APPROVED
By Decision of the Supervisory Board 140/2025 dated 17.10.2025
Entered into force on 17.10.2025.
Approved by Decision of the Management Board No. 975 dated 03.10.2025

INFORMATION SECURITY POLICY REQUIREMENTS IN JOINT-STOCK COMPANY "KREDOBANK"

In order to ensure the highest possible level of security of banking services and products provided to the Bank's Clients, as well as internal processes, infrastructure, ICT and information processed in them, the Bank has implemented an Information Security Management System (ISMS) and ensures the maintenance, improvement and development of the ISMS, taking into account the requirements of:

- regulatory and legal acts of the National Bank of Ukraine,
- standards ISO/IEC 27 001:2022, ISO/IEC 27002:2022, ДСТУ(State Standard of Ukraine) ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Information security, cybersecurity and confidentiality protection. Information security management systems. Requirements; ДСТУ(State Standard of Ukraine) ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) Information security, cybersecurity and confidentiality protection. Means of information security control;
- requirements stipulated by the current legislation and internal regulatory documents of JOINT-STOCK COMPANY "KREDOBANK" (hereinafter referred to as the Bank);
-requirements of card organizations and payment systems, a participant of which is the Bank;
- international standards on information security, cybersecurity and information security in cloud environments, generally accepted in international practice principles of ensuring information security and cyber protection;
- requirements arising from concluded agreements.

Section 1. Declaration of the Bank's Management Board.

1.1. The Bank's Management Board is aware that the Bank's current and future position in the financial market depends on:

- speed, efficiency and accuracy of identifying threats/cyber threats and favorable conditions for the Bank's activities;
- assessment of the probability of their occurrence;
- assessment of their impact on the continuity, quality and compliance with the legislation of the Bank's business processes, as well as the impact on the Bank's market position and image;
- effectiveness of selecting and implementing appropriate measures to prevent threats/cyber threats or reduce their negative consequences;
- accuracy of selecting and implementing solutions that increase the probability of using opportunities;
- deep digital transformation in all aspects of its activities, bold changes in the operating model and distribution model;
- diversification and discipline in the field of risk management and cybersecurity, resilience to market shocks.

1.2. The Bank has identified external and internal circumstances that are important for achieving its goals and affect the possibility of achieving the planned results of the information security management system.

1.3. Given that the nature of threats in banking activities is changing towards cyber threats, the Bank's Management Board pays special attention to ensuring information security and cyber protection of the Bank's ICT and the data processed in it, and also understands the need to adopt a holistic, systemic approach to information security management in the Bank.

1.4. The functioning of the cyber protection system is based on the principles of:

1) proportionality and adequacy of the implemented cyber protection measures to real and potential cyber threats;
2) prioritization of preventive measures;
3) minimization of cyber risks in the Bank's activities;
4) compliance with the requirements of the National Bank's regulatory legal acts on information security and cyber protection, recommendations of the National Bank, including those that may be provided by the National Bank based on the results of control;
5) constant support by the Bank's Management Board for the bank's cyber resilience by organizing effective cyber risk management.

Section 2. Information security management system.

2.1. **The Bank is constantly improving, enhancing the suitability, adequacy and effectiveness of the ISMS**, which aims to provide management with confidence in:

- compliance with the requirements of the Information Security Policy and information security objectives,
- conducting an analysis of information security/cybersecurity events and incidents and taking corrective and preventive actions to minimize the prpbability of their recurrence in the future;
- analyzing the results of audits;
- conducting an assessment of information security risks and drawing up a risk treatment plan;
- conducting an analysis of ISMS performance indicators, including feedback from stakeholders;
- analyzing ISMS non-conformities and planning corrective actions.

2.2. The Bank **manages information security risk**, which is implemented in compliance with the three lines of defense model and ensures comparability of results, taking into account the requirements of the National Bank's regulatory acts regulating the organization of information security and cyber protection measures, and ensures:

- compliance with the principles of information security and cyber protection and mandatory minimum requirements for the organization of information security and cyber protection measures;
- implementation of effective measures to ensure the confidentiality, integrity and availability of information, its protection from internal and external threats, including cyber attacks and threats to physical security.

2.3 . Information security events and incident managements includes:

- prompt detection and recording of information security events, event assessment to confirm classification as an information security incident;
- incident response – consists of identifying and taking special security measures or corrective actions, in accordance with the priority of incident processing;
- incident analysis – consists of establishing, verifying information about the incident and the measures taken in connection with it, which takes into account the priority of incident processing, documentation and escalation of the incident (if necessary), collecting evidence and traces related to the occurrence of the incident, identifying its causes;
- improvements that limit the recurrence of a security incident – consist of taking corrective measures, system solutions aimed at preventing the recurrence of a security incident in the future;
- information obtained from the analysis and processing of information security incidents is used in the assessment of information security risks to reduce the probability or impact of future incidents.

