On Approval of the Requirements for the Use of Information and Communication Technologies and Information Security in Organizing the Activities of Credit Bureaus, Information Providers and Recipients of Credit Reports, and the Requirements of Credit Bureaus to Information Providers and Recipients of Credit Reports

Unofficial translation

Resolution of the Board of the National Bank of the Republic of Kazakhstan of September 27, 2018 No. 228. Registered with the Ministry of Justice of the Republic of Kazakhstan on November 6, 2018 No. 17702.

Unofficial translation

Footnote. The heading - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall be enacted ten calendar days after the date of its first official publication).

In accordance with the Law of the Republic of Kazakhstan dated July 6, 2004 "On credit bureaus and formation of credit records in the Republic of Kazakhstan", the Board of the National Bank of the Republic of Kazakhstan shall **DECIDE**:

1. That the following shall be approved:

1) Requirements for the application of information and communication technologies and information security when organizing the activities of credit bureaus, information providers and recipients of credit reports as per Annex 1 to this Resolution;

2) Requirements imposed by credit bureaus on information providers and recipients of credit reports pursuant to Annex 2 to this Resolution.

Footnote. Paragraph 1 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall come into effect upon expiration of ten calendar days after the day of its first official publication).

2. To recognize as invalid the regulatory legal acts of the Republic of Kazakhstan, as well as the structural elements of some regulatory legal acts of the Republic of Kazakhstan according to the list in accordance with the Annex 3 to this resolution.

3. In the procedure established by the legislation of the Republic of Kazakhstan, the Department of information threats and cyber protection (Perminov R.V.) shall ensure:

1) The state registration of this resolution in the Ministry of Justice of the Republic of Kazakhstan together with the Legal department (Sarsenova N.V.);

2) within ten calendar days from the date of the state registration of this resolution, to send it in the Kazakh and Russian languages to the Republican state enterprise on the basis of the right of economic management "Republican Center for Legal Information" for official

publication and inclusion into the Reference Control Bank of regulatory legal acts of the Republic of Kazakhstan;

3) the placement of this resolution on the official Internet resource of the National Bank of the Republic of Kazakhstan after its official publication;

4) within ten working days after the state registration of this resolution, to submit the information to the Legal department on implementation of the measures provided for by subparagraphs 2), 3) of this paragraph and paragraph 4 of this resolution.

4. The Directorate for protection of the rights of consumers of financial services and external communications (A.T. Terentiev) shall ensure, within ten calendar days after the state registration of this resolution, the submission of its copy for official publication in periodicals.

5. Deputy Chairman of the National Bank of the Republic of Kazakhstan Smolyakova O.A shall be entitled to control the execution of this resolution.

6. This resolution shall enter into force upon the expiry of ten calendar days after the day of its first official publication.

Chairman of the
National Bank *D. Akishev*

Annex 1
to the resolution of the Board of
the National Bank of the
Republic of Kazakhstan
dated September 27, 2018,
№ 228

Requirements for the application of information and communication technologies and ensuring information security when organizing the activities of credit bureaus, information providers and recipients of credit reports

Footnote. The title - as revised by Resolution of the Management Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall enter into force ten calendar days after the date of its first official publication).

Chapter 1. General provisions

1. These Requirements for the Application of Information and Communication Technologies and Information Security in organizing the Activities of Credit Bureaus, Information Providers and Recipients of Credit Reports have been developed in line with sub-paragraph 6) of Article 5 of the Law of the Republic of Kazakhstan “On Credit Bureaus and the Formation of Credit Histories in the Republic of Kazakhstan” and establish requirements for the use of information and communication technologies and ensuring information security when organising the activities of credit bureaus, banks, organisations

engaged in certain types of banking transactions, organisations engaged in microfinance activities, collection agencies and service companies, managing rights (claims) under bank loan agreements and (or) agreements on granting a microloan under an agreement on trust management of rights (claims) under bank loan agreements and (or) agreements on granting a microloan concluded with a bank, an organisation engaged in certain types of banking transactions, an organisation engaged in microfinance activities, a collection agency, a subsidiary of a bank acquiring doubtful and uncollectible assets of a parent bank, an organisation specialising in improving the quality of loan portfolios of second-tier banks, a legal entity - pledgee of rights of claim under a contract on granting a microloan when a microfinance organisation issues secured bonds or obtains loans, a special financial company established in line with the legislation of the Republic of Kazakhstan on project financing and securitisation under a securitisation transaction, by a person who repurchases mortgage loans of natural persons not related to entrepreneurial activity, one hundred percent of shares of which belong to the National Bank of the Republic of Kazakhstan, by a special fund for development of private entrepreneurship - under a bank loan agreement, under an agreement on granting a microloan concluded within the framework of a transaction on financing private entrepreneurship entities by means of conditional placement of funds in banks and organisations, engaged in certain types of banking transactions, microfinance organisations, by another person - in respect of a right (claim) under a bank loan agreement, under an agreement on granting a microloan to a natural person related to entrepreneurial activity, or under a bank loan agreement under a microloan agreement of a legal entity for which impairment indicators have been revealed in line with International Financial Reporting Standards, including at the time of acquisition or emergence (creation) of a right (claim) under a bank loan agreement, under a microloan agreement.

Footnote. Paragraph 1 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall become effective ten calendar days after the date of its first official publication).

