Information Security Policy
of KREDOBANK JSC

In order to guarantee the maximum level of security of provision of banking and financial services/conduction of economic transactions, as well as internal processes, infrastructure, ICT and information being processes in such system, the Bank implemented the Information Security Management System (ISMS) as required by the standards of the National Bank of Ukraine and ISO/IEC 27001:2022.

Through the implementation, maintenance and development of the ISMS, the Bank undertakes to comply with information security requirements and consistently improve the ISMS.

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

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

1. Considering the fact that the nature of threats in banking is changing toward cyber threats, the Management Board of the Bank pays special attention to ensuring information security and cyber protection of the Bank's ICT and the data processed in it, and is also aware of the need to adopt a complete, systematic approach to information security management in the Bank.

2. The functioning of the cyber defense system is based on the following principles:

- ✓ proportionality and adequacy of the implemented cyber defense measures to real and potential cyber threats;
- ✓ prioritization of preventive measures;
- ✓ minimization of cyber risks in the bank's activities;
- ✓ compliance with the requirements of the NBU's regulations on information security and cyber defense, and the NBU's recommendations, including those that may be provided by the NBU based on the results of verification;
- ✓ the ongoing support of The Management Board of the Bank for cyber resilience through the organization of effective cyber risk management.

3. OBJECTIVES OF INFORMATION SECURITY

Principles arising out of the Information Security Management System, realized by the Bank, should ensure achievement of the following objectives of information security:

✓ **Compliance with the law.** Processing of the information, in particular organization of its protection, should comply with the applicable laws of Ukraine.

✓ **Accessibility of information.** Information and facilities for its processing are accessible for the authorized persons. The Bank ensures the acceptable level of information accessibility, taking into account the requirements of the law and business operations

✓ **Confidentiality of information.** Information is accessible exclusively for the persons and processes with corresponding access rights. In particular, these rights arise out of ownership of the information (information of Customers/Counterparts), as well as obligations and tasks fulfilled for the benefit ofthe Bank.

✓ **Information integrity.** The Bank takes organizational and technical measures to ensure protection of accuracy and integrity of information, as well as correct operation of the information processing equipment. In particular, information is protected from unauthorized changes.

✓ **Observability.** Provision for the possibility of identification of users and processes, as well as recording of actions of users and processes with respect to this information for the purpose of prevention and/or investigation of violations of the Information Security Policy of the Party 1.

✓ **Application of principles of protected processing of information.** Processing of information and exploitation of information processing facilities is carried out in accordance with the defined principles . Principles applicable to external business entities are based on the agreements concluded with ~~the Party 1~~ the Bank.

✓ **Supervision over information security.** The Bank controls the compliance of information processing methods of the Party 2 with the information security requirements. In case of the established noncompliance, the required corrective measures shall be taken promptly.

✓ **Adequate protection of information and information processing facilities based on the level of risk.** Selection of protection facilities is carried out in accordance with management of information risks in the Bank. Such approach ensures efficiency of information processes.

✓ **Adequate optimization of protection facilities based on the current needs of the**Bank . By means of risk management, audit, review and measurement of efficiency, the Bank establishes whether organizational and technical protection facilities are optimally compliant with the requirements of security and business operations of the Party 1.

✓ **Provision of quick and efficient response to violations of information security.** The Bankpromptly responds to any indications of violations of the Information Security Policy, what allows minimizing of potential adverse effects of the accident and taking urgent corrective measures.

5.MAIN PRINCIPLES OF INFORMATION SECURITY MEASURES

Organization of information security in the Bank is based on the following fundamental principles:

✓ **Principle of minimal authorities:** access of employees of the Bank and users of information systems to the information resources of the computer network of the Bank should be organized in a way that grants only those authorities that are required for specific work assignments.

✓ **Principle of required knowledge:** every employee of the Bank or any person involved into cooperation with the Bank has access only to the data about information resources and facilities for their processing and protection that is required for fulfilment of assigned tasks and obligations. Third parties have access only to the information classified as public (open) by the Bank.

✓ **Principle of distribution of duties:** fulfilment of tasks that are critically important in the context of security of financial and information resources of theBank , ICT and bank services shall be organized in a way that requires involvement of more than one person (two-man rule).

✓ **Principle of authorization of actions:** actions of employees of the Bank that are not explicitly allowed by the law, regulatory documents of the National Bank of Ukraine, internal administrative or regulatory documents are prohibited.

✓ **Principle of legitimacy:** ISMS takes into account the requirements of the applicable laws of Ukraine, as well as international regulatory requirements in the sphere of information security.

✓ **Principle of consistency and integrity:** objectives and tasks of the Information Security Policy correspond to the strategic goals and business objectives of theBank, and information security management is an integral part of the management process.

✓ **Principle of adequacy and efficiency:** facilities for protection of information resources are introduced in accordance with their criticality level, i.e. categories of classification and level of risk of a certain information resource based on the principles of assessment of the risk taken by theBank.

