Appendix
to Resolution of the Board of Directors
No. 0219/1 dated 19.02.2024

Approved
by the Minutes of the Management Board
No. 0129/8 dated 29.01.2024

Information Security Policy
Bank CenterCredit JSC

Content

1. General Provisions 1

2. Objectives, Tasks and Basic Principles of Building an Information Security Management System 2

3. Scope of the Information Security Management System 3

4. Requirements for access to information created, stored and processed in the Bank information systems and monitoring of information and access to it 3

5. Requirements for monitoring information security activities and measures to identify and analyze threats and counteract attacks and investigate information security incidents; 3

6. Requirements for collection, consolidation and storage of information on information security incidents 4

7. Requirements for analysis of information on information security incidents 4

8. Responsibility of Bank employees for ensuring information security in performance of their assigned functional duties 4

9. Ensuring information security in the Subsidiaries of the Bank 6

10. Requirements for competencies of managers and employees responsible for ensuring information security 7

11. Final Provisions 7

1. General Provisions

1. This Information Security Policy (hereinafter referred to as the Policy) is a fundamental document of the information security management system of JSC Bank CenterCredit (hereinafter referred to as the Bank), defining goals, objectives and scope of the Bank's information security management system (hereinafter referred to as the ISMS).

2. The ISMS ensures protection of the Bank's information assets, allowing for a minimum level of potential damage to the Bank's business processes.

3. The Policy has been developed in accordance with the legislation of the Republic of Kazakhstan, including regulatory legal acts governing requirements for ensuring the information security of second-tier banks, as well as requirements of international standards in the field of information security.

4. Requirements for the processes of the Bank's information security management system, set out in this Policy, are described in detail in the Bank's internal regulatory documents developed in accordance with Chapter 9 “Requirements for the Information Security Management System Processes” of the Resolution of the Board of the National Bank of the Republic of Kazakhstan dated March 27, 2018 No. 48 “On approval of the Requirements for Ensuring Information Security of

Banks, Branches of Non-Resident Banks of the Republic of Kazakhstan and Organizations Carrying Out Certain Types of Banking Operations, the Rules and Deadlines for Providing Information on Information Security Incidents, Including Information on Violations, Failures in Information Systems".

2. Objectives, Tasks and Basic Principles of Building an Information Security Management System

5. The Bank's top manager ensures creation, operation and improvement of the ISMS, which is part of the overall management system of the bank, the organization, designed to manage the process of ensuring information security

6. Purpose of the ISMS is to improve efficiency of information security processes, ensure required level of confidentiality, integrity and availability of critical information assets, and, as a result, reduce information security risks and associated damage.

7. The tasks of the ISMS include:

1) categorization of information assets;

2) organization of access to information assets;

3) ensuring security of the information infrastructure;

4) monitoring information security activities and measures to identify and analyze threats and vulnerabilities, counteract attacks and investigate information security incidents;

5) analysis of data on information security incidents, including information on violations, failures in information systems;

6) definition of the procedure for managing cryptographic information protection tools;

7) ensuring information security when third parties access information assets;

8) conducting internal audits of the state of information security.

8. The ISMS is built and operated in accordance with the following key principles:

1) legality – any actions taken to ensure information security are carried out on the basis of current legislation, using all methods of detection, prevention, localization and suppression of negative impacts on the Bank's information assets permitted by law;

2) business orientation – information security is viewed as a process of supporting the core business, any measures to ensure information security should not entail serious obstacles to doing business;

3) comprehensiveness – ensuring security of information assets throughout their entire life cycle, at all technological stages of their use and in all modes of operation;

4) reasonableness and economic feasibility – capabilities 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 the specified level of security and must comply with the imposed requirements and standards. In all cases, the cost of measures and technological solutions to ensure information security must not exceed the cost of information assets being protected;

5) adaptability – defining and applying methods and means of protecting information assets in accordance with their criticality;