2. The terms, specified by the Law on credit bureaus shall be used in the Requirements, as well as the following concepts:

1) information providers - information providers, specified in subparagraph 1) of paragraph 1 of article 18 of the Law on credit bureaus;

2) information asset - a set of data and an object of information and communications infrastructure, used to store it and (or) to process;

3) information and communication infrastructure (hereinafter - the information infrastructure) - a set of objects of the information infrastructure, designed to ensure the functioning of the technological environment in order to create electronic information resources and to provide access to them;

4) information security - the state of security of electronic information resources, information systems and ICT infrastructure from external and internal threats;

5) the risk of information security - the probability of occurrence of damages due to privacy violations and intentional violations of the integrity or availability of information assets of a credit bureau;

6) information security - a process aimed at the maintenance of the confidentiality, integrity and availability of information assets of a credit bureau;

7) an incident of information security - separately or serially occurring failures in the information infrastructure or its separate objects that threaten their proper functioning and (or) conditions for illegal obtaining, copying, distribution, modification, destruction, or blocking of electronic information resources of a credit bureau;

8) privileged account - an account in the information system with the privileges to create, delete and modify access rights of other accounts;

9) audit trail - a chronological sequence of records containing evidence of data change as a result of performing functions of an information system;

10) authentication - confirmation of authenticity of the subject or object of access to the information system by determining the compliance of the shown details of access;

11) business process - a set of interrelated activities or tasks designed to create a specific product or service for the external (customer) or internal (employee, a department of a credit bureau, other business process) consumer;

12) virtual environment - computational resources, or their logical association, abstracted from the hardware implementation, providing a logical isolation of computational processes from each other, performed on a single physical resource;

13) data processing center - a dedicated room, which houses servers and communication equipment of the information infrastructure of a credit bureau. The data processing center is divided into primary and backup ones;

14) a responsible person – an employee of the recipient of credit reports, having access to credit reports;

15) workstation - a personal computer used to access the information system of a credit bureau;

16) a business owner of the information system of a credit bureau - a department (employee) of a credit bureau, which is (are) the owner of the main business process that is automated by the information system of the credit bureau;

17) recipients of credit reports – the recipients of credit reports, specified in subparagraph 1) of part one of paragraph 1 of article 20 of the Law on credit bureaus;

18) access - the ability to use the information assets;

19) an operator – an employee responsible for the correctness of data input in the information system of the credit bureau;

20) a backup copy – a copy of the data on media, intended to restore the data in the original or a new place of their location if necessary;

21) technical safety – a process of providing security of a credit bureau with the use of technical means (fire and intruder alarm systems, monitoring and access control, CCTV, fire fighting, temperature and humidity control in the data processing center);

22) technological account - an account in the information system, intended for authentication between the information systems;

23) corrective measure - a set of organizational and technical measures, aimed at correcting the existing problem in the process of information security or the consequences of its violation;

24) an authorized body - the authorized body for regulation, control and supervision of the financial market and financial organizations.

Chapter 2. Requirements to the use of information and communication technologies

3. A credit bureau shall develop an information system (hereinafter – an information system of a credit bureau), which provides for:

1) the receipt of information from the information provider;

2) formation of a database of credit records;

3) formation, issuance and storage of credit reports;

4) identification and authentication of users of the information system of the credit bureau ;

5) maintenance of an audit trail of the information system of the credit bureau.

4. Information system of a credit bureau shall meet the following requirements:

1) development, introduction and maintenance of the information system of the credit bureau (or adaptation of the ready product) on the basis of technical specifications and in accordance with the internal documents of the credit bureau, regulating the stages and procedure of development, modifications, testing, acceptance and commissioning, and documentation of all stages;

2) ensuring the distribution of the access rights of users of the information system of the credit bureau;

3) ensuring the account management of the information system of the credit bureau;

4) ensuring the information security of the protected data of the information system of the credit bureau.

5. Credit bureau shall ensure the availability and distribution of the development environments, testing and production operation of the information system of the credit bureau so that the changes made to the information system of the credit bureau in any of these environments had no effect on the information system of the credit bureau, located in another environment. Development and updating of the information system of the credit bureau shall not be made in the environment of commercial operation.

6. Third-party organizations and employees of the department of information technology, engaged in software development, shall not have access to the transfer of changes of the information system of the credit bureau in the environment of commercial operation and shall not have administrative access to the information system of the credit bureau in the environment of commercial operation.

7. Before the putting of the information system of the credit bureau into commercial operation, the settings set in it by default, shall change to the settings that meet the requirements of information security, defined by the internal documents of the credit bureau. These settings shall include the replacement of passwords used during testing, and deleting all test accounts.

8. Source codes (if available) and the executable modules of the information system of the credit bureau shall be stored in a protected storage of software that is suitable for their recovery.

9. An audit trail shall be maintained in the information system of the credit bureau that reflects the following:

1) the events of connection, identification, authentication and authorization (successful and unsuccessful);

2) the events of the change of the stored data;

3) the events of modification of security settings;

4) the events of modification of the user groups and their authorities;

5) the events of modification of user accounts and their authorities;

6) the events that reflect the installation of updates and (or) changes in the information system;

7) the events of the change of the parameters of maintenance of an audit trail;

8) the events of the changes of the system parameters.

10. The format of the audit trail shall include the following information:

1) identifier (login) of the user who committed the action;

2) date and time of the action;

3) names of objects with which the action was performed;

4) type or name of the action performed by the administrator or end user of the information system;

5) the result of an action (successfully or unsuccessfully).

11. The storage time of the audit trail shall be at least 3 (three) months in the operational access and at least one (1) year of archival access. It shall be allowed to store the audit trail in a specialized information system for storage, processing and analysis of events.

12. Credit bureau shall ensure the consistency of the audit trail by both organizational and technical means. Administrators of the information system shall be granted the access only to transfer the logs of the audit trail to the archive.