To reduce the risks of the occurrence of information security incidents, the Bank carries out systematic actions to raise the level of staff awareness of information security, namely:

- notifying the Bank's employees about the implementation (new or changes) of internal regulatory documents that define the principles of security (in particular, this Policy) and the obligation of employees to familiarize themselves with them and comply with the requirements of these documents;
- conducting trainings and exercises for employees in the field of information security;
- conducting internal campaigns and events (activities), in particular after a serious security incident and in the event of the detection of information about new methods of attacks on Banks and their Clients;
- conducting security tests and audits (including socio-technical tests), testing the Bank's business continuity plans and discussing their results with the responsible persons of the relevant structural divisions.

Each employee of the Bank is obliged to report the occurrence of an information security incident. The principles and procedure for reporting and contact details of persons to be notified are defined in a separate document, which describes in detail the procedure for responding to information security incidents.

All employees of the Bank, when entering the job, sign an undertaking not to disclose restricted information, including banking secrecy and personal data. Employees of the Bank are obliged not to disclose or use for their own benefit or for the benefit of third parties restricted information that has become known to them in the course of performing their official duties.

The Bank operates a Training and professional development programme for on information security issues, which defines the goals, objectives, main types of training, the procedure for interaction between the Bank's structural divisions, and the authorities and responsibilities of employees when organizing training on information security and cybersecurity.

2.4**. The Bank operates a principle of granting the minimum level of authority** when granting access to the bank's information systems (including access for privileged users).

2.5. **The Bank's software** must comply with the information security requirements of the legislation of Ukraine, documents and standards of the NBU, as well as international standards ISO 2700X and meet the following requirements:

- availability of a built-in information protection system, and it is impossible to process information without its use;
- availability of built-in mechanisms for proper protection of information during its transmission between various subsystems in which information is processed;
- for automated systems operating in the "client-server" mode, user access to the database should occur only through additional software, which authenticates and authorizes persons who are allowed to use this database;
- the use of enhanced authentication of the payment service user;
- availability of built-in mechanisms that ensure unambiguous and undeniable identification of the user on each access device to the system, in each module or element of the system to which the user has access, as well as when performing any operations in the system;
- ensuring the possibility of automatic blocking of the account in the system after exceeding the number of allowed unsuccessful attempts to enter the password on any device for accessing the system of ensuring continuous technological control over the integrity of information and imposing/verifying a digital signature on all payment bank documents at each stage of the technological cycle of their processing; ensure encryption of electronic banking documents containing confidential information during transmission on external carriers or via appropriate communication channels in on-line mode with appropriate confirmation of their receipt; ensure mandatory registration of all access attempts, all operations and other actions in the system, as well as their recording in an automated system, in an electronic register protected from modification, with constant control of its completeness and integrity.

The above requirements must apply both to ready-made software purchased by the Bank (COTS – Commercial Off-The-Shelf), and to software developed by the Bank independently or by external suppliers in accordance with the Bank's order.

The Bank uses the standards, documents and guidelines of the Open Web Application Security Project (OWASP) for the development of secure applications

2.6. The Bank maintains a high level of security of information processed, stored and transmitted using cloud storage technologies. The processes of acquiring, using, managing and exiting cloud services must be established in accordance with the Bank's information security requirements that comply with legal requirements.

2.7. The Bank has developed, operates, tests and updates a business continuity plan, which takes into account the continuity of information security measures within the framework of the Bank's business continuity management process, measures to restore information systems after failures.

2.8. Each employee or person cooperating with the Bank is obliged to contribute to activities aimed at achieving and maintaining an appropriate level of information security in the Bank to the extent consistent with his/her official duties and granted authorities.

2.9. **The Bank requires Suppliers** to have knowledge and comply with information security requirements, in particular, in contractual relations to regulate issues in the field of protection of the Bank's assets and to guarantee that the access they receive to the Bank's assets will be used exclusively for the purpose of providing services in accordance with the contract concluded between the Bank and this Supplier, and the Supplier will not initiate access to such assets unless this is specified in the written contractual relations between the parties.

Suppliers are obliged to inform the Contract Supervisor of any changes and problems that arise in the course of cooperation, in order to take the necessary measures to maintain the continuity of the provision of the service.

Suppliers are obliged to inform the Contract Supervisor of any incidents related to information security that were registered during the provision of the service in favor

of the Bank, including situations where the incident was detected after the termination of cooperation.

Section 3. Information Security Objectives

The principles implemented by the Bank, arising from the Information Security Management System, must ensure the achievement of the following information security objectives:

