On approval of uniform requirements in the field of information and communication technologies and information security

Unofficial translation

Decree of the Government of the Republic of Kazakhstan dated December 20, 2016 № 832.

Unofficial translation

In accordance with subparagraph 3) of article 6 of the Law of the Republic of Kazakhstan dated November 24, 2015 On Informatization, the Government of the Republic of Kazakhstan hereby **RESOLVES**:

1. To approve the attached uniform requirements in the field of information and communication technologies and ensuring information security (hereinafter - the uniform requirements).

2. To recognize as invalid some decisions of the Government of the Republic of Kazakhstan in accordance with the appendix to this resolution.

3. This resolution shall be enforced upon expiry of ten calendar days after the date of its first official publication.

Paragraph 140 of the uniform requirements is valid until January 1, 2018.

Prime Minister
of the Republic of Kazakhstan *B. Sagintayev*

Approved By
Order No. 832 of the Government
of the Republic of Kazakhstan
dated December 20, 2016

Uniform requirements in the field of information and communication technologies and information security Chapter 1. General Provisions

1. Unified requirements in the field of information and communication technologies and ensuring information security (hereinafter referred to as UR) have been developed in accordance with subparagraph 3) of Article 6 of the Law of the Republic of Kazakhstan "On Informatization" (hereinafter referred to as the Law) and shall determine the requirements in the field of information and communication technologies and ensuring information security.

Footnote. Paragraph 1 - as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

2. UR provisions related to information security shall be mandatory for application by state bodies, local executive bodies, state legal entities, quasi-public sector entities, owners and holders of non-state information systems, integrated with information systems of state

bodies or intended for the formation of state electronic information resources, also owners and holders of critical information and communication infrastructure facilities.

3. The provisions of the UR shall not apply to:

1) relations arising from the implementation by the National Bank of the Republic of Kazakhstan and organizations that are part of its structure, work on the creation or development, operation of Internet resources, information systems that are not integrated with the objects of the information and communication infrastructure of "electronic government", local area networks and networks telecommunications, as well as procurement of goods, works and services in the field of informatization;

2) secure information systems classified as state secrets in accordance with the legislation of the Republic of Kazakhstan on state secrets, as well as special purpose telecommunications networks and/or presidential, government, classified, encrypted and coded communications;

3) relations arising from the implementation by the authorized body for regulation, control and supervision of the financial market and financial organizations of work on the creation or development of information systems that are integrated with the information systems of the National Bank of the Republic of Kazakhstan, which are not integrated with the objects of the information and communication infrastructure of "electronic government";

4) organizations in cases where the implementation of such provisions leads to a violation of paragraph 4 of Article 50 of the Law of the Republic of Kazakhstan "On banks and banking activities in the Republic of Kazakhstan".

Footnote. Paragraph 3 - as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

4. The purpose of the UR is to establish requirements in the field of information and communication technologies and information security that are binding to state bodies, local authorities, state legal entities, quasi-public sector entities, owners and holders of non-state information systems integrated with information systems of state bodies or intended for the formation of state electronic information resources, also to the owners and holders of critical information and communication infrastructure facilities.

5. The tasks of UR are:

1) determination of the principles of organization and management of the informatization of state bodies for solving current and strategic tasks of public administration;

2) determination of uniform principles for ensuring and managing information security of objects of informatization of "electronic government";

3) establishment of requirements for the unification of the components of information and communication infrastructure facilities;

4) the establishment of requirements for the structuring of the information and communication infrastructure and the organization of server rooms;

5) establishment of the obligation to apply the recommendations of standards in the field of information and communication technologies and information security at all stages of the life cycle of objects of informatization;

6) increasing the level of security of state and non-state electronic information resources, software, information systems and the information and communication infrastructure supporting them.

Footnote. Clause 5 as amended by the Decree of the Government of the Republic of Kazakhstan No. 1047 dated December 31, 2019 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); No. 12 dated January 18, 2021 (shall be enforced upon the expiration of ten calendar days after the day of its first official publication).

6. For the purposes of these URs, the following definitions are used:

1) marking of an asset associated with information processing facilities - the application of symbols, letters, numbers, graphic signs or inscriptions on an asset for its further identification (recognition), the indication of its properties and characteristics;

2) means of cryptographic information protection (hereinafter referred to as MCIP) - software or a hardware-software complex that implements algorithms for cryptographic transformations, generation, formation, distribution or management of encryption keys;

3) assets associated with information processing facilities (hereinafter referred to as Asset) - a tangible or intangible object that is information or contains information, or is used to process, store, transfer information and is of value to the organization in the interests of achieving the goals and continuity of its activities;

4) technical documentation on information security (hereinafter referred to as TD IS) - documentation that establishes policies, rules, and protective measures related to the processes of ensuring IS of informatization objects and (or) organizations;

