On approval of Requirements to the organization of safe work, ensuring safety and information security from unauthorized access to data stored in the insurance (reinsurance) organization, and also cybersecurity of the insurance (reinsurance) organization

Unofficial translation

Resolution of the Board of the National Bank of the Republic of Kazakhstan of July 30, 2018 № 164. Registered with the Ministry of Justice of the Republic of Kazakhstan on August 9, 2018 № 17289.

Unofficial translation

Pursuant to the Law of the Republic of Kazakhstan "On Insurance Activities", the Board of the National Bank of the Republic of Kazakhstan **RESOLVES:**

Footnote. Preamble - as amended by the Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market dated 29.08.2024 № 73 (effective sixty calendar days after the date of its first official publication).

1. Approve the attached Requirements for organization of safe work, ensuring safety and information security from unauthorized access to data stored in the insurance (reinsurance) organization, also cybersecurity of the insurance (reinsurance) organization.

2. In accordance with the procedure established by the legislation of the Republic of Kazakhstan, the Department for the Regulation of Non-Bank Financial Organizations (A.M. Kosherbayeva) shall:

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

2) within ten calendar days from the date of state registration of this resolution, direct its paper and electronic copy in the Kazakh and Russian languages to the Republican State Enterprise with the Right of Economic Management “Republican Center of Legal Information ” for official publication and inclusion in the Reference Control Bank of Regulatory Legal Acts of the Republic of Kazakhstan;

3) place 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, submit to the Legal Department the data on execution of the actions provided for in subparagraphs 2), 3) of this paragraph and paragraph 3 of this resolution.

3. The Directorate for the Protection of the Rights of Consumers of Financial Services and External Communications (A.L. Terentiev) shall direct its copy for official publication in periodicals.

4. Control over the execution of this resolution shall be entrusted to the Deputy Chairman of the National Bank of the Republic of Kazakhstan, Zh.B. Kurmanov.

5. This resolution shall be enforced on January 1, 2019 and is subject to official publication.

Chairman
of the National Bank *D. Akishev*

Approved
by Resolution № 164
of the Board
of the National Bank
of the Republic of Kazakhstan
of July 30, 2018

Requirements to the organization of safe work, ensuring safety and information security from unauthorized access to data stored in the insurance (reinsurance) organization, and also cybersecurity of the insurance (reinsurance) organization Chapter 1. General Provisions

1. These Requirements to the organization of safe work, ensuring information safety and security from unauthorized access to data stored in the insurance (reinsurance) organization, as well as cybersecurity of the insurance (reinsurance) organization (hereinafter referred to as the Requirements) have been developed pursuant to the Law of the Republic of Kazakhstan " On Insurance Activities" and establish requirements for the organization of safe work, ensuring information safety and security from unauthorized access to data stored in the insurance (reinsurance) organization, as well as cybersecurity of the insurance (reinsurance) organization.

Footnote. Paragraph 1 as amended by the Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market dated 29.08.2024 № 73 (effective sixty calendar days after the date of its first official publication).

2. In the Requirements the following concepts shall be used:

1) data asset – a set of information and the object of information-communication infrastructure used for storage and (or) information processing;

2) objects of information and communication infrastructure - information systems of an insurance (reinsurance) organization, technological frameworks, the hardware and software, telecommunications networks, and also systems of ensuring smooth functioning of technical means and information security;

3) information and communication infrastructure (hereinafter - information infrastructure) – a set of information and communication infrastructure facilities intended to ensure functioning of the technological environment for the purpose of forming electronic information resources and provision of access to them;

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

5) threat of information security – a set of the conditions and factors creating prerequisites to emergence of an information security incident;

6) ensuring information security - the process directed to maintenance of condition of confidentiality, integrity and availability of data assets of the insurance (reinsurance) organization;

7) information security incident - separately or serially arising malfunctions in the work of the information infrastructure or its separate objects posing threat to their proper functioning and (or) conditions for unlawfully obtaining, copying, distributing, modifying, destroying or blocking electronic information resources of the insurance (reinsurance) organization;

8) data processing center - a specially designated room in which the server and communication equipment of the information infrastructure of the insurance (reinsurance) organization is placed;

9) access - the ability to use data assets;

10) backup copy - a copy of the data on a storage medium intended to restore the data to the original or new location if need arises;

11) information system of insurance (reinsurance) organization - an information system in which data of the insurance (reinsurance) organization and its clients are stored and processed ;

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

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

14) attack - an attempt of destroying, disclosing, changing, restricting access, theft, obtaining unauthorized access or unauthorized use of a data asset.