13. The data processing center of the credit bureau shall comply with the following requirements:

1) uninterrupted power supply system is provided by two or more independent inputs of electrical networks and automatically connected backup power supply devices that ensure an autonomous power supply for at least twenty-four hours;

2) the presence of two or more data transmission channels from independent providers of telecommunications services, installed in the building in different ways, in the main data processing center and at least two communication channels in the backup datacenter. The bandwidth of communication channels shall ensure the provision of services in accordance with the terms of agreements on information provision and contracts on obtaining credit reports.

14. In order to ensure sustainable functioning of information system of the credit bureau, the credit bureau shall comply with the following requirements:

1) information system of the credit bureau operates on the server system, enabling maintenance work without interrupting the functioning of its core services. When using virtualization technologies of hardware capacity, the virtual main and backup servers shall be placed on separate physical servers;

2) backup data processing center of the credit bureau is located outside the location of the credit bureau and provides recovery of the work of the information system of the credit bureau within a period not exceeding twelve hours from the time of closedown of the primary data processing center.

15. When connected to the information system of the credit bureau, the information provider shall use the workstation:

1) meeting the requirements of the credit bureau, reflected in the contract on provision of information;

2) secured by a license antivirus software with current antivirus databases.

16. When connected to the information system of the credit bureau, the recipient of the credit reports shall:

1) provide the availability of one or more workstations, used to connect only to the information system of the credit bureau;

2) provide protection of workstations by the license antivirus software with current antivirus databases.

17. In case of automation of the processes of information transmission by the information provider to the credit bureau and transfer of credit reports by the credit bureau to the recipient of the credit reports, the requirements of paragraphs 15 and 16 of the Requirements shall not apply to the information providers and recipients of the credit reports.

Chapter 3. Requirements to information security in organization of work of credit bureaus

Paragraph 1. Requirements to organization of information security management system

18. Credit bureau shall provide information security of the protected information when it is received, stored and processed and in the preparation and issuance of credit reports.

19. Credit bureaus shall ensure the establishment and functioning of the information security management system, which is part of the overall management system of the credit bureau that is designed to control the process of information security.

20. Information security management system shall ensure the protection of information assets of the credit bureau, allowing a minimum level of potential damage to the business processes of the credit bureau.

21. In order to ensure the proper level of the information security management system, its development and improvement, the credit bureau shall ensure the availability of the internal documents defining:

1) information security policy that includes:

goals, objectives and basic principles of development of the information security management system;

the area of action of the information security management system;

responsibility within the information security management system;

dissemination and accessibility of information security policy;

conditions for the review of the information security policy;

2) rules for the management of information assets, including:

basic requirements to the information, specifying the levels of confidentiality;

the requirement for labelling and certification of assets;

the treatment of information based on the confidentiality levels;

3) the backup (backup) procedure, including:

requirements for backup and archive copy;

testing of backups;

4) methods of risk assessment and risk management of information security, including:

the process of assessment and handling of information security risks;

acceptability criteria of information security risks;

information security risk handling plan;

report on the assessment and handling of information security risks;

5) the procedure for restriction of access and obligations of information system users (operators, administrators of information systems), including:

the order of termination or changes in functional responsibilities, including the requirements to disclose confidential information following the termination of the employment contract;

the procedure for training and awareness-raising;

the order to control access to information, information systems, networks, services, equipment and facilities;

regular review of access rights;

the requirement to control user and privileged access rights;

the procedure for the technical implementation of granting, changing, deleting the access rights;

6) procedure for work with information system of a credit bureau, including:

the procedure of development and change management of the information system of a credit bureau;

the rights and obligations of operators and administrators of the information system of the credit bureau;

7) procedures for management of information security incidents, including:

classification of incidents, the procedure for notification about incidents with an indication of the persons subject to notification;

the response and handling of incidents;

the rules for protection of information assets from malicious software.

22. Participants of information security management system of a credit bureau shall be:

1) the management body;

2) an executive body;

3) the collegial body, authorized to make decisions on the tasks of information security provision (hereinafter – the collegial body);

4) a risk management department;

5) a department for information security;

6) a department of information technology;

7) a security department;

8) a department for work with the personnel;

9) a legal entity;

10) additional departments.

The functions of the departments, specified in subparagraphs 4), 5), 6), 7), 8) and 9) of this paragraph, shall be allowed to be performed by the responsible persons in accordance with their functional responsibilities.

23. Credit bureau in establishment and functioning of information security management system shall ensure the independence of the departments of information security and information technology through their subordination to different members of the executive body of the credit bureau or directly to the head of the executive body of the credit bureau.

24. The management body of the credit bureau shall approve the information security policy.

25. The management body of the credit bureau shall approve the list of protected information, including information about the data constituting official, commercial or other secret protected by the law (hereafter – the protected information), and the procedure of work with the protected information.

26. The executive body of the credit bureau shall approve the internal documents, regulating the process of information security management, procedure and periodicity of revision which is determined by the internal documents of the credit bureau.

27. A credit bureau shall establish a collegial body, composed of representatives of the department of information security, the risk management department, the department of information technology, and if necessary the representatives of other departments of the credit bureaus. The head of the collegial body shall be the head of the executive body of a credit bureau or a member of the executive body of the credit bureau that oversees the operations of the department of information security.

28. The risk management department shall be responsible for the organization and coordination of the risk management process of the information security and shall perform the following functions:

1) development, introduction and continuous development of risk management information security system;

2) development of procedures on information security risk management;

3) analysis of the processes in the field of information security;

4) monitoring and assessment of the level of information security risks.