5) monitoring of information security events (hereinafter referred to as IS events monitoring) - constant monitoring of the informatization object to detect and identify information security events;

6) scalability - the ability of an informatization object to provide the possibility of increasing its performance as the volume of processed information and (or) the number of simultaneously working users grows;

7) software robot - software of a search engine or monitoring system that performs automatically and (or) according to a given schedule browsing web pages, reading and indexing their content, following the links found in web pages;

8) unloaded (cold) redundancy of equipment - the use of additional server and telecommunications equipment, software prepared for operation and in an inactive mode for prompt restoration of an information system or an electronic information resource;

9) loaded (hot) redundancy of equipment - the use of additional (redundant) server and telecommunications equipment, and software and keeping them in active mode to flexibly and

promptly increase the throughput, reliability and fault tolerance of an information system, an electronic information resource;

10) workstation - a stationary computer as part of a local area network, designed to solve applied tasks;

11) system software - a set of software to ensure the operation of computing equipment;

12) Internet browser - application software designed to visually display the content of Internet resources and interactively interact with it;

13) encrypted communication - secure communication using documents and coding techniques;

14) multi-factor authentication - a method of user authentication using a combination of various parameters, including the generation and input of passwords or authentication features (digital certificates, tokens, smart cards, one-time password generators and biometric identification tools);

15) cross room - a telecommunications room designed to accommodate connecting, distribution points and devices;

16) application software (hereinafter referred to as AS) - a software package for solving an applied problem of a certain class of subject area;

17) classified communication - secure communication using classified equipment;

18) server center of state bodies (hereinafter referred to as the server center of SB) - a server room (data processing center), the owner or owner of which is the operator of the information and communication infrastructure of "electronic government", intended to accommodate objects of informatization of "electronic government";

19) event logging - the process of recording information about software or hardware events occurring with the informatization object in the event log;

20) server room (data processing center) - a room designed to accommodate server, active and passive network (telecommunication) equipment and equipment of structured cable systems;

21) a local area network of an external loop (hereinafter referred to as LAN of an external loop) - a local area network of subjects of informatization, determined by an authorized body, assigned to the outer loop of the telecommunications network of subjects of informatization, having a connection to the Internet, access to which for subjects of informatization is provided by telecom operators only through single gateway access to the Internet;

22) terminal system - a thin or zero client for working with applications in a terminal environment or programs - thin clients in a client-server architecture;

23) time source infrastructure - a hierarchically connected server equipment using a network time synchronization protocol that performs the task of synchronizing the internal clocks of servers, workstations and telecommunications equipment;

24) government communications - special secure communications for the needs of public administration;

25) organization - a state legal entity, a subject of the quasi-public sector, the possessor and owner of non-state information systems integrated with the information systems of state bodies or intended for the formation of state electronic information resources, as well as the possessor and owner of critical information and communication infrastructure facilities;

26) federated identification - a set of technologies that allows using a single user name and authentication identifier to access electronic information resources in systems and networks that have established trust relationships;

27) encrypted communication - secure communication using manual cyphers, encryption machines, linear encryption equipment and special computer equipment;

28) internal loop local area network (hereinafter referred to as internal loop LAN) - a local area network of informatization subjects, determined by the authorized body, related to the inner loop of the telecommunications network of informatization subjects, having a connection with a single transport environment of state bodies;

29) external gateway of "electronic government" (hereinafter referred to as EGEG) - a subsystem of the gateway of "electronic government", designed to ensure the interaction of information systems located in the SB UTE with information systems located outside the SB UTE;

30) internal audit of information security - an objective, documented process of monitoring the qualitative and quantitative characteristics of the current state of information security of informatization objects in an organization, carried out by the organization itself in its interests;

31) firewall - a hardware-software or software complex that operates in the information and communication infrastructure, which monitors and filters network traffic in accordance with specified rules;

32) subjects of informatization, determined by the authorized body - state bodies, their subordinate organizations and LEBs, as well as other subjects of informatization using a single transport environment of state bodies for the interaction of local (except for local area networks with access to the Internet), departmental and corporate networks.

Footnote. Paragraph 6 - as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

6-1. Digitalization of civil defence and LEB as part of digital transformation shall be carried out by creating and developing objects of informatization of "electronic government" or by acquiring objects of informatization of "electronic government" or information and communication services in accordance with the architecture of "electronic government", including taking into account:

1) platforming - the formation and continuous development of interdepartmental centralized technological platforms for the information and communication infrastructure of "

electronic government" and tools for solving common technical problems within various branches (areas) of public administration;

2) universality of solutions - determination and ensuring the use of ready-made software and service software products for solving typical applied problems and automating typical supporting state functions;

3) component building solutions - ensuring the development and implementation of individual standard components of the "electronic government" informatization objects in the format of microservices, which are planned, developed and implemented iteratively, gradually providing parts of the functionality of the entire solution and the benefits of its use;

4) effectiveness - extracting the maximum benefit from the use of "electronic government " informatization objects, reducing costs and risks by optimizing structural components and costs;

5) optimization of technical diversity - ensuring the reasonable use of free software and the systematic management of technical diversity.

