Krka Group Information Security Policy

1 Purpose and Scope

This Information Security Policy (hereinafter: the Policy) applies to the controlling company Krka, tovarna zdravil, d. d., Novo mesto, and its subsidiaries, which together constitute the Krka Group (hereinafter: Krka).

The Policy sets out information security principles and commitments, but does not include confidential operational details, technical configurations, internal procedures or references to internal documents. The Policy covers information assets used in business operations, regardless of their form, location or technology platform.

It sets out the publicly available principles according to which Krka manages and protects information against unauthorised access, disclosure, alteration, destruction, disruption, misuse or loss. It describes Krka's approach to information security governance and its commitments regarding the confidentiality, integrity, availability and authenticity of information.

The Policy applies to all Krka employees. It also applies to contractors, suppliers, service providers and anyone who accesses Krka's information assets. Krka requires them to protect information by applying appropriate security practices and acting responsibly.

At Krka, we align the information security framework with established international standards and applicable regulations. Where national requirements are more stringent, we comply with them.

Krka recognises information and data as key business assets. We protect them through responsible governance, risk management, employee training and regular awareness activities, preventive action and continual improvement.

2 Governance and Responsibility

We provide comprehensive governance mechanisms to oversee information security and integrate it into business planning, risk management and operational decision-making at Krka level.

Information security is the shared responsibility of all Krka employees. The Krka Management Board provides direction for information security governance and oversight. The Chief Information Security Officer (hereinafter: CISO) coordinates the management system, participates in identifying and managing risks, monitors the effectiveness of established systems and promotes continual improvement in information security. The person responsible for business continuity oversees the business continuity management system, while the Data Protection Officer provides support in the protection of personal data. Security engineering within Information Technology actively monitors, reviews and assesses the security of the information environment.

Information owners are responsible for protecting and controlling information generated in their processes, including its classification, identification of related threats and risks, approval and review of access rights, segregation of incompatible duties, and the secure handling, retention and disposal of information throughout its life cycle. Human Resources and other functions that process the personal data of employees and other individuals ensure the security of personal data in accordance with applicable regulations.

Oversight of the information security management system is exercised through Krka's corporate committees. These committees monitor management reviews of the information security management

system, review and approve risk assessments and risk treatment plans, examine the results of internal audits and compliance assessments, and monitor the effectiveness of security measures.

CISO reports at least annually on the effectiveness, adequacy and compliance of information security governance. The Krka Management Board is responsible for making key decisions concerning this system.

3 Information Security Principles and Commitments

Confidentiality

Information is accessible only to authorised persons and is handled according to its sensitivity and legitimate business needs.

Integrity and Authenticity

Information is protected against unauthorised or accidental alteration. At Krka, we strive to ensure the accuracy, completeness, reliability and verifiability of information.

Availability and Resilience

Information and supporting services are available when needed. Preventive action through measures that ensure resilience, business continuity, and data and system recovery supports key business activities.

Protection Based on Identified Risks

We implement security measures based on identified risks, business needs, regulations and recognised good practices.

Protection of Information Throughout Its Life Cycle

We protect information during its creation, use, exchange, storage, retention and secure disposal.

Responsible Planning and Implementation of Changes

We take information security requirements into account when planning or introducing business processes, technologies and services, and when implementing significant changes.

Access Rights Management

We assign access rights according to roles and business needs and review them regularly.

Continual Improvement

In response to the changing business environment, we review and assess risks and improve the information security management system, practices, measures and capabilities.

Segregation of Responsibilities

Responsibilities and authorities are clearly defined and segregated to prevent conflicts of interest.

Compliance and Cooperation

We comply with applicable regulations and contractual obligations, report potential incidents in accordance with them, and cooperate with the competent authorities.

4 Information Security Management

We maintain an information security management system, which is a structured framework for setting information security objectives, managing risks, implementing measures, evaluating performance and improving information security. We observe the following commitments:

4.1 Risk and Vulnerability Management

We identify and assess information security risks and implement appropriate measures to address them. We perform vulnerability analyses and security reviews to identify vulnerabilities, assess exposure and prioritise corrective actions.

We conduct risk assessments periodically and following major organisational changes, changes of location, or major changes to information systems and services. We assess threats, the likelihood of their occurrence and their potential consequences. On this basis, we prioritise organisational, physical and technical measures and reduce residual risk to an acceptable level. We also consider relevant external factors that could affect information systems and facilities.

4.2 Incident Reporting and Handling

Reporting channels are in place through which information security incidents, vulnerabilities, security weaknesses or suspicious activities can be reported. Reports are handled by authorised or responsible persons. Further actions are determined according to the nature and potential impact of the event.

Information technology incidents must be reported to sos@krka.biz, by telephone on +386 7 331 2114, or to the Compliance Officer at compliance.officer@krka.biz or by telephone on +386 7 331 2600.

4.3 Business Continuity

Business continuity and data and system recovery plans support the availability of key information systems and services during disruptions. We maintain, test and improve these plans in accordance with business needs and risks.

4.4 Data and Information Protection

We implement measures to protect data and information throughout their life cycle. We classify and handle information according to its value, sensitivity, applicable regulations and business requirements. We manage retention and disposal in accordance with applicable regulations.