✓ **Principle of practicability:** facilities for protection of information resources should be practical and should support the balance between the functional capability and safety of information systems.

✓ **Principle of continuity:** information security is an ongoing process of prevention of threats/cyber threats and management of risks typical for the field of activity of theBank.

✓ **Principle of responsibility:** executive management of the Bank of all levels, employees of the Bank and other persons involved into cooperation with the Bank that have access to information resources of the Bank should follow the requirements of internal documents of the Bank in the sphere of information security and bear personal responsibility for their fulfilment.

✓ **Principle of ongoing improvement:** the Information Security Management System implemented by the Bankhas mechanisms and indicators for measurement and control of efficiency of the management system and facilities for rational planning introduced by the Bank and realization of actions aimed at improvement.

✓ **Principle of multi-level protection:** organization of information security of the Bank stipulates the development of the following series of consecutive levels of protection of information resources and employees of the Bank from potential threats/cyber threats:

- organizational and legal level that defines legal and regulatory requirements and obligations of employees, users of information resources and counterparts of the Bank1 with respect to information security;
- physical level of protection that prevents unauthorized physical access, damage or trespass on the office premises with a purpose of authorized access to information;
- level of the application program software responsible for interaction with users of information resources;
- level of the database management system responsible for data storing and processing;
- level of the operational system responsible for safe and reliable servicing of the application program software and database management systems;
- network level responsible for interaction of nodes of the information system.

✓ **Principle of complexity and systematicity:** information security of the Bank is organized in an integrated manner with due account for all aspects of information security, in particular:

- security strategy and objectives;
- management of information resources and data carriers;
- safety of human resources,
- management of physical safety and safety of the environment,
- safety of relations with the Providers,
- safety of internal and external communication processes,
- management of compliance with legal, regulatory and contractual requirements,
- management of incidents related to information security,
- management of business continuance,
- safety in processes of projecting, search, development, implementation and support of IT systems,
- safety in processes of IT systems operation.

Systematic approach of the Bank to the information security management means, in particular, ensuring coordination of processes and actions in the sphere of security:

✓ with conditions of environment, where the Bankfunctions,
✓ with the strategy and business objectives of theBank ,
✓ with results of assessment of risks and possibilities,
✓ with results of assessment of efficiency of the management system and introduction of protection facilities,
✓ with all aspects of administration of operating activity and information technologies of theBank.

6. 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 that cannot be disabled and the information cannot be processed without its use;
- availability of a built-in mechanisms for proper protection of information during its transfer between different subsystems in which information is being processed;
- For automated systems operating in client-server mode, users should only access the database through additional software that authenticates and authorizes persons that are permited to use this database;
- application of strong authentication of the payment service user;
- availability of a built-in mechanisms that provide unambiguous and certain identification of the user on each system access device, in each module or system element to which the user has access, as well as during implementation of any operations in the system;
- ensuring the possibility of automatic locking of the account in the system after exceeding the number of allowed unsuccessful attempts to enter a password on any system access device ensuring continuous technological control over data integrity and imposing/verifying a digital signature on all payment bank documents at each stage of the technological cycle of their processing; ensuring encryption of electronic banking documents containing confidential information when transmitted on external media or through appropriate communication channels on-line with appropriate confirmation of their receipt to ensure mandatory registration of all access attempts, all operations and other actions in the system, as well as recording them in an automated system, in an electronic register protected from modification, with constant control of its completeness and integrity.

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

8. The Bank uses standards, documents, and guidelines from the Open Web Application Security Project (OWASP) to develop secure applications.

9. The bank maintains a high level of security of information that is processed, stored and transmitted using cloud storage technologies.

10. The Bank has the principle of granting a minimum level of authority when providing access to the Bank's information systems (including access of privileged users).

11. 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 process of managing the continuity of the Bank's activities, measures to restore information systems after failures.

12. To reduce the risks of information security incidents occurrence, the Bank takes 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 determine the principles of ensuring security (in particular, this Policy) and the obligation of employees to get acquainted with them and comply with the requirements of these documents;
- providing trainings and workshops for employees in the field of information security;
- conducting internal campaigns and events (activities), in particular after a serious security incident occurrence and in case of detection of information concerning new methods of attacks on Banks and their Customers;
- conducting security tests and audits (including sociotechnical tests), testing the Bank's business continuity plans and discussing their results with the responsible persons of the relevant organizational units.

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

14. Each employee or person cooperating with the Bank is obliged to contribute to the activities to achieve and maintain an appropriate level of information security in the Bank to the extent pursuant to his official duties and conferred powers.

15. All employees of the Bank sign a non-disclosure obligation concerning information with limited access, including bank secrecy and personal data, upon employment. Employees of the Bank are obliged not to disclose and not to use for their own benefit or for third parties information with limited access, which became known to them in the performance of their official duties.