NAKA

QUALITY ASSURANCE,INFORMATION SECURITY MANAGEMENT AND BUSINESS CONTINUITY POLICY

POL

DATE
01. 06. 2026

VERSION
3.2

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

Document Information

Document Name:	Quality Assurance,Information Security Management and Business Continuity Policy
Document reference:	POL
Confidentiality level:	Public
Status:	Final version
Version:	3.2
Date of admission:	01. 06. 2026
Authors:	Luka Planinc, Timotej Polach, David Mirosavljević
Administrator:	Quality Assurance Manager
Reviewed by:	Tamara Starič Petrović, Head of Business Compliance
Accepted:	Dejan Roljić, Director

Document history

Version	Date of admission:	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 - Amendment due to SUNP
3.1	22. 05. 2026	Draft – reviewed 2026
3.2	01. 06. 2026	Final version – reviewed 2026

Data confidentiality and copyright

1 Quality Assurance, Information Security Management and Business Continuity Policy

With regard to the vision of the Company and with regard to the level of awareness and responsibility for the implementation of the Quality Management System, Information Security Management and Business Continuity (hereinafter: **Management System**), the Management of the Company has established a policy of quality assurance, information security management and business continuity (hereinafter: **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 (including those relating to ensuring the protection of personal data when processed in public clouds) 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 contents, 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. Quality assurance is just as important to the quality of the results achieved by contractors as it is to those achieved by employees.

The purpose of information security management is to set basic security bases 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 also contains requirements related to the processing of personal data in the company's ICT systems, especially in cloud systems. It is a document that must be followed by everyone who has access to the company's information resources – the director, employees, external collaborators, as well as third parties. In this regard, it is also important to take into account the purposes of managing the protection of personal data in public clouds, which include ensuring the highest level of privacy in the processing of data of our users and their customers, including ensuring the limitation of the purpose of personal data processing, prohibition of marketing, data security, transparency of processing and ensuring the rights of individuals.

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 of 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. Quality assurance of information security processes is carried out through annual internal audits. It is crucial to ensure a quality management system 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:

- informs and reminds 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, with which all employees are familiar;
- regularly review the POL and related documents;
- ensures that quality objectives at system, process, design and product level are always clearly defined;
- ensures the availability of resources for the adequate, high-quality and efficient implementation of management systems;
- ensures 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;
- monitors and supervises the implementation of development tasks and reviews reports on their progress;
- support the implementation of measurements and analyses of operations and, on the basis of their results, determine at least once a year the extent to which the quality objectives have been achieved;
- conducts management reviews;
- determine the necessary corrective actions;
- Through improvement programs, it sets new, higher goals.

Quality assurance procedures are broadly divided into procedures that include quality planning, i.e. the definition of quality standards (when they can be defined) and the definition of the necessary activities for quality assessment, and 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 quality assurance 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 above 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;

- **Comprehensiveness:** 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 authenticity and non-falsification of data, information and systems, in 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.

In addition**, privacy and transparency are ensured**, which include the company's obligation to ensure that cloud data processing operations are transparent, clearly communicated to customers, and strictly limited to the agreed scope of service delivery.