4.5 Notification of Significant Incidents to Competent External Authorities

We are required to notify the competent authorities of significant information security incidents within the time limits and in the manner prescribed by applicable regulations. Authorised functions coordinate notification and all subsequent communication in cooperation with the responsible Management Board member and CISO. This also applies to Krka's units abroad, where local responsible persons communicate with the competent local authorities in cooperation with the relevant functions and CISO at Krka's controlling company. Public communication concerning incidents is conducted in accordance with Krka's corporate communication rules and the instructions of the competent authority.

4.6 Security Measures and Cyber Hygiene

We implement organisational, physical and technical security measures proportionate to the identified risks and applicable requirements. Without disclosing configurations or other operational details, these measures include:

- cyber hygiene and timely software updates, including remediation of known vulnerabilities;
- network segmentation and separation of critical systems, and management of data traffic and communications;
- identity and access management, including multi-factor authentication;
- protection against malware, and monitoring and retention of activity logs;
- appropriate cryptographic protection of sensitive information;
- redundancy of critical infrastructure, secure backups and regular testing of data and system recovery;
- security testing, including independent security reviews and penetration tests;
- secure design and implementation of changes to systems, networks and software;
- physical and technical protection of premises and equipment;
- monitoring of information security threats and vulnerabilities;
- ongoing assessment and handling of security events, with appropriate response and escalation.

The effectiveness of implemented measures is assessed and improved based on reviews, testing and lessons learned.

4.7 Data Integrity in Regulated Processes

Information generated in research and development, manufacturing, quality assurance and other regulated processes is used as evidence of activities performed and as a basis for decision-making. We therefore comply with requirements concerning the integrity, accuracy, completeness, authenticity and traceability of such information, including requirements applicable to computerised systems, electronic records and electronic signatures. We retain, archive and dispose of this information in accordance with applicable legislation.

5 Information Security Culture

At Krka, we promote a culture of secure behaviour, responsible handling of information and timely reporting of potential risks.

We raise awareness and train employees in information security so that they can more easily recognise threats, understand their own responsibilities and the protection of information, and use information resources appropriately. Awareness activities are regularly updated to reflect current threats, technologies and ways of working.

Employees:

- protect information, information resources, trade secrets and other confidential data entrusted to them;
- comply with applicable information security requirements;
- use access rights and company assets responsibly;
- report changes in their area of work that could affect information security or business continuity;
- participate in required information security awareness and training activities;
- immediately report incidents, threats and suspicious activities;
- cooperate in authorised reviews, investigations and corrective actions.

6 Information Security in Cooperation with Contractors and Other Partners

Third parties (suppliers, service providers and other third parties) may participate in carrying out Krka's processes or processing its information. We define information security requirements for them in proportion to the type of service, the scope of access and the associated risks.

We take information security requirements into account when selecting contractors and other partners, concluding contracts, onboarding, delivering services, making changes and terminating cooperation.

We assess the security practices of these partners that are relevant to Krka and monitor compliance with agreed requirements. Partners notify Krka of security incidents and cooperate in risk management, investigations, remediation and business continuity activities.

We also enforce information security requirements throughout the information and communication technology (ICT) supply chain. We carefully select IT service suppliers, cloud service providers and other partners that process Krka's information or have a significant impact on Krka's information security or business continuity, assess them from a risk perspective and evaluate them in various ways. Security requirements are included in contracts and service and product specifications. We monitor compliance with these requirements and retain evidence of completed assessments. We also prepare exit plans that enable transition to other solutions or termination of services without a significant impact on Krka's operations.

7 Review, Certification and Improvement

7.1 Internal and External Review

We conduct internal audits and reviews of infrastructure, information technology and the information security management system. Risk assessments, vulnerability analyses, management reviews and other assurance activities help assess whether the measures remain appropriate and effective.

We ensure independent external audits and assessments of Krka's information security management system and information technology environment. These activities provide additional assurance and also enable the identification of opportunities to improve governance, risk management and measures.

7.2 Commitment to ISO/IEC 27001, Compliance Assessment and Reporting

We are committed to maintaining the ISO/IEC 27001 certification already obtained for information security management systems, which includes an independent external audit. Maintaining this certification supports a systematic approach to information security that enables risk management and continual improvement.

We regularly review and update the Statement of Applicability, which defines how we address the controls in ISO/IEC 27001. We regularly and periodically assess compliance with applicable information security regulations and document the results. We define corrective and preventive actions and monitor their implementation through to completion.

8 Cooperation with Competent Information Security Authorities

We provide the competent authorities with all notifications and disclosures required by applicable regulations or by the competent authorities.

We cooperate with competent national authorities, national computer security incident response teams, personal data protection supervisory authorities, external experts, professional organisations and interest groups.

We monitor applicable regulations, recommendations, guidelines and standards and incorporate necessary changes into Krka's information security management system. We also monitor external sources of information on emerging threats and take them into account in measures for preventing and detecting those threats.

9 Final Provisions

The Policy was adopted by the Management Board of Krka, tovarna zdravil, d. d., Novo mesto, at its 13th regular meeting on 21 October 2026.

The Policy is a public document and is published on Krka's website. It is reviewed and, where necessary, updated at least once every five years and whenever significant changes occur in the applicable legal framework. All amendments and supplements must be approved by the Management Board.