Евразийский Банк

Approved
by the Board of Directors of
Eurasian Bank JSC
Minutes No. 60
dated 12 July 2023

*for general use*

# POLICY
# THE INFORMATIONAL SECURITY

The Informational Security Policy (hereinafter referred to as the Policy) was developed in accordance with Resolution No. 48 of the Management Board of the National Bank of the Republic of Kazakhstan dated 27 March 2018 "On Approval of the Requirements for Ensuring Informational Security of Banks and Organizations Engaged in Certain Types of Banking Operations" (hereinafter referred to as the Resolution No. 48), the Resolution of the Government of the Republic of Kazakhstan dated 20 December 2016 No. 832 "On Approval of Uniform Requirements in the Field of Information and Communication Technologies and Informational Security", ST RK ISO/IEC 27001-2015 "Informational technology. Methods and means of ensuring security. Informational security management systems. Requirements", ST RK ISO/IEC 27002-2015 "Informational technology. Methods and means of ensuring security. A set of rules on Informational Security Management Tools" and the internal normative documents (hereinafter referred to as the INDs) of Eurasian Bank JSC (hereinafter referred to as the Bank), including the Policy of Internal Normative Regulation.

## Section 1. GENERAL PROVISIONS

1. The Policy was designed to determine the basic principles and directions in the field of informational security (hereinafter - IS) and covers all business processes, informational systems (hereinafter - IS) and documents owned and used by the Bank.
2. This Policy determines:

1) goals, objectives and basic principles of building an informational security management system (hereinafter – the ISMS);
2) scope and participants of the ISMS;
3) Informational Security management requirements, including:

– requirements for access to created, stored and processed information in the Bank's informational systems, monitoring of information and access to it;
– requirements for monitoring informational security activities and measures to identify and analyze threats, counter attacks and investigate informational security incidents;
– requirements for the collection, consolidation and storage of information about informational security incidents;
– requirements for the analysis of information about informational security incidents;
– the responsibility of the Bank employees for providing informational security in the performance of their functional duties.

3. The Bank ensures the creation and operation of the ISMS, which is part of the Bank's general management system designed to manage the process of providing IS.
4. The purpose of the ISMS is to ensure the protection of the Bank's informational assets, allowing for a minimum level of potential damage to the Bank's business processes, minimizing damage from events that pose a threat to informational security.
5. The main objectives of the ISMS in the Bank are:

– categorization of informational assets by dividing them into critical and non-critical based on the maximum level of criticality of the information stored and processed in them;
– timely identification of potential informational security threats and vulnerabilities in the Bank's informational assets;
– regular assessment of IS risks based on identified potential IS threats and vulnerabilities of the Bank's informational assets;
– exclusion or minimization of identified risks;
– application of reasonable, cost-effective organizational and technical measures to ensure informational security;
– prevention of IS incidents or minimization of their consequences;
– identification of applicable requirements of current legislation and regulators in the field of informational security, achieving compliance with these requirements;
– establishing the responsibility of employees for ensuring informational security, training and raising their awareness of informational security;
– monitoring the effectiveness of ISMS processes.

6. The Policy uses the basic concepts provided for by the legislation of the Republic of Kazakhstan, including Resolution No. 48, as well as an electronic directory.

## Section 2. SPECIAL PROVISIONS

### Chapter 1. Areas of application of the ISMS

7. The specific organizational scope and boundaries of the informational security management system (hereinafter referred to as ISMS) established by the Bank include:

- all business processes of the Bank, including processes of information exchange with clients and counterparties of the Bank.

- all employees of the Bank, as well as employees of counterparties when performing work in the Bank's infrastructure or when processing information provided by the Bank.

- all the information that is collected, processed, and stored as a result of the Bank's business processes, including the information by which security responsibility has been delegated to a third party within the framework of information exchange with counterparties.

8. The specific scope and boundaries of the Informational Security Management System (ISMS) for information and communication technologies include all the Bank's informational assets necessary for the functioning of the Bank's business processes, including informational assets for which security responsibility has been transferred to a third party (such as hosting server capabilities in external data processing centers, using external data processing and/or storage services).