Chapter 2. Requirements to the organization of safe work, ensuring safety and information security from unauthorized access to data stored in the insurance (reinsurance) organization, and also cybersecurity of the insurance (reinsurance) organization

3. The insurance (reinsurance) organization shall organize safe work ensuring safety and information security from unauthorized access to data stored in the insurance (reinsurance) organization, and also cybersecurity of the insurance (reinsurance) organization by creating an information security management system (hereinafter information security management system), which is part of the overall management system of the insurance (reinsurance) organization, intended to manage the process of information security provision.

4. The information security management system shall provide protection of information assets of the insurance (reinsurance) organization.

5. The insurance (reinsurance) organization shall ensure the functioning of the information security management system, its development and improvement.

6. Participants in the information security management system of an insurance (reinsurance) organization shall be:

1) the management body;

2) the executive body;

3) information security unit;

4) information technology unit;

5) security unit;

6) human resources unit;

7) legal unit;

8) compliance control unit;

9) internal audit unit.

It shall be allowed to exercise the functions of the subdivisions indicated in subparagraphs 3), 4), 5), 6), 7), 8) and 9) of this paragraph by responsible persons.

7. In the creation and functioning of the information security management system the insurance (reinsurance) organization shall ensure independence of information security and information technology units through their subordination to various members of the executive body of the insurance (reinsurance) organization or directly to the head of the executive body of the insurance (reinsurance) organization.

8. The management body of the insurance (reinsurance) organization shall approve information security policy that shall determine:

1) goals, objectives and basic principles of building an information security management system;

2) requirements to the organization of access to the created, stored and processed information in the information systems of the insurance (reinsurance) organization, monitoring of information and access to it;

3) requirements to the collection, consolidation and storage of data on information security incidents;

4) requirements to monitoring of the information security activities;

5) requirements to carrying out the analyses of data on information security incidents;

6) responsibility of employees of the insurance (reinsurance) organization in ensuring information security in the performance of their functional duties.

9. The management body of the insurance (reinsurance) organization shall approve the list of protected information, including data on information constituting the insurance secret, official, commercial or other secrets protected by law (hereinafter - the protected information) , and the procedure for working with the protected information.

10. The management body of the insurance (reinsurance) organization shall exercise control over the state of the information security management system of the insurance (reinsurance) organization.

11. The executive body of the insurance (reinsurance) organization shall approve the internal documents of the insurance (reinsurance) organization governing the information security process, the order and frequency of revisions of which shall be determined by the internal documents of the insurance (reinsurance) organization.

12. For the purposes of ensuring confidentiality, integrity and accessibility of information of the insurance (reinsurance) organization, the information security unit shall perform the following functions:

1) organize the information security management system, carry out coordination and monitoring of activities of the insurance (reinsurance) organization in the provision of information security and measures to identify and analyze threats, counter attacks and investigate information security incidents;

2) develop the information security policy of the insurance (reinsurance) organization;

3) provide methodological support for the process of ensuring the information security of the insurance (reinsurance) organization;

4) select, implement and apply methods, means and mechanisms for managing, ensuring and controlling the information security of the insurance (reinsurance) organization within its authority;

5) collect, consolidate, store and processes data on information security incidents;

6) carry out analyses of the data on information security incidents;

7) organize and conduct apprising of the insurance (reinsurance) organization's employees of the information security matters;

8) monitor condition of the information security management system of the insurance (reinsurance) organization;

9) apprise the insurance (reinsurance) organization's management of the condition of the information security management system of the insurance (reinsurance) organization.