29. In order to ensure confidentiality, integrity and availability of information of the credit bureau, the department of information security shall perform the following functions:

1) to organize the information security management system, coordination and control of activity of departments of the credit bureau to ensure the information security and the activities to identify and analyze the threats, to counter attacks and investigate the information security incidents;

2) to develop information security policy of the credit bureau;

3) to provide methodological support for the process of information security of the credit bureau;

4) to make selection, introduction and use of methods, tools and mechanisms for the management, maintenance and control of information security of a credit bureau in the framework of their powers;

5) to conduct collecting, consolidating, storing and processing of information about information security incidents;

6) to analyze information about information security incidents;

7) to prepare proposals for adoption of a decision by the collegial body on the matters of information security;

8) to ensure the introduction and proper functioning of software and hardware, automating the process of ensuring information security of a credit bureau, as well as providing access to them;

9) to define the restriction on the use of privileged accounts;

10) to organize and conduct activities to ensure awareness of employees of the credit bureau on the matters of information security;

11) to monitor the state of the information security management system of a credit bureau;

12) to inform the credit bureau leadership about the status of the information security management system of a credit bureau.

30. The department of information technology of a credit bureau shall develop the internal documents determining:

1) the general scheme of the information infrastructure indicating a physical location of its elements;

2) a list of responsible administrators of the nodes of the information infrastructure (telecommunications devices, servers and operating systems placed on them, database management systems and the applied software of the user of the information system).

31. Credit bureau shall determine the possibility to impose the functions on technical safety on the department of information security. The department of information security shall perform the functions, entailing a conflict of interest with their main functions.

32. Credit bureau shall determine the possibility of delegating of following functions of the department of information security to other departments:

1) introduction and administration of software and hardware, automating the process of ensuring information security of a credit bureau – a department of information technology;

2) the organization and conduct of activities to ensure awareness of employees of the credit bureau about the information security – the department for work with the personnel;

3) recording and processing of events and information security incidents involving violations of the information security condition - the department of security or another department, not depending on the department of information technology.

33. The department of information technology shall perform the following functions:

1) develops the schemes of information infrastructure of a credit bureau;

2) ensures the provision of user access to information assets of a credit bureau;

3) provides the configuration of system and applied software of a credit bureau;

4) provides execution of the requirements, established by the internal documents of a credit bureau, on continuity of functioning of information infrastructure, confidentiality, integrity and availability of data of information systems of a credit bureau (including reservations and (or) the archiving and information backup);

5) ensures the observance of information security requirements in the selection, introduction, development and testing of information systems.

34. The department of security shall perform the following functions:

1) implements the measures of physical and technical security of credit bureau, and also arranges the access and intra-facility regime;

2) conducts preventive actions, aimed at minimizing the risk of threats to information security in the employment and dismissal of employees of the credit bureau.

35. The department for the work with the personnel shall perform the following functions:

1) ensures that the employees of a credit bureau, as well as persons, involved in the work under the contract on rendering of services, trainees, probationers sign the obligations on non-disclosure of confidential information;

2) participates in the process of raising the awareness of employees of the credit bureau in the field of information security.

36. The legal department shall provide legal expertise of internal documents of the credit bureau on the issues of provision of information security.

37. Heads of structural units of a credit bureau shall:

1) ensure that employees are familiarised with the credit bureau's internal documents containing information security requirements (hereinafter referred to as information security requirements);

2) be personally responsible for ensuring information security in the units headed by them ;

3) ensure the conclusion of agreements on non-disclosure of confidential information and inclusion of information security conditions in agreements, service/work agreements in cases when the credit bureau unit initiates the conclusion of such agreements and contracts.

Footnote. Paragraph 37 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

38. Credit bureau shall determine the business owner of the information system of the credit bureau, who is responsible for compliance with the requirements to information security in the creation, introduction, modification, provision of customers with products and services.

39. Workers of structural departments of the credit bureau shall:

1) be responsible for compliance with information security requirements, adopted in the credit bureau;

2) control the fulfillment of requirements to information security by the third parties with whom they interact within their functional responsibilities, including through inclusion of these requirements in the contracts with third parties;

3) notify their direct manager and the department of information security about all suspicious situations and violations when dealing with information assets.

Paragraph 2. Requirements for organization of access to information assets

40. Access to information shall be granted to the employees to the extent necessary for performance of their duties.

40-1. Access to information assets of the credit bureau of third parties shall be granted for the period and to the extent specified by the work, being implemented based on an agreement,

contract, including conditions on compliance with information security requirements, excluding cases stipulated by the legislation of the Republic of Kazakhstan. Agreements, contracts concluded with the information provider, the recipient of credit reports, third parties shall specify confidentiality clauses, provisions on compensation for damages resulting from information security violations, as well as information system failures and security infringements caused by the action or inaction of the credit bureau, the information provider, the recipient of credit reports, third parties.

Footnote. Paragraph 2 has been supplemented with paragraph 40-1 in compliance with Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall be enacted upon expiration of ten calendar days after the day of its first official publication).

41. The access to the information system of a credit bureau shall be carried out after identification and authentication of users.

42. Identification and authentication of users of the information system of the credit bureau shall be made through one of the following ways:

1) by typing the pair "account (ID) and password" and using the methods of two-factor authentication;

2) using the methods of biometric and (or) cryptographic and (or) hardware authentication .

43. The information system of the credit bureau shall use the personalized user accounts only.

44. The use of technological accounts shall be allowed in accordance with the list of such accounts for each information system, indicating the persons, personally responsible for their use and relevance, approved by the head of the department of information technology in coordination with the head of the department of information security.