9. The physical areas of operation and boundaries of the ISMS defined by the Bank include the administrative premises of the Bank and/or its branches (outlets) and other premises used by it (them) for various purposes, with equipment placed in them, or the adjacent territory (if available and/or within the established area of responsibility of the Bank).

10. The Policy is revised annually to analyze and update the information contained in them.

### Chapter 2. Principles for constructing the ISMS

11. The ISMS construction in the Bank and its functioning must comply with the following fundamental principles:

- legality - all measures taken to ensure informational security are conducted in compliance with the existing legislation of the Republic of Kazakhstan and the Bank's INDs, using all legally permissible methods to detect, prevent, localize, and neutralize any negative impact on the Bank's informational protection objects.

- business-orientedness - informational security is seen as a process of supporting business processes in the Bank. Any measures to ensure Informational Security should not entail serious obstacles to the Bank activities;

– continuity – the use of informational security management systems, the implementation of any measures to ensure the informational security of the Bank should be carried out without interrupting or stopping the current business processes of the Bank;

– complexity – ensuring the security of informational resources throughout their entire life cycle, at all technological stages of their use and in all modes of operation;

- validity and economic feasibility - the possibilities and means of protection used must be implemented at the appropriate level of scientific and technological development, justified from the point of view of the specified level of security, and must correspond to the requirements and norms imposed.

– priority – categorization (ranking) of all information resources of the Bank according to the degree of criticality based on the maximum level of criticality of the information stored and processed in them, as well as potential threats to informational security;

- essential knowledge and the lowest level of privileges - the user is granted the minimum level of privileges and access only to the data that is necessary for performing their functional responsibilities within their authority.

- specialization - the operation of technical means and the implementation of Informational Security measures must be performed by professionally trained Bank employees.

- awareness and personal responsibility – managers at all levels and employees of the Bank should be aware of all informational security requirements and are personally responsible for meeting these requirements and compliance with established informational security measures.

– interaction and coordination – informational security measures are performed on the basis of the interconnection of the relevant structural subdivisions of the Bank, coordination of their efforts for achieving their goals, as well as establishing the required relations with external companies, professional associations and communities, government agencies, legal entities and individuals;

– confirmability – critical documentation and all records – documents confirming the fulfillment of the informational security requirements and the efficiency of the system of its organization should be created and stored with the possibility of prompt access and recovery.

## Chapter 3. Functions of participants of the ISMS

12. The main participants of the Bank's informational security management system are:
1) The Board of Directors;
2) The Management Board;
3) The Informational Security Committee (hereinafter referred to as the ACB);
4) the informational security subdivision;
5) the informational technology subdivision;
6) the security subdivision;
7) the HR subdivision;
8) the legal subdivision;
9) the compliance and internal control subdivision;
10) the internal audit subdivision;
11) the IT and informational security risk management subdivision.

13. The Board of Directors approves the list of protected information, including the information comprising official, commercial or other legally protected secrecy (hereinafter – the protected information), and the procedure for working with the protected information.

14. The Chairman of the Management Board performs strategic planning, coordination of activities of all the Bank subdivisions for the organization and maintenance of the appropriate level of informational security.

15. The Management Board of the Bank approves internal documents regulating the informational security management process, the procedure and frequency of revision of which is determined by the Instructions for Managing Internal Normative Documents.

16. The Bank establishes the ACB, which includes representatives of the informational security subdivision, the informational security risk management subdivision, the informational technology subdivision, as well as, if required, representatives of other subdivisions of the Bank. The Chairperson of the Management Board of the Bank or the Deputy Chairperson of the Management Board of the Bank, who oversees the activities of the informational security subdivision, is appointed as the Head of the ACB.

17. The ACB performs periodic monitoring of informational security activities and measures for identification and analysis of threats, counter-attacking and investigating informational security incidents at least once a year. The process of monitoring informational security activities, measures for identification and analysis of threats, as well as counter-attacking should include a report on the identification, analysis of threats and counter-attacking based on data provided by the informational security subdivision on the amount of threats identified, measures taken and incidents of informational security. Monitoring of informational security incident investigation activities includes an assessment of the consequences of incidents, indication of causes and action plans for preventing or reducing the impact of informational security incidents.

18. The head of the informational security subdivision ensures the development, implementation and improvement of documented standards and procedures in the field of informational security.