13. The information technology unit shall perform the following functions:

1) develop information infrastructure schemes for the insurance (reinsurance) organization ;

2) provide employees' access to the information assets of the insurance (reinsurance) organization;

3) provide compliance with the established requirements for continuity of the information infrastructure, confidentiality, integrity and accessibility of information systems of the insurance (reinsurance) organization (including reservation and (or) archiving) in accordance with the internal documents of the insurance (reinsurance) organization;

4) provide compliance with the internal documents of the insurance (reinsurance) organization containing information security requirements when selecting, implementing, developing and testing information systems of the insurance (reinsurance) organization.

14. The security unit shall perform the following functions:

1) implement measures of physical and technical safety in the insurance (reinsurance) organization, including organization of access and internal security control regime;

2) conduct preventive measures directed at minimization of risks of threats to information security when hiring and firing employees of the insurance (reinsurance) organization.

15. The human resources unit shall perform the following functions:

1) provide the signing of non-disclosure obligations by employees of the insurance (reinsurance) organization, also by persons involved in the work under a service contract, trainees, interns;

2) contribute to organization of awareness raising process in the field of information security for the insurance (reinsurance) organization's employees.

16. The legal unit shall provide legal expertise on the internal documents of the insurance (reinsurance) organization regarding information security.

17. The compliance control unit together with the legal unit of the insurance (reinsurance) organization shall determine the types of information to be included in the list of protected information provided for in paragraph 9 of the Requirements.

18. The internal audit unit shall perform assessment of condition of the information security management system in accordance with the internal documents of the insurance (reinsurance) organization governing the arrangement of the internal audit system of the insurance (reinsurance) organization.

19. Heads of insurance (reinsurance) organization's units shall:

1) apprise the staff of the information security requirements;

2) bear personal responsibility for information security safeguarding in the units they are in charge of.

20. Employees of the insurance (reinsurance) organization shall:

1) ensure compliance with the information security requirements adopted by the insurance (reinsurance) organization;

2) notify their immediate supervisor and the information security unit about all dubious situations and violations arising in the work with information assets.

21. Provision of physical access to information assets of the insurance (reinsurance) organization shall be in line with the internal documents of the insurance (reinsurance) organization.

22. Access to information shall be provided to employees in the amount necessary for the performance of their functional duties.

23. Access to information systems of the insurance (reinsurance) organization shall be carried out by identifying and authenticating the users of the insurance (reinsurance) organization's information systems.

24. In the information systems of the insurance (reinsurance) organization, solely personalized accounts shall be used.

25. The use of technology accounts shall be permissible in accordance with the list of such accounts for each information system with indication of individuals that are personally responsible for their use and relevance, approved by the head of the information technology department in coordination with the head of the information security department.

26. In the information systems of the insurance (reinsurance) organization, functions or means of managing accounts and passwords, also of blocking accounts shall be applied, determined by internal documents of the insurance (reinsurance) organization.

27. The insurance (reinsurance) organization shall provide backup storage of the data of the information systems of the insurance (reinsurance) organization, their files and settings, which enables restoration of workable copies of the information systems.

28. The order and periodicity of backup, storage, recovery of information shall be determined by the internal document of the insurance (reinsurance) organization.

29. The insurance (reinsurance) organization shall provide anti-virus protection of the information infrastructure in accordance with the internal documents of the insurance (reinsurance) organization.

30. Information systems of the insurance (reinsurance) organization shall use audit trail function, which shall reflect the following events (successful and unsuccessful):

1) connection setup, identification and authentication in the information system of the insurance (reinsurance) organization;

2) modification of accounts and their powers;

3) installation of updates and (or) changes in the information system of the insurance (reinsurance) organization;

4) change of the audit parameters;

5) changes of system parameters.

31. The shelf life of the audit trail shall be at least 3 (three) months in the information systems of the insurance (reinsurance) organization and at least 1 (one) year in the form of backup copies of the audit trail.

32. The information technology unit shall monitor updates of the insurance (reinsurance) organization’s information systems and, together with the information security unit, shall determine the procedure for managing updates of the insurance (reinsurance) organization’s information systems.

33. Updates of information systems of the insurance (reinsurance) organization shall be tried in a test environment prior to installation in an industrial environment.