45. The information system of the credit bureau shall use the functions on administering accounts and passwords, and locking of user accounts, defined by the internal document of the credit bureau.

46. Physical access to information assets of a credit bureau shall be provided in accordance with the internal documents of a credit bureau.

Paragraph 3. Requirements to information security of the information system of the credit bureau

47. Information security of information systems of a credit bureau shall be provided through:

1) protection of information during its processing, storage and transmission;

2) data backup on the side of the credit bureau;

3) the presence of recovery procedures of the information system of the credit bureau after failures and faults;

4) establishment of cryptographic protection of traffic between a credit bureau and information provider and (or) the recipient of the credit reports.

48. Credit bureau shall provide anti-virus protection of the information infrastructure in the order, established by the internal document of the credit bureau.

49. The department of information technology shall determine the order of any changes of information systems in coordination with the department of information security.

50. Update of the security of information systems, eliminating critical vulnerability, shall be established not later than one month from the date of their publication and distribution by the manufacturer, except for the cases agreed upon with the department on information security.

51. Update of the information system of the credit bureau prior to installation in the production environment shall be tested in a test environment.

52. Credit bureau shall provide the data backup storage of the information system of the credit bureau, its files and settings which ensures the restoration of its working copy.

53. The order and frequency of backup, storage, recovery of information, the frequency of testing the recovery efficiency of the information system of the credit bureau from the backups shall be determined by the internal document of the credit bureau.

Paragraph 4. Requirements for the process of protection of workstations of a credit bureau

54. Credit bureau shall define a list of software and equipment, permitted for the work with the information system of the credit bureau.

55. Software which is not intended for performance of functional duties of employees of the credit bureau shall not be installed on the workstations.

56. Internal documents of a credit bureau shall determine the organizational and technical measures, providing protection of workstations and storage devices and network resources, used to work with the information system of the credit bureau.

57. The credit bureau shall define and introduce the organizational and technical measures that prohibit the users from installation and configuration of software, workstations and peripheral equipment.

58. Users of the information system of the credit bureau shall not have the rights of a local administrator or similar rights, except for the cases where such rights are necessary for the functioning of the software, automating the functions, performed by the users.

59. Separate groups of users shall be entitled to install and configure software and equipment in cases where it is necessary for performance of official duties. These groups of users shall be provided with the local administrator rights or similar rights.

60. A list of users referred to in paragraphs 58 and 59 of the Requirements shall be formed , updated and approved by the head of the department of information technology in

coordination with the department of information security. In case of granting the users with additional rights in accordance with paragraphs 58 and 59 of the Requirements, the department of information security shall control their use.

Paragraph 5. Requirements to the process of physical security of data processing centers of credit bureaus

61. The order of the physical security of data processing centers shall be determined by the internal document.

62. The data processing center shall be equipped with the following technical security systems:

1) control system and access control;

2) security alarm;

3) fire alarm system;

4) automatic fire extinguishing system;

5) the system of maintaining the preset parameters of temperature and humidity;

6) video surveillance system;

7) uninterruptible power system.

63. Access to the data processing center shall be granted to employees of the credit bureau , the list of which is approved by the head of the department of information technology in coordination with the department of information security.

64. A credit bureau shall keep a log of the monitoring system and access control in the data processing center, which is stored at least 1 (one) year.

65. Automatic fire extinguishing system of the data processing center shall ensure the elimination of ignition throughout the volume of the room and shall have a back-up stock.

66. Video surveillance system of the data processing center shall provide the monitoring of all entrances to the data processing center. In the data processing center the placement of the camera shall eliminate the presence of areas inside the data processing center and in front of its entrance that are not covered by video surveillance.

67. Event recording by the video surveillance system of the data processing center shall be continuous or with the use of motion detection.

68. Archive of the video surveillance system of the data processing center shall be kept at least 3 (three) months.

69. In order to prevent an unauthorized physical access to the servers and active network equipment outside the data processing center, the internal documents of a credit bureau shall define the measures to ensure their safety.

Paragraph 6. Requirements to the procedure of monitoring and processing of information about information security incidents in the credit bureaus

70. Information about information security incidents, obtained in the course of monitoring of activities to ensure information security, shall be subject to consolidation and systematization.

71. Credit bureau shall ensure the integrity of data on information security incidents.

72. If the credit bureau identifies the need to monitor individual sources of events of information security during the non-office hours, a round-the-clock monitoring service shall be established.

73. Credit bureau shall determine the procedure of informing the executives and departments of the credit bureau about the incident of information security.

74. Credit bureau shall determine the procedure for adoption of urgent measures to address the incident of information security, its causes and consequences.

75. The credit bureau shall keep a register of information security incidents indicating the information about the incident of the information security, the measures taken and the proposed remedial measures, in paper or in electronic form.

76. Following the results of processing of the incident of the information security, a credit bureau shall conduct a comprehensive analysis of the causes of the incident of information security, its mechanism and consequences. When collecting the technical data from software and hardware involved in the incident of the information security, the safety and consistency of the collected data shall be ensured.

77. Information about the incident of information security, as well as proposals for corrective measures in order to reduce the likelihood and potential damage from the repeated incident of information security shall be stored in the credit bureau.

78. For incidents of information security, the likelihood of which is high and cannot be reduced in a short time, the credit bureau shall develop internal documents, describing the algorithm of handling of incidents of information security, the model urgent measures for localization of information security incidents and their consequences, methods of processing of incidents of information security.