6) necessary knowledge and the lowest level of privileges – user receives minimum level of privileges and access only to those information assets that are necessary for performance of activities within the scope of his authority;

7) specialization – implementation of measures and operation of technological solutions to ensure information security must be carried out by professionally trained specialists;

8) awareness and personal responsibility – managers at all levels and performers must be aware of all information security requirements and bear personal responsibility for the fulfillment of these requirements and compliance with the established information security measures;

9) interaction and coordination – information security measures are implemented on the basis of the relationship between relevant structural divisions of the Bank, coordination of their efforts to achieve the set goals, as well as establishment of the necessary connections with external organizations, professional associations and communities, government agencies, legal entities and individuals;

10) Confirmability – evidence confirming compliance with information security requirements and effectiveness of the ISMS must be created and stored with the possibility of prompt access and recovery.

3. Scope of the Information Security Management System

9. The scope of the ISMS is the Bank's core business processes directly focused on providing services to clients, representing value to clients and ensuring profit, defined by the business process classification procedure, as well as processes that ensure operation of the Bank's Certification Authority.

10. Objects of protection are critical information assets necessary for functioning of the core business processes, as well as information assets that ensure functioning of the Certification Authority, which may include:

1) individual information processing devices;
2) information carriers;
3) peripheral computer equipment;
4) servers;
5) databases;
6) network equipment;
7) telephony equipment;
8) physical communication channels;
9) virtual communication channels;
10) virtualization systems;
11) operating systems
12) hardware software;
13) application software;
14) telephony software;
15) cryptographic information protection tools.

4. Requirements for access to information created, stored and processed in the Bank information systems and monitoring of information and access to it

11. Access to information and the Bank's information systems is provided to employees in the amount necessary to perform their functional duties.

12. Access to the Bank's critical information systems is provided by forming and implementing roles to ensure that the access rights of information system users correspond to their functional duties.

13. Access to the Bank's information assets by persons who are not employees of the Bank (hereinafter referred to as third parties) is provided for the period and in the amount necessary to perform work on the basis of the relevant agreement/contract, which includes conditions for compliance with information security requirements, except for cases stipulated by the legislation of the Republic of Kazakhstan. Agreements/contracts concluded with third parties contain provisions on confidentiality, conditions on compensation for damages arising from a breach of information security, as well as failures in the operation of information systems and breaches of their security caused by the actions or inactions of third parties.

5. Requirements for monitoring information security activities and measures to identify and analyze threats and counteract attacks and investigate information security incidents;

14. The Bank ensures creation of a structural unit for responding to information security incidents – the information security incident response service.

15. The Bank ensures proper monitoring of information security activities and measures to identify and analyze threats, counter attacks and investigate information security incidents.

6. Requirements for collection, consolidation and storage of data on information security incidents

16. The Bank shall ensure availability of documents, information and facts confirming implementation of the procedure for responding to information security incidents, as well as recording, storage, consolidation, systematization, integrity and safety of information on information security incidents, including information on violations, failures in information systems, the results of an internal investigation of information security incidents and investigation materials on paper and (or) in electronic form.

7. Requirements for analysis of data on information security incidents

17. The Bank shall ensure:

1) analysis of identified information security incidents and the damage caused by them for consideration by the Bank's collegial body, to assess information security risks, adjust methods and means of ensuring information security, change the Bank's business processes;

2) assessment of effectiveness to adjust the process of responding to information security incidents using metrics of the process of responding to information security incidents;

3) revision of metrics of the process of responding to information security incidents considering result of the assessment of effectiveness of the process of responding to information security incidents;

4) revision of the list of information security events subject to monitoring, event sources, frequency, procedure and methods for monitoring information security events.