Footnote. Paragraph 1 is supplemented by paragraph 6-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

7. For the purposes of these URs, the following abbreviations shall be used:

1) HSC – hardware and software complex;

2) IS - information security;

3) IS - information system;

4) ICI - information and communication infrastructure;

5) ICT - information and communication technologies;

6) SW- software;

7) LEB - local executive bodies;

8) FS –free software;

9) UIAG- unified Internet access gateway;

10) IR – Internet resource;

11) SB - the central executive body, the state body directly subordinate and accountable to the President of the Republic of Kazakhstan, territorial units of the department of the central executive body;

12) SB UTM - unified transport medium of state bodies;

13) SB UPIR – unified platform of Internet resources of state bodies;

14) - excluded by the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

15) EIR - electronic information resources;

16) EG ICP - information and communication platform of "electronic government";

17) EDS - electronic digital signature.

Footnote. Paragraph 7 as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication); dated 10.02.2023 No. 112 (shall be enforced from 01.01.2023).

7-1. Platforming shall be based on the following requirements:

1) implementation of the creation and development of solutions based on the technological platforms of the information and communication infrastructure of "electronic government" and (or) the use of the functionality of the technological platforms of the information and communication infrastructure of "electronic government";

2) exclusion of components that duplicate the functionality of the technological platforms of the information and communication infrastructure of "electronic government";

3) ensuring the automation of the processes of performing state functions and the services arising from them using technological platforms of the information and communication infrastructure of "electronic government".

Footnote. Paragraph 1 is supplemented by paragraph 7-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

Chapter 2. Requirements for organization and management of informatization and information security Paragraph 1. Requirements for informatization of a state body

8. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

8-1. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

8-2. The versatility of solutions shall be based on the fulfillment of the following requirements:

1) the use of ready-made software and service software products for automating the processes of performing typical applied tasks and typical supporting state functions;

2) adaptation of the features of the performance of state functions of a state body to the processes implemented in ready-made software and service software products, without the need to configure and refine the software in the implementation process;

3) the absence of additional costs of state bodies for the implementation, training of users, the purchase of software and components of the information and communication infrastructure when using service software products.

Footnote. Paragraph 2 is supplemented by paragraph 8-2 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

9. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

9-1. Component construction of solutions shall be based on the following requirements:

1) building solutions based on microservice architecture using standard components;

2) the use of the minimum required set of components to solve the tasks and ensure compliance with the requirements;

3) exclusion of redundant components that simultaneously automate unrelated specific state functions and (or) typical providing state functions;

4) ensuring adaptability, scalability and flexibility of the composition, structure and functionality of the components to changes in the legislation of the Republic of Kazakhstan, the priorities of socio-economic development, as well as the composition, structure and powers of state bodies;

5) full compliance of the components with the goals, objectives and purpose of the " electronic government" informatization object;

6) ensuring functional independence and lack of duplication of tasks and functionality of components;

7) the formation of components based on open standards and using a set of standard application programming interfaces (application programming interface, API) provided by the component to third-party solutions to ensure its reuse;

8) multi-level construction of the architecture by excluding the coverage of solution components simultaneously by several levels of architecture, including presentation levels, business logic and data storage;

9) ensuring the availability of components for revision and reuse.

Footnote. Paragraph 2 is supplemented by paragraph 9-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

10. Development of the "electronic government" architecture shall be carried out in accordance with the requirements for development of architecture of "electronic government" approved by the authorized body in accordance with subparagraph 10) of article 7 of the Law.

10-1. Efficiency shall be based on the fulfillment of the following requirements:

1) ensuring the maximum quantitative economic effect by reducing costs, ensuring payback and increasing the volume of budget receipts;

2) focus on meeting the needs of individuals and legal entities, the industry (sphere) of public administration and (or) the state as a whole;

3) ensuring the consistency of values and units of measurement of indicators of the results of the functioning of objects of informatization of "electronic government" and target indicators of the industry (sphere) of public administration;

4) ensuring the priority of automation of the processes of performing specific state functions;

5) sequential iterative creation and development of solutions by introducing part of the solution components with a basic set of functionality, followed by expanding the number of components and (or) increasing the level of their functionality.

