Continuity (hereinafter: **the Policy** or **POL**), which defines (i) the objectives of ensuring the quality of the Company's products and services, (ii) the objectives of ensuring information security and (iii) the objectives of ensuring a business continuity management system.

The purpose of the quality management system is: (i) to enable a qualitative assessment of the quality of the results, (ii) to monitor the compliance of the results with the plans, technical specifications and good practice, (iii) to ensure the continuity of the implementation of the information security system, (iv) to regularly inform key persons about the results and materials, thereby enabling them to submit comments and views in a timely manner, thereby introducing corrective actions and improvements. The quality of the results is of utmost importance to meet the specific and/or expected needs of customers and end users of our products and services. Ensuring quality is just as important with respect to the quality of the results achieved by contractors, as it is with respect to those achieved by employees.

The purpose of information security management is to set basic security starting points for the protection of the Company's information assets from threats, whether internal or external, intentional or accidental. Therefore, the Policy contains binding rules relating to the general principles of conduct, access, processing, storage, transfer and destruction of information data within the Company. It is a document that must be followed by everyone who has access to the Company's information assets – the director, employees, external associates, as well as third parties.

The purpose of business continuity management is to ensure robust operations of the Company, to reduce the possibility of interruption of the Company's operations due to disruptions or extraordinary events that may affect the provision of essential (critical) processes within the Company, and to ensure an appropriate response of all responsible persons in the Company in the event of such an event.

Quality assurance of products and services is carried out primarily by conducting a quality assessment, which is made for all major products and services. Ensuring quality of information security processes is carried out through annual internal audits. When ensuring a quality management system it is crucial that an attempt is made to ensure the highest possible level of independence in quality assessment. The assessment is carried out by independent individuals who are not involved in the process of preparing the results and objectives of each process.

The Company's management ensures quality, information security management and business continuity system management by:

- informing and reminding employees of the importance of consistent compliance with requirements in connection with products and services, the importance of information security and the importance of strict compliance with legislation and other legal requirements, while at the same time encouraging employees to be aware of the importance of responsibility for the implementation of the processes entrusted to them, as well as the importance of appropriate response in the event of emergencies;

- takes care of the implementation of the management system, which has been made known to all employees;
- regularly reviewing the POL and related documents;
- ensuring that quality objectives (in terms of the system, processes, projects and products) are always clearly defined;
- ensuring the availability of resources for the adequate, high-quality and efficient implementation of the Management Systems;
- ensuring that processes and procedures to ensure quality, information security and business continuity are consistently implemented at all stages of the life cycle of products and services, or that the operations of critical processes of the Company continue regardless of any extraordinary events;
- monitoring and supervising the implementation of development tasks and reviewing reports on the progress;
- supporting the implementation of measurements and analyses of operations and, on the basis of the results, determining at least once a year the extent to which the quality objectives have been achieved;
- conducting management reviews;
- determining the necessary corrective actions;
- setting new, higher goals through improvement programs.

Procedures for ensuring quality are broadly divided into procedures that include quality planning, i.e., defining the quality standards (when they can be defined) and defining the necessary activities for quality assessment, as well as the procedures actually used to assess the quality of the results. Quality growth in the Company is decisively based on a long-term quality improvement plan. This is achieved through the following steps:

1. **Planning**: Setting the basic standards that the Company must constantly follow to ensure a high level of quality and information security. It requires setting concrete strategic goals for achiving quality and information security in the Company, which precisely define the direction that the Company must follow in order to meet the level of quality and information security it has set for itself. In addition to setting baseline standards, the planning process also requires establishing measures to address risks and opportunities.
2. **Operation and implementation**: Determination of requirements for products and services, determination of requirements for supplier verification; determination and management of processes for the development of products and services.
3. **Performance evaluation**: Internal assessment and management review.
4. **Action**: Depending on the established results of the Management System, the management makes appropriate decisions on corrective and preventive measures to eliminate and prevent the causes and discrepancies for the future.

The aforementioned elements of the Management System process ensure the fulfilment of the requirements for the quality of products and services and the requirements in terms of information security management, such as the protection of:

- **Confidentiality and Secrecy**: protecting business and personal data and other important information from disclosure to unauthorized persons and ensuring accountability for the services provided;
- **Integrity**: addresses ensuring the accuracy and integrity of information and software. Integrity checks are used to protect data and systems from unauthorized modification. Integrity facilitates the identification of changes and prevents the altered copy from being treated as an original;
- **Authenticity**: authenticity refers to the genuinity and non-falsification of data, information and systems, with respect to their condition, form and quality;

- **Availability and Accessibility**: protecting data, information and services from interruptions in operation and providing information to authorised users at the appropriate time and in an appropriate manner.