Paragraph 7: Requirements for reporting information on the status of the information security management system, events and information security incidents of credit bureaus

Footnote. The heading of paragraph 7 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 dated 16.08.2024 (shall take effect upon expiry of ten calendar days after the day of its first official publication).

79. Annually, not later than January 20 of the year following the reporting year, the credit bureau shall provide the authorised body with information on the status of the information security management system and its compliance with the Requirements.

Footnote. Paragraph 79 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of

16.08.2024 (shall come into effect upon expiration of ten calendar days after the day of its first official publication).

80. Data on the status of the information security management system shall comprise data on (about):

1) the scope of the credit bureau's information security management system and its participants with specification of compliance of their functionality with the Requirements;

2) availability of documents governing the creation and operation of the information security management system;

3) availability and quantitative composition of software and hardware tools applied to ensure information security;

4) conditions and obligations on information security provided in agreements on rendering services concluded with telecom operators;

5) availability, logistics and readiness of backup data processing centres;

6) measures implemented to align the credit bureau's information security management system and information assets with the Requirements.

Footnote. Paragraph 80 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall enter into force ten calendar days after the date of its first official publication).

81. Data on the status of the information security management system, information security events and incidents shall be reported to the authorised body via an automated information processing system (hereinafter - AIPS) designated for processing information on information security events and incidents and integrated with information security systems or credit bureau systems, collecting and analysing information on events in the information infrastructure in real time or in electronic format using a transport system of guaranteed delivery of information with cryptographic protection means ensuring confidentiality and uncorrectability of the data supplied.

For a credit bureau with state participation, it shall be permitted to furnish data on information security events and incidents to the authorised body via informatisation objects of the National Bank of the Republic of Kazakhstan integrated with the AIPS.

Footnote. Paragraph 81 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall become effective ten calendar days after the day of its first official publication).

81-1. The credit bureau shall furnish the authorised body with data on the following information security incidents revealed:

1) exploitation of vulnerabilities in application and system software;

2) unauthorised access to the information system;

3) a denial-of-service attack on an information system or data network;

4) infection of the server with a malicious programme or code;

5) unauthorised transfer of funds caused by breach of information security controls;

6) other information security incidents involving downtime of information systems for more than one hour.

Data on information security incidents mentioned in this paragraph shall be reported immediately to the credit bureau via AIPS or in electronic format using a transport system of guaranteed information delivery with cryptographic protection means ensuring confidentiality and unadjustability of the reported data.

For a credit bureau with state participation, it shall be permitted to report data on information security events and incidents to the authorised body via informatisation objects of the National Bank of the Republic of Kazakhstan integrated with the AIPS.

Footnote. Paragraph 7 has been supplemented with paragraph 81-1 pursuant to Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall be put into effect upon expiration of ten calendar days after the date of its first official publication).

81-2. Data on information security events shall be made available in an automated mode by transmission from information security systems or systems of the credit bureau that collect and analyse information on events in the credit bureau's information infrastructure to the AIPS in real time.

For a credit bureau with state participation, it shall be permitted to report data on information security events and incidents to the authorised body via informatisation objects of the National Bank of the Republic of Kazakhstan integrated with the AIPS.

Footnote. Paragraph 7 has been supplemented with paragraph 81-2 pursuant to Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall become effective ten calendar days after the date of its first official publication).

Paragraph 8: Information security requirements for the remote service provision software by credit bureaus

Footnote. Chapter 3 is supplemented by paragraph 8 pursuant to Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall come into effect upon expiry of ten calendar days after the day of its first official publication).

81-3. Software for remote provision of credit bureau services shall cover:

1) web application server software (hereinafter referred to as web application);

2) software for mobile devices (hereinafter - mobile application);

3) software for software interface servers (hereinafter - server software).

81-4. The credit bureau shall develop and (or) finalise the software for remote service provision in line with the internal documents of the credit bureau governing the procedure for

development and (or) finalisation of the software, stages of development and their participants.

81-5. Where the development and (or) modification of the credit bureau's remote service delivery software is outsourced to a third party organisation and (or) a third party, the credit bureau shall ensure that the third party organisation and (or) third party organisation fulfils the requirements of this Chapter and internal documents, and shall be liable for the security status of the remote service delivery software.

81-6. The source codes of remote services software developed at the credit bureau shall be archived in specialised code repository management systems located within the security perimeter of the credit bureau, with back-up copying ensured.

81-7. Regardless of the credit bureau's approach to the development and/or enhancement of remote service delivery software, security testing shall be mandatory and shall cover, at a minimum, the following activities:

1) static analysis of the source code;

2) analysis of components and (or) third-party libraries.

81-8. Static source code analysis of the credit bureau's remote service delivery software shall be conducted with the use of a static source code analysis scanner that supports the analysis of all programming languages used in the software under audit, which functions include, but are not limited to, detecting the following vulnerabilities:

1) existence of mechanisms that allow malicious code injection;

2) use of vulnerable operators and functions of programming languages;

3) use of weak and vulnerable cryptographic algorithms;

4) using the code that, under certain conditions, causes denial of service or substantial slowdown of the remote service software of the credit bureau;

5) existence of mechanisms for bypassing the protection systems of the credit bureau's remote service delivery software;

6) use of open secrets in the code;

7) breaching application security templates and practices.

81-9. Analysis of components and (or) third-party libraries of the credit bureau's remote service provision software shall be aimed at identifying known vulnerabilities inherent in the used version of the component and (or) third-party library, as well as tracking dependencies between components and (or) third-party libraries and their versions.