19. The informational security subdivision monitors informational security events and informational security incident management, which determines the list of informational security events subject to monitoring, sources of events, frequency, monitoring rules and their methods. The informational security subdivision that conducts monitoring has the right to introduce additional controls, partial or complete shutdown of the business process in the event of an informational security incident.

20. The informational security subdivision ensures timely analysis of information about informational security incidents, which should include disclosure of the circumstances of the event in which the implementation of the informational security incident became possible, interaction with the informational security risk management subdivision, if required, the formation of recommendations for the implementation of protective measures.

21. The informational technology subdivision ensures compliance with the established requirements for the continuity of the information infrastructure, confidentiality, integrity and availability of data of the

Bank's informational systems (including backup and (or) archiving and backup of information)) in accordance with the Bank's INDs, and also ensures compliance with the requirements of the informational security when selecting, implementing, developing and testing IS.

22. The informational security risk management subdivision is responsible for categorizing informational assets by dividing them into critical and non-critical based on the maximum level of criticality of the information stored and processed in them.

23. The security subdivision implements physical and technical security measures, including organizing access and on-site security, as well as conducting preventive measures aimed at minimizing the risks of informational security threats when hiring and dismissing Bank employees.

24. The HR subdivision ensures that employees of the Bank, as well as persons involved in the work under the service agreement, interns, practicing young professionals, sign obligations on non-disclosure of confidential information, and also participates in the organization of the process of raising awareness of the Bank employees in the field of informational security.

25. The legal subdivision conducts the legal expertise of the INDs and internal documents of the Bank on the issues of informational security, in accordance with the Instructions for Managing Internal Normative Documents.

26. The compliance control subdivision, together with the legal subdivision of the Bank, determines the types of information to be included in the list of protected information.

27. The internal audit subdivision evaluates the state of the Bank's ISMS during audits.

28. The Management Board of the Bank coordinates the activities of all subdivisions of the Bank to organize and maintain an appropriate level of informational security and is responsible for the implementation of the Policy provisions.

29. The Management Board of the Bank, together with the informational technology subdivision and the informational security subdivision, shall be obliged to actively implement a set of measures to maintain the IS and electronic informational resources (hereinafter referred to as the EIR) of the Bank by giving clear instructions, demonstrated obligations, clear statements of objectives and awareness of employees about their duties to ensure informational security.

30. The Informational Security coordination should include the interconnection and cooperation of users, administrators, application software developers and qualified specialists in such areas as human resources, informational technology and risk management.

This activity should:

1) ensure compliance with the implementation of informational security measures;

2) determine measures to ensure informational security in case of its non-compliance with the Policy;

3) approve the methodology and processes for ensuring informational security, for example, risk assessment, classification of information;

4) identify all changes in informational security threats and the degree of vulnerability of information and information processing tools to informational security threats;

5) assess the adequacy of decisions taken and coordinate the implementation of informational security control measures;

6) increase the level of training of users in the field of informational security and awareness about it;

7) evaluate the information obtained from monitoring and viewing IS incidents and recommend appropriate measures in response to identified IS incidents.

31. The Management Board of the Bank should ensure clear management and visible support for initiatives to improve the ISMS.

32. The Management Board of the Bank should ensure coordination of control measures over the informational security and provide resources to ensure informational security.

33. The Management Board of the Bank should approve the distribution of specific roles and responsibilities for informational security.

34. The Management Board of the Bank undertakes to ensure that the IS complies with the current requirements related to informational security, legislative requirements, including requirements for compliance with intellectual property rights.

35. Requirements for training and awareness of informational security issues:

1) users, employees of the informational technology subdivision, and counter-parties should read the Policy;

2) the person responsible for the Bank's informational security should conduct an initial briefing on informational security;

3) employees of the informational technology subdivision that ensure the functioning of the IS and EIR should undergo regular instruction on compliance with the requirements of the informational security;

4) responsible for informational security, as necessary, but at least one (1) time in three (3) years, takes advanced training courses in informational security;

36. The Bank provides advanced training for employees of informational security, informational security risk management and internal audit subdivisions by conducting external training (attending courses, seminars – at least one (1) time in three (3) years for each employee).