8. Responsibility of Bank employees for ensuring information security in performance of their assigned functional duties

18. Participants of the Bank ISMS are:

1) Board of Directors;
2) Management Board;
3) Peer body authorized to make decisions on information security tasks (hereinafter referred to as the APB);
4) Information security unit;
5) Information technology unit;
6) Security unit;
7) HR unit;
8) Legal unit;
9) Compliance control unit;
10) Internal audit unit;
11) IT and information security risk management unit;
12) Business owners of information systems and subsystems;
13) Heads of structural units;
14) Employees of structural units.

19. The Board of Directors approves the information security policy and the list of protected information, including information on data constituting an official, commercial or other secret protected by law, and the procedure for working with protected information. When forming the budget, the Board of Directors considers the resource requirements for ensuring the Bank's information security.

20. The Management Board approves internal regulations governing the information security management process, training program and the plan for testing employees on their knowledge of requirements of internal regulations on information security, the procedure and frequency of revision of which are determined by the Bank's internal documents.

21. The Management Board ensures the existence of APB on making decisions on information security issues, which acts within the powers granted by the Management Board.

22. The Information Security Unit performs following functions to ensure confidentiality, integrity and availability of the Bank's information:

1) arranges information security management system, coordinates and controls activities of the Bank's units to ensure information security and measures to identify and analyze threats, counter attacks and investigate information security incidents;

2) develops the Bank's information security policy;

3) provides methodological support for the process of ensuring the Bank's information security;

4) selects, implements and applies methods, means and mechanisms for managing, ensuring and controlling the Bank's information security, within its powers;

5) collects, consolidates, stores and processes information on information security incidents;

6) analyzes information on information security incidents;

7) prepares proposals for the Information Security Committee to make a decision on information security issues;

8) ensures implementation, proper functioning of software and hardware that automate the process of ensuring the Bank's information security, as well as providing access to them;

9) defines information security requirements for use of privileged accounts;

10) ensures that events are held to raise awareness of the Bank's employees in the field of information security;

11) monitors the state of the Bank's information security management system;

12) informs the Bank's management about state of the Bank's information security management system;

13) assesses information security risks;

14) develops measures to process information security risks and provides reports on their implementation to the IT and information security risk management unit;

15) prepares and provides reports on implementation of significant information security risks to the IT and information security risk management unit, as well as on the elimination of their consequences;

16) develops an action plan for implementation of the Bank's strategy in terms of ensuring information security, which discloses, but is not limited to, the following:

- determining resource needs, including determining the budget related to implementation of measures aimed at managing information security risks;
- description of required information security measures, indicating deadlines and persons responsible for their implementation.

23. The Information Technology Department performs the following functions:

1) develops and maintains the relevance of the Bank's information infrastructure diagram;

2) ensures that users have access to the Bank's information assets, except for specialized information assets, access to which is provided by IT managers of information systems who are not part of the Information Technology Department;

3) ensures the formation of standard settings and configuration of the Bank's system and application software taking into account information security requirements;

4) ensures compliance with established requirements for continuity of the information infrastructure, confidentiality, integrity and availability of data of the Bank's information systems (including backup and (or) archiving and backup copying of information) in accordance with the Bank's internal documents;

5) ensures compliance with information security requirements when selecting, implementing, developing and testing information systems.

24. The Security Department performs the following functions:

1) implements physical and technical security measures in the Bank, including organizing access control and internal facility regime;

2) carries out preventive measures aimed at minimizing the risks of information security threats when hiring and firing Bank employees.

25. The HR Department performs the following functions:

1) ensures that Bank employees, as well as persons engaged to work under a service agreement, interns, and trainees sign obligations to non-disclosure of confidential information;

2) participates in organizing the process of raising awareness of the Bank's employees in the field of information security;

3) notifies authorized body of the appointment and dismissal of employees of the information security department.

26. The legal department carries out a legal examination of the Bank's internal regulatory documents on information security issues.

27. The Compliance Control Department, together with the Legal Department, determines types of information to be included in the list of protected information provided for in paragraph 19 of this Policy.