34. The procedure for assuring physical security of data processing centers shall be determined by the internal documents of the insurance (reinsurance) organization.

35. The insurance (reinsurance) organization shall determine the list of software authorized for use in the insurance (reinsurance) organization.

36. The data processing center of the insurance (reinsurance) organization shall be equipped with the following technical safety systems:

1) access monitoring and control system;

2) security alarm;

3) fire alarm;

4) automatic fire extinguishing system;

5) system for maintaining specified microclimate parameters;

6) video surveillance system (CCTV);

7) uninterruptible power supply system.

37. Access to the data processing center shall be provided to individuals that are on the list approved by the head of the information technology unit in agreement with the information security unit.

38. Recording of events shall be made by the video surveillance (CCTV) system of the data processing center continuously or using the motion detection.

39. The archive of the data center's CCTV system shall be stored for at least 3 (three) months.

40. Data on information security incidents obtained in the course of monitoring of the information security activities shall be subject to consolidation, systematization and storage for at least five (5) years.

41. The insurance (reinsurance) organization shall determine the procedure for notifying the executives and units of insurance (reinsurance) organization about the occurrence of information security incident.

42. The insurance (reinsurance) organization shall determine the procedure for taking urgent measures to eliminate information security incident, its causes and consequences.

43. The insurance (reinsurance) organization shall maintain a log of information security incidents in paper or electronic format, in which registration data of the conclusion on the analysis of information security incident shall be entered in accordance with paragraph 46 of the Requirements.

44. At the collection of technical data from software and hardware involved in the information security incident, the collected data shall be kept safe and unaltered.

45. Upon the processed results of the information security incident, an analysis shall be conducted of the causes of the information security incident, its mechanism and consequences .

46. Upon the analysis of the information security incident, a conclusion shall be drawn, reflecting full information on the information security incident, along with proposed corrective actions to reduce the likelihood and possible damage of a repeated security incident .

47. The insurance (reinsurance) organization shall undertake organizational and technical measures that prohibit the insurance (reinsurance) organization's employees to install and configure software on their own.

48. In exceptional cases, individual groups of users shall be permitted to independently install and configure software and hardware. These user groups shall be granted local administrator or similar rights.

49. The list of users specified in clause 48 of the Requirements shall be formed, updated and approved by the head of the information technology department in agreement with the information security department. In the event of granting additional rights to users in accordance with clause 48 of the Requirements, the information security division shall monitor their exercising.

50. Annually, no later than January 10 of the year following the reporting year, the insurance (reinsurance) organization shall submit information to the authorized body on the state of the information security management system.

51. The information specified paragraph 50 of the Requirements shall include data on:

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

2) availability and numerical composition of software and hardware used to maintain information security;

3) availability and logistics of the data processing facilities;

4) measures taken to improve the information security management system and information assets of the insurance (reinsurance) organization or their absence.

52. The information, specified in paragraph 50 of the Requirements shall be submitted to the authorized body via an automated information processing system designed to process information on information security events and incidents, or in electronic format using a guaranteed data transport system with cryptographic safeguards that ensure confidentiality and non-correctability of the provided data.

Footnote. Paragraph 52 as amended by the Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market dated 29.08.2024 № 73 (effective sixty calendar days after the date of its first official publication).

53. The authorized body shall check compliance of the insurance (reinsurance) organization with the Requirements at least once in 3 (three) years.

Chapter 3. Requirements for ensuring information security of software for remote provision of services of an insurance (reinsurance) organization

Footnote. The requirements have been supplemented by Chapter 3 pursuant to the Resolution of the Board of the Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market dated 29.08.2024 № 73 (effective sixty calendar days after the date of its first official publication).

54. The software for remote provision of services by an insurance (reinsurance) organization includes:

1) software for web application servers (hereinafter referred to as the web application);

2) software for mobile devices (hereinafter referred to as the mobile application);

3) software for program interface servers (hereinafter referred to as the server software).

55. The development and (or) modification of software for remote provision of services shall be performed by the insurance (reinsurance) organization in accordance with the internal documents of the insurance (reinsurance) organization regulating the procedure for developing and (or) modifying software, the stages of development and their participants.