37. In order to ensure compliance with the requirements contained in the Policy, it is required to ensure that third parties comply with it. Therefore, in appropriate cases, all contracts concluded by third-party legal entities and individuals should contain a requirement to comply with the requirements of the Informational Security Policy and IS provision. All activities involving the contact of counterparties with the data contained in the Bank's ISs and EIR must be conducted in accordance with the regulatory requirements set out in the Policy. This requirement shall apply to all counterparties.

## Chapter 4. informational Security management requirements

38. The main measures to protect the confidentiality, integrity and availability of the Bank's informational assets are:

– network security management;
– vulnerability and security policy management;
– end device security management;
– identity and access management;
– Informational Security incident management;
– management of cryptographic means of protection;
– management of anti-virus protection tools;
– ensuring the physical security of informational assets;
– ensuring security when interacting with counterparties;
– training and awareness-raising of personnel in informational security issues;
– ensuring the security of Internet resources.

39. Regarding the organizational measures of the Bank's Informational Security, the following is required:

1) creation and functioning of the informational security subdivision responsible for the management of informational security and the development of measures to ensure informational security;

2) compliance of the number of employees and employees responsible for informational security and their qualifications with the level of tasks assigned to them;

3) approval and regular review of the current documentation regarding the informational security (a four-level system of documented rules, procedures, practices or guidelines), as well as reading them by the employees of the Bank in terms of their responsibilities, at least once a year.

4) planning of measures to ensure informational security based on an assessment of informational security risks.

40. The objectives for ensuring the security of informational resources are solved by the following methods:

– minimization of data and privileges based on the principles of minimum sufficiency;
– separation of powers and duplication of control;
– establishment of a unified procedure for storing and processing confidential information;
– maintaining the operability of informational systems related to informational security;
– response of responsible persons to the violation of the Informational Security regime;
– obtaining from employees of the Bank and the counterparties an obligation to comply with the requirements of the informational security and to ensure the safety of confidential information;
– conducting periodic training and advanced training of the Bank employees in the field of informational security.

41. The Bank develops internal procedures for the creation, collection, storage and processing of information in the Bank ISs. The Bank monitors the processes of creation, storage and processing of information and access to it using IP mechanisms and technical means of ensuring security. Access to the information created, stored and processed in the Bank ISs is provided to employees in accordance with their functional responsibilities in accordance with the principle of the lowest level of privileges.

42. The list of informational security events subject to monitoring, sources of events, frequency, monitoring rules and their methods are reviewed by the informational security subdivision at least once a year, taking into account available statistics and monitoring effectiveness.

43. The procedure for managing informational security incidents is determined by the relevant Bank’s IND and contains provisions for consolidating, systematizing and storing information about informational security incidents, procedures for classifying an informational security event as an informational security incident, subsequent analysis of an informational security incident and informing about an informational security incident.

44. The process of consolidating, systematizing and storing information about IS incidents should ensure the integrity, accessibility and confidentiality, as well as the completeness of incident data sufficient to analyze the incident, conduct internal audits and generate reports provided for by Resolution No. 48.

45. IS business owners are responsible for compliance with informational security requirements when creating, implementing, modifying, providing products and services to customers, and also form and maintain the relevance of IS access matrices.

46. The heads of the Bank’s structural subdivisions ensure that employees read the Bank’s IND, which contains requirements for informational security, and are also responsible for ensuring compliance with informational security requirements in subordinate subdivisions, the introduction of protection measures in the development of new products, services, business applications, business processes and technologies.

## Section 3. FINAL PROVISIONS

47. All employees of the Bank are responsible for non-fulfillment/improper fulfillment of the requirements of the Policy, as well as for ensuring informational security in the performance of their functional duties.

48. Control over the fulfillment of the requirements established by the Policy is assigned to the ACB.

49. The Policy comes into force on the next business day after it is entered into the INDs Database and is generally binding on the application and management of all employees of the Bank, as well as brought to the attention of third parties with access to the Bank’s informational assets.

50. Issues not regulated by the Policy are resolved in accordance with the legislation of the Republic of Kazakhstan and the Bank’s INDs.

**Director of IT Security Service**
**Rustamov E. A.**

## LIST OF CHANGES AND ADDITIONS

| s.i. No. | Minutes No. | Minutes date | Effective date | Initiator of changes |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |