Евразийский Банк

Approved by
the Board of Directors of
Eurasian Bank JSC
Minutes No. 15
dated 26 February 2019

for internal use

THE INFORMATIONAL SECURITY POLICY

POLICY

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 (hereinafter referred to as the RoK) 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) and the internal normative documents (hereinafter – 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 and covers all business processes, informational systems and documents owned and used by the Bank.

2. The purpose of informational security management activities in the Bank is to ensure the protection of the Bank's informational assets and minimize damage from events that pose a threat to informational security.

3. The objectives of informational security management activities 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 threats to informational security and vulnerabilities in the Bank's informational assets;

– exclusion or minimization of identified threats;

– prevention of informational security incidents or minimization of their consequences.

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

– network security management;

– vulnerabilities and security policies 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 at interaction with counterparties;

– training and awareness-raising of personnel in informational security issues;

– ensuring the security of Internet resources.

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

Section 2. SPECIAL PROVISIONS

5-1. The Bank ensures the creation and operation of the informational security management system, which is part of the Bank's general management system designed to manage the informational security process.

5-2. The informational security management system ensures the protection of the Bank's informational assets, allowing for a minimum level of potential damage to the Bank's business processes.

6. The construction of the informational security management system in the Bank and its functioning should be performed in accordance with the following basic principles:

– legality – any actions taken to ensure informational security are performed on the basis of the current legislation of the Republic of Kazakhstan and the Bank's INDs, using all methods permitted by the laws of identification, prevention, localization and suppression of negative impacts on the Bank's informational protection facilities;

– focus on business - informational security is considered as a process of supporting business processes in the Bank. Any measures to ensure informational security should not cause serious obstacles to the Bank's activities;

– continuity – the use of informational security management systems, the implementation of any measures to ensure the informational security of the Bank should be performed 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 development of science and technology, justified from the point of view of a given level of security and must comply with the requirements and norms;

– priority – categorization (ranking) of all informational 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;

– the required knowledge and the lowest level of privileges – the user receives the minimum level of privileges and access only to those data that are required for him to perform functional duties within his/her authority;

– specialization – the operation of technical means and the implementation of informational security measures should be performed by professionally trained employees of the Bank;

– 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 informational security requirements and the efficiency of its organization's system should be created and stored with the possibility of prompt access and recovery.

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

7-1. The 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 ACB);
4) the informational security subdivision;
5) the informational technology subdivision;
6) the security subdivision;
7) the HR subdivision;
8) the banking and corporate issue legal support subdivision;
9) the compliance and internal control subdivision;
10) the internal audit subdivision;
11) the IT and informational security risk management subdivision.

7-2. 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.

7-3. The Management Board 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.

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

9. 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 countering-attacking should include a report on identification, analysis of threats

and countering-attacks based on data provided by the informational security subdivision on the amount of threats identified, measures taken and informational security incidents that have occurred. 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.

10. 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.

11. 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 efficiency.

12. The procedure for managing informational security incidents is determined by the relevant INDs of the Bank and contains provisions for the consolidation, systematization and storage of information about informational security incidents, procedures for attributing an informational security event to informational security incidents, subsequent analysis of an informational security incident and informing about an informational security incident.

13. The process of consolidating, systematizing and storing information about informational security incidents should ensure the integrity, accessibility and confidentiality, as well as the completeness of incident data sufficient for analyzing the incident, conducting internal audits and generating the reports stipulated by the Resolution No. 48.

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

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

16. 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 it becomes possible to implement an informational security incident, the interaction with the informational security risk management subdivision, if required, the recommendations for the implementation of protective measures.

17. The informational technology subdivision ensures compliance with the established requirements for the continuity of the informational 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 informational security requirements at selection, implementation, development and testing of informational systems.

18. 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.

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

20. The HR subdivision ensures that the Bank employees, as well as persons involved in the work under the service agreement, trainees, interns, 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.

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

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

23. The internal audit subdivision evaluates the state of the Bank's informational security management system during audits.

24. Business owners of informational systems or subsystems are responsible for compliance with informational security requirements at creating, implementing, modifying, providing products and services to customers, and also form and maintain the relevance of access matrices to informational systems.

25. The heads of the Bank's structural subdivisions ensure that the employees are familiar with the Bank's INDs containing informational security requirements, and are also responsible for ensuring that subordinate subdivisions comply with informational security requirements and implement security measures in the development of new products, services, business applications, business processes and technologies.

Section 3. FINAL PROVISIONS

26. 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.

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

28. The Policy comes into force on the next business day after it is entered into the INDs DB, and is generally binding on the application and guidance by all employees of the Bank, and is also brought to the attention of third parties with access to the Bank's informational assets.

29. Issues not regulated by the Policy are resolved in accordance with the legislation of the Republic of Kazakhstan and the 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.	No. 42	11.06.2019	14.06.2019	IT Security Service
2.				