- **Compliance with legal requirements**. When processing information by the Bank, and in particular the organization of its protection, must comply with the current legislation of Ukraine and the requirements of the security standards of the PKO Bank Polski S.A. group.
- **Information accessibility.** Information and means of its processing are available to authorized persons and to the PKO Bank Polski S.A. group. The Bank ensures an acceptable level of information accessibility, taking into account the requirements of the law and the Bank's operational activities.
- **Information confidentiality**. Information is available exclusively to persons and processes that have appropriate access rights to them. These rights arise, in particular, from the ownership of the information (information of the Bank's Clients), as well as the duties and tasks performed for the benefit of the Bank by the Bank's employees and service providers.
- **Information integrity**. The Bank applies organizational and technical measures that ensure the protection of the accuracy and completeness of information, and the protection of the correct operation of mechanisms that process information. In particular, information is protected from unauthorized changes.
- **Surveillance.** Ensuring the ability to identify users and processes, as well as record the actions of users and processes on this information in order to prevent and/or investigate violations of the security policy.
- **Application of the principles of secure information processing**. Information processing and exploitation of its processing facilities are carried out in accordance with the specified principles. The principles that are valid for external business entities are implemented on the basis of agreements concluded with the Bank.
- **Information protection supervision**. The Bank monitors whether the method of processing information meets the requirements for information protection. In case of confirmation of non-compliance, timely measures are taken to correct them.
- **Adequate protection of information and means of its processing in relation to the level of risk**. The selection of protection means follows from the management of information risk in the Bank. This approach makes it possible to ensure the efficiency of information processes
- **Adequate optimization of protection measures in accordance with the current needs of the Bank**. Through risk management, auditing, review and measurement of effectiveness, the Bank determines whether organizational and technical protection measures are optimal for the security requirements and operational activities of the Bank.
- **Ensuring a rapid and effective response to information security breaches**. The Bank promptly responds to any signs of information/cybersecurity breaches, which ensures the minimization of the likely negative consequences of the event and the adoption of immediate corrective actions.

Section 4. Basic principles of information security insurance

The organization of the Bank's information security is based on the following fundamental principles:

- **The principle of least authority**: access of the Bank's employees and users of information systems to the information resources of the Bank's computer network must be organized in such a way as to provide only those powers that are necessary to perform official tasks.
- **The principle of necessary knowledge:** each employee or person cooperating with the Bank possesses only that information about the Bank's information resources, means of their processing and methods of their protection that is necessary to perform the assigned tasks and duties. Third parties have access only to that information that the Bank has determined to be public (open).
- **The separation of duties principle:** performance of tasks that are critical from the point of view of the security of the Bank's financial and information resources, information and communication systems and banking services is organized in such a way that their implementation requires the participation of more than one person ("two-handed rule").
- **The principle of sanctioning actions:** those actions of Bank employees that are not explicitly permitted by law, NBU regulations, internal administrative or regulatory document, that are prohibited.
- **The principle of legality:** The Bank's ISMS takes into account the requirements of the current legislation of Ukraine, as well as the requirements of international regulatory requirements in the field of information security.
- **The principle of coherence and unity**: the goals and objectives of information security correspond to the strategic goals and business objectives of the Bank, and information security management is an integral part of the Bank's management.
- **The principle of adequacy and effectiveness:** means of protecting information resources are implemented in accordance with their criticality, i.e. the classification category and risk level of the information resource, based on the principles of risk assessment adopted by the Bank.
- **The principle of practicality:** means of protecting information resources must be practical and maintain a balance between the operability and security of information systems.
- **The principle of continuity:** information security is a continuous process of countering threats/cyber threats and managing risks specific to the Bank's field of activity.
- **The principle of of responsibility:** the Bank's management at all levels, employees, suppliers and other third parties who have access to the Bank's information resources must comply with the requirements of the Bank's internal documents in the field of information security and are personally responsible for their implementation.
- **The principle of continuous improvement:** the Information Security Management System implemented in the Bank contains mechanisms and indicators for measuring and monitoring the effectiveness of the management system and implemented measures for rational planning and implementation of improvement actions.
- **The principle of multi-level protection:** the organization of information security involves the creation of the following series of sequential levels of protection of information resources and personnel of the Bank from potential threats/cyber threats:

- organizational and legal level, which determines the legal and regulatory requirements and obligations of personnel, users of information resources and counterparties of the Bank regarding information security;
- physical level of protection, which prevents unauthorized physical access, damage or intrusion into the Bank's office premises for the purpose of unauthorized access to information;
- application software level, which is responsible for interaction with the user of information resources;
- database management system level, which is responsible for data storage and processing;
- operating system level, which is responsible for safe and reliable maintenance of application software and database management systems;
- network level, which is responsible for the interaction of nodes of the Bank's information system.

- **Principle of comprehensiveness and systematicity:** the Bank's information security is built comprehensively, taking into account all aspects of information protection, in particular:

- security strategies and objectives,
- management of information resources and information carriers,

- human resources security,
- management of physical security and environmental security,
- security of relations with suppliers,
- security of internal and external communication processes,
- management of compliance with legal, regulatory and contractual requirements,
- management of information security incidents,
- business continuity management,
- security in the processes of design, search, development, implementation and support of IT systems,
- security in the processes of operation of IT systems,
- 100% identification of the risk of system changes to the continuity and integrity of their functioning.

The systematic approach to information security management adopted by the Bank provides for ensuring consistency of processes and actions taken in the field of security:

- with the conditions of the environment in which the Bank operates,
- with the Bank's strategy and business goals,
- with the results of the risk and opportunity assessment,
- with the results of the assessment of the effectiveness of the management system and the implementation of protection measures,
- with all aspects of the Bank's operational and information technology management.