56. If the development and (or) modification of software for remote provision of services by an insurance (reinsurance) organization is transferred to a third-party organization and (or) a third party, the insurance (reinsurance) organization shall ensure that the third-party organization and (or) third party comply with the requirements of this chapter and internal documents, and shall be responsible for the security status of the software for the remote provision of services.

57. Source codes of the software of remote provision of services developed by an insurance (reinsurance) organization shall be stored in specialized code repository management systems placed within the security perimeter of the insurance (reinsurance) organization, with backup copying provided.

58. Regardless of the approach adopted by the insurance (reinsurance) organization to the development and (or) modification of software for remote provision of services, it is mandatory to test the main functions of the system, such as user registration, messaging and other key operations, test the security of the system for protection against threats such as unauthorized access, phishing, hacking and data leakage.

59. The insurance (reinsurance) organization shall ensure implementation of corrective measures to eliminate the identified vulnerabilities in the procedure established by the internal document approved by the executive body. In this case, critical vulnerabilities shall be eliminated before putting into operation the software for remote provision of services and (or) its new versions.

60. The insurance (reinsurance) organization shall put into operation the software for remote provision of services and (or) its new versions after coordination with the person responsible for information security.

61. The insurance (reinsurance) organization shall ensure storage and online access to all versions of the source codes of the software for remote provision of services and the results of security testing, which were put into operation over the past 3 (three) years.

62. Data exchange between the client and server sides of the software for remote provision of services shall be encrypted using the Transport Layer Security encryption protocol version no lower than 1.2.

63. During the initial registration of a client in the mobile application the insurance (reinsurance) organization shall perform biometric identification of the client through the Identification Data Exchange Center (hereinafter referred to as the IDEC) and a one-time personal identifier (password) received in an SMS.

64. Changing of the access code (password) to the mobile application shall be made with the use of biometric identification of the client using biometric data confirmed by the IDEC and a one-time personal identifier (password) received in an SMS message.

65. Identification and authentication of the client in the software for remote provision of services shall be made by two-factor authentication methods (using two of the three factors: knowledge, possession, inalienability) in accordance with the security procedures established by the internal documents of the insurance (reinsurance) organization.

66. The mechanism of cross-domain authentication of software for remote provision of services shall be agreed upon with the information security department.

67. The web application shall ensure:

1) unambiguous identification of the web application belonging to the insurance (reinsurance) organization (domain name, logos, corporate colors);

2) prohibition of storing authorization data in the browser memory;

3) masking of input secrets;

4) informing the client on the authorization page about the measures to ensure cyber hygiene that are recommended to follow when using the web application;

5) handling errors and exceptions in a secure manner, preventing the display of confidential data in the client interface by providing minimally sufficient error information.

68. The mobile application shall ensure:

1) unambiguous identification of the mobile application belonging to the insurance (reinsurance) organization (data in the official application store, logos, corporate colors);

2) blocking of the functionality for the provision of remote services of the insurance (reinsurance) organization in the event of detected signs of integrity breaching and (or) bypassing of the protective mechanisms of the operating system, detection of remote management processes;

3) notification of the client about availability of updates to the mobile application;

4) the ability to force installation of updates to the mobile application or block the functionality of the mobile application before their installation when critical vulnerabilities need to be addressed;

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

6) exclusion of confidential data caching;

7) exclusion of confidential data in clear text from the mobile application backups;

8) informing the client about the methods of ensuring cyber hygiene that are recommended to follow when using the mobile application;

9) informing the client about events of authorization under his account, change and (or) recovery of the password, change of the mobile phone number registered by the insurance company;

10) during cash transactions - transfer to the server software of the insurance (reinsurance) company the geolocation data of the mobile device with the authorization of the client or transfer of information about the absence of such authorization.

69. The insurance (reinsurance) organization shall ensure on its side:

1) handling of errors and exceptions in a secure manner, preventing disclosure of confidential data in the response, providing minimally sufficient information for diagnosing the problem;

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

3) checking data for validity to prevent query spoofing and malware injection attacks.