81-10. The credit bureau shall implement preventive measures to eliminate the vulnerabilities revealed in the order specified by an internal document approved by the executive body. Meanwhile, critical vulnerabilities shall be eliminated prior to the commissioning of the remote service provision software and (or) its new versions.

81-11. The credit bureau shall launch the remote service delivery software and (or) its new versions upon approval of the information security unit.

81-12. The credit bureau shall maintain storage and operational access to all versions of source codes of remote service delivery software and security testing results that have been commissioned within the last 3 (three) years.

81-13. Data exchange between the customer and server sides of the remote service provision software shall be encrypted using Transport Layer Security encryption protocol version 1.2 or higher.

81-14. When a customer is initially registered in the mobile application, the credit bureau shall biometrically identify the customer via the Identification Data Exchange Centre (hereinafter - IDEC), or using biometric data obtained via the credit bureau's devices.

81-15. Access code (password) to the mobile application shall be changed using biometric identification of the customer with the use of biometric data confirmed by the IDEC or with the use of biometric data obtained via credit bureau devices.

81-16. The customer shall be identified and authenticated in the remote service delivery software using two-factor authentication methods (using two out of three factors: knowledge, possession, inalienability) in line with the security procedures established by the internal documents of the credit bureau.

81-17. The cross-domain authentication mechanism for the remote service delivery software shall be coordinated with the information security unit.

81-18. The web application shall ensure:

1) unambiguous identification of the web application belonging to the credit bureau (domain name, logos, corporate colours);

2) prohibition to store authorisation data in the browser memory;

3) masking of entered secrets;

4) informing on the customer's authorisation page of the cyber hygiene measures that are recommended to be followed when using the web application;

5) handling errors and exclusions in a secure manner, preventing sensitive data from being displayed in the customer interface by providing minimally sufficient error information.

81-19. The mobile application shall ensure:

1) unambiguous identification of the mobile application belonging to the credit bureau (data in the official application shop, logos, corporate colours);

2) blocking the functionality of remote services of the credit bureau in case of detecting signs of breach of integrity and (or) bypassing the protective mechanisms of the operating system, detection of remote management processes;

3) notification of the customer on the availability of mobile application updates;

4) the possibility of forced installation of mobile application updates or blocking of mobile application functionality prior to their installation in cases of the need to eliminate critical vulnerabilities;

5) storage of confidential data in a secure container of the mobile application or storage of system credentials;

6) exclusion of caching of confidential data;

7) eliminating sensitive data in public form from the mobile application backups;

8) informing the customer of the cyber hygiene practices that are recommended to be followed when using the mobile application;

9) notifying the customer on the events of authorisation under his/her account, change and (or) restoration of password, change of mobile phone number registered by the credit bureau;

10) in the course of cash transactions - transmission of geolocation data of the mobile device to the credit bureau's server software if authorised by the customer, or transmission of information on the absence of such authorisation.

81-20. The credit bureau shall ensure on its side:

1) processing errors and exclusions in a secure manner, without disclosing confidential data in the response, ensuring minimum sufficient information to diagnose the problem;

2) identification and authentication of mobile applications and associated devices;

3) validation of data to avoid query spoofing and malware injection attacks.

Chapter 4. Requirements to information security in organization of activities of information providers

82. Information provider shall guarantee the integrity and confidentiality of the information, transmitted to the information system of the credit bureau.

83. The information provider shall provide the appropriate level of information security in accordance with the terms of the contract on provision of information.

84. The information provider shall provide the performance of organizational-technical, technological requirements and measures necessary for operation and protection of system and applied software used to interact with the information system of the credit bureau.

85. When using equipment for working with the information system of the credit bureau, the need to protect it from unauthorized access and protection of media and network resources shall be taken into account.

86. The information provider shall designate the operator (s).

87. The information provider shall provide a presence of the signed obligations of the operator (s) for non-disclosure and non-distribution of information that became known to them in the course of performance of their duties.

88. The information provider shall provide the presence of internal documents (including job descriptions), determining the procedure of appointment of operator (s), his (their) rights and responsibilities.

89. Access to information shall be granted to employees of information providers to the extent necessary for performance of their duties.

90. The account of the operator, through which he authorizes in the information system of the credit bureau, shall belong to a particular individual.

91. At the request of the authorized body, an information provider shall provide the information confirming its compliance with the requirements, stipulated by the contract on provision of information.

92. The operating system of a workstation shall provide the functions for identification and authentication of user and access rights of users and authorization in accordance with the assigned rights.

93. If a workstation is used to connect to the information system of a credit bureau, the simultaneous connection to other Internet resources shall not be made.

94. Employees of information provider shall ensure the confidentiality of personal identification and authentication data, used to access information systems.

95. Employees of information provider shall guarantee the confidentiality of information that became known in the course of using of the information system of the credit bureau.

Chapter 5. Requirements to information security in organization of activities of recipients of credit reports

96. The recipient of the credit report shall ensure the confidentiality and integrity of the information, received from the information systems of the credit bureau.

97. The recipient of the credit report shall ensure the appropriate level of information security in accordance with the terms of the contract on receiving the credit reports.

98. The recipient of the credit report shall ensure the implementation of organizational-technical, technological requirements and measures necessary for operation and protection of system and applied software, used to interact with the information system of the credit bureau and the processing of the information received.

99. When using equipment for working with the information system of the credit bureau, the need to protect it from unauthorized access and protection of media, and network resources, used for work with the information system of the credit bureau shall be taken into account.

100. The recipient of the credit report shall determine and approve the list of responsible persons.

101. The recipient of the credit report shall ensure the presence of obligations, signed by the responsible (competent) person (s) of the organization, on non-disclosure of the information that became known to them in the course of performance of their duties.

102. The recipient of the credit report shall ensure the availability of internal documents, defining the procedure for determining and approving the list of responsible persons, their rights and responsibilities (including job descriptions).

103. Access to information shall be granted to employees to the extent necessary for the performance of their duties.

104. Account of a responsible person through which he authorizes in the information system of the credit bureau shall correspond to the particular individual.

105. The recipient of the credit report will carry out the scheduled and unscheduled inspections of compliance of workstations with the Requirements and internal documents of the recipient of a credit report, regulating the information security.

106. The recipient of the credit report at the request of the authorized body shall submit information confirming its compliance with the requirements, specified in the contract for obtaining credit reports.

107. Operating system of a workstation shall provide the functions for identification and authentication of user and access rights of users and authorization in accordance with the assigned rights.

108. The recipient of credit reports shall use its own workstation.

109. If a workstation is used to connect to the information system of the credit bureau, the simultaneous connection to other Internet resources shall not be made.

110. Employees of the recipient of credit reports shall ensure the confidentiality of personal identification and authentication data used to access the information systems.

111. Employees of the recipient of credit reports shall ensure the confidentiality of the information that became known in the course of using the information system of the credit bureau.

Annex 2
to the resolution of the Board of
the National Bank of the
Republic of Kazakhstan
dated September 27, 2018,
№ 228

Requirements imposed by credit bureaus on information providers and recipients of credit reports

Footnote. The heading - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall become effective ten calendar days after the day of its first official publication).

1. These Requirements imposed by credit bureaus on information providers and credit report recipients (hereinafter referred to as the Requirements) have been drawn up under sub-paragraph 6) of Article 5 of the Law of the Republic of Kazakhstan “On Credit Bureaus and the Formation of Credit Histories in the Republic of Kazakhstan”, and establish requirements for credit bureaus to use information and communication technologies and ensure information security when organising the activities of information providers who are individual entrepreneurs or legal entities, selling goods and services under a loan agreement or granting deferred payments, the systematised attributes thereof are set out in Decree № 25 of the Government of the Republic of Kazakhstan of January 18, 2005 “On Approval of Systematised Attributes of Individual Entrepreneurs or Legal Entities Selling Goods and Services under a Loan Agreement or Granting Deferred Payments” (hereinafter referred to as

Decree № 25), natural monopoly entities rendering public utilities services other persons under agreements on provision of information (hereinafter referred to as information providers), as well as recipients of credit reports who are individual entrepreneurs or legal entities, selling goods and services under a loan agreement or granting payment deferrals, the systematised attributes thereof being established by Decree № 25, other persons under the information provision agreements, a representative of bondholders regarding the credit report of the bond issuer with whom an agreement on representation of bondholders' interests has been concluded (hereinafter referred to as the recipients of credit reports).

Footnote. Paragraph 1 - as revised by Resolution of the Board of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market № 59 of 16.08.2024 (shall be enforced upon expiration of ten calendar days after the date of its first official publication).

2. The requirements of the credit bureaus to the information providers and recipients of credit reports shall be included in the contract on information provision and the contract on receipt of credit reports.

3. The requirements of credit bureaus to the use of information and communication technologies in organization of activities of information providers and recipients of credit reports shall comply with the requirements of paragraphs 15, 16 and 17 of the Requirements to the use of information and communication technologies and ensuring the information security in organization of the activities of the credit bureaus, information providers and recipients of credit reports, that are banks, organizations, engaged in certain types of banking operations, micro-finance organizations and collection agencies, approved by this resolution.

4. The requirements of credit bureaus to the provision of information security in organization of activities of information providers and recipients of credit reports shall meet the requirements of chapters 4 and 5 of the Requirements to the use of information and communication technologies and information security in organization of activities of credit bureaus, information providers and recipients of credit reports that are banks, organizations engaged in certain types of banking operations, microfinance organizations and collection agencies, approved by this Resolution.

Annex 3
to the resolution of the Board
of the National Bank of the
Republic of Kazakhstan
dated September 27, 2018,
№ 228

The list of regulatory legal acts of the Republic of Kazakhstan, as well as structural elements of some regulatory legal acts of the Republic of Kazakhstan, recognized as invalid

1. Resolution of the Board of the National Bank of the Republic of Kazakhstan dated May 27, 2015 № 91 "On approval of the Requirements to the use of information and

communication technologies and provision of information security in organization of the activities of credit bureaus, information providers and recipients of credit reports" (registered in the Register of state registration of regulatory legal acts under №11669, published on July 30, 2015 in the legal information system "Adilet").

2. Paragraph 2 of the Resolution of the Board of the National Bank of the Republic of Kazakhstan dated May 30, 2016 № 146 “On amendments and addenda to some regulatory legal acts of the Republic of Kazakhstan on reduction of permits and simplification of authorization procedures (registered in the Register of state registration of regulatory legal acts under №14208, published on October 5, 2016 in the information and legal system "Adilet ").

3. Resolution of the Board of the National Bank of the Republic of Kazakhstan dated June 14, 2017 № 102 "On amendments and addenda to the resolution of the Board of the National Bank of the Republic of Kazakhstan dated May 27, 2015 № 91" On approval of the Requirements to the use of information and communication technologies and provision of information security in organization of the activities of credit bureaus, information providers and recipients of credit reports" (registered in the Register of state registration of regulatory legal acts under № 15608, published on September 15, 2017 in the Reference Control Bank of regulatory legal acts of the Republic of Kazakhstan).