28. The Internal Audit Department assesses the state of the Bank's information security management system in accordance with the Bank's internal regulatory documents governing the organization of the Bank's internal audit system.

29. The Information Technology and Information Security Risk Management Department performs the functions stipulated by the Rules for the Formation of a Risk Management and Internal Control System for Second-Tier Banks, approved by Resolution of the Board of the National Bank of the Republic of Kazakhstan dated November 12, 2019 No. 188 “On Approval of the Rules for the Formation of a Risk Management and Internal Control System for Second-Tier Banks, Branches of Non-Resident Banks of the Republic of Kazakhstan”.

30. Business owners of information systems and subsystems;

1) are responsible for compliance with information security requirements when creating, implementing, modifying, operating information systems and providing products and services to clients and divisions of the Bank, as well as when integrating information systems with external information systems, including information systems of government agencies;

2) form and maintain the relevance of access matrices to information systems.

31. Heads of the Bank's structural divisions:

1) ensure that employees are familiar with the Bank's internal regulatory documents containing information security requirements;

2) are personally responsible for ensuring information security in the divisions they head;

3) ensure that confidentiality agreements are concluded and that information security conditions are included in agreements and contracts for the provision of services/performance of work in cases where a division of the Bank initiates the conclusion of such agreements and contracts.

32. Employees of the Bank's structural divisions:

1) are responsible for compliance with the information security requirements adopted by the Bank;

2) monitor compliance with information security requirements by third parties with whom they interact within the framework of their functional responsibilities, including by including such requirements in agreements with third parties;

3) notify their immediate supervisor and the information security department of all suspicious situations and violations when working with information assets.

33. Failure to comply with the procedure and rules for the use of information resources and the measures taken by the Bank to ensure information security when employees perform their assigned functional responsibilities entails liability in accordance with the current legislation of the Republic of Kazakhstan and the internal regulatory documents of the Bank.

9. Ensuring information security in the Subsidiaries of the Bank

34. In order to ensure supervision and build interaction between the information security department and the Subsidiaries of Bank CenterCredit JSC (hereinafter – SC) in terms of ensuring the necessary and sufficient level of information security in the SC of the Bank, the information security department performs the following functions to coordinate the activities of the SC:

1) determines requirements for ensuring information security;

2) agrees on internal regulatory documents in terms of information security;

3) recommends and coordinates implementation of organizational measures and software and hardware to ensure information security;

4) coordinates annual action plans and the SC budget in the field of information security;

5) provides consulting support in terms of developing the information security management system, as well as in matters of training and professional development of SC employees responsible for ensuring information security;

6) assists in passing external inspections and audits in the field of information security;

7) conducts information security checks, requests information, coordinates action plans to eliminate identified issues, requires their implementation;

8) participates in specialized SC committees (if any).

10. Requirements for competencies of managers and employees responsible for ensuring information security

35. Managers and employees responsible for ensuring information security have relevant competencies and experience in the field of information security.

36. Detailed requirements for qualifications of managers and employees responsible for ensuring information security are reflected in the relevant qualification requirements and job descriptions.

37. Managers and employees responsible for ensuring information security improve their qualifications in accordance with the requirements of the Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market dated September 21, 2020 No. 89.

11. Final Provisions

38. All issues not regulated by this Policy are resolved in accordance with the legislation of the Republic of Kazakhstan, internal regulations and decisions of the authorized bodies of the Bank, as well as the established practice of the Bank.

39. The Policy shall enter into force on the date of approval by the Board of Directors of the Bank and shall cease to be effective from the moment it is recognized as invalid by the Board of Directors of the Bank.

40. If, because of changes in the legislation of the Republic of Kazakhstan, individual provisions of this Policy conflict with the current legislation of the Republic of Kazakhstan, then until Policy is amended, the current legislation of the Republic of Kazakhstan and the Policy in the part that does not contradict the legislation of the Republic of Kazakhstan shall govern.

41. This Policy is revised at least once a year.