Footnote. Paragraph 2 is supplemented by paragraph 10-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

11. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

11-1. Optimization of technical diversity shall be based on the fulfillment of the following requirements:

1) alienability and independence from the names and versions of software, as well as restrictions on the components of the existing information and communication infrastructure of the state body;

2) ensuring optimization of the diversity of existing software and simplification of the existing information and communication infrastructure of the state body;

3) exclusion of restrictions for further development as a result of changing operating conditions and expanding the number of automation objects;

4) ensuring the use of up-to-date software versions;

5) implementation of the creation and development of solutions using free software in cases of ensuring the ability of the components of the solution to function without restrictions and the optimal total cost of ownership concerning proprietary licensed software.

Footnote. Paragraph 2 is supplemented by paragraph 11-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

12. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

13. Provision of SB and local authorities with goods, works, services in the field of informatization shall be carried out by procurement, taking into account the conclusion of the authorized body in the field of informatization on the calculations of expenses for public procurement of goods, works and services in the field of informatization submitted by the administrators of budget programs.

Footnote. Paragraph 13 - as amended by the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

13-1. SB and organizations shall place on the architectural portal of "electronic government" information about informatization objects and electronic copies of technical documentation for them in accordance with the rules for recording information about informatization objects of "electronic government" and placing electronic copies of technical documentation of informatization objects of "electronic government".

The list of technical documentation for the informatization object required for placement shall be determined by the Rules for recording information about the "electronic government" informatization objects and placing electronic copies of the technical documentation for the " electronic government" informatization objects.

Footnote. Paragraph 2 is supplemented by paragraph 13-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

14. Informatization tasks in the SB or LEB shall be implemented by the information technology unit, which shall:

1) monitor and analyze the ICT use;

2) participate in accounting and analysis of the ICT assets use;

3) develop proposals to the SB strategic plan on informatization;

4) coordinate works on the creation, maintenance and development of the "electronic government" software;

5) control the provision by suppliers of the quality of informatization services stipulated by the agreements;

6) registration and updating of information about objects of informatization of "electronic government" and electronic copies of technical documentation of objects of informatization of "electronic government" on the architectural portal of "electronic government";

7) transfer to the service integrator of "electronic government" for accounting and storage of the developed software, source program codes (if any), a set of settings for licensed software of objects of informatization of "electronic government";

8) excluded by the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

9) fulfill requirements for information security.

Footnote. Clause 14 as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); dated 10.02.2023 No. 112 (shall be enforced from 01.01.2023).

14-1. Owners and (or) possessors from the moment of putting into commercial operation the object of informatization of "electronic government" shall ensure the transfer to the operator for accounting and storage of all versions of the developed software, source code (if any), a set of settings for licensed software of objects of informatization of "electronic government" in accordance with the Rules for accounting and storage of developed software, source program codes (if any), a set of settings for licensed software of "electronic government" informatization objects, approved by the authorized body in accordance with subparagraph 31) of Article 7 of the Law.

Footnote. Paragraph 2 is supplemented by paragraph 14-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

15. The workspace in SB and MPR is organized in accordance with the sanitary rules " Sanitary and Epidemiological Requirements for Administrative and Residential Buildings" approved by the authorized body in the field of sanitary and epidemiological welfare of the population in accordance with paragraph 6 of Article 144 of the Code of the Republic of Kazakhstan dated September 18, 2009 year "On the health of the people and the health care system."

Footnote. Clause 15 as amended by the Decree of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after its first official publication).

16. The workplace of a SB and LEB servant shall be equipped with regard to his functional responsibilities and comprise:

1) a workstation or a unified workstation or terminal system connected to the LAN internal circuit of the SB or LEB. It shall be allowed to equip the workplace with an extra monitor if necessary;

2) a set of multimedia equipment (headphones, microphone and webcam) for working with multimedia EIR or video conferencing system, if necessary;

3) telephone or IP telephony device.

17. Requirements for a unified workplace or terminal system of SB and LEB, as well as components of information and communication infrastructure facilities shall be approved by the authorized body.

Footnote. Paragraph 17 - as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

17-1. Compliance of the workplace or terminal system of SB and LEB with the requirements for a unified workplace or terminal system of SB and LEB, approved by the authorized body, is ensured.

Requirements are updated and updated as needed.

Footnote. The unified requirements are supplemented by paragraph 17-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

18. When choosing models of procured workstations, the following rules shall be complied with:

1) the hardware characteristics of workstations meeting or exceeding the system requirements recommended by the developer (manufacturer) of the software used;

2) workstation configurations are unified to ensure general level of services;

3) centralized automated distribution of software updates is organized for workstations;

4) to improve the quality and speed of administration, the number of different hardware-software configurations of workstations is reduced to three types:

workstation for working with application software;

high-power workstation for working with graphic packages, modeling software packages and others, used for applications with developed graphics, high requirements for processor performance, random access memory (RAM) and video subsystems amount;

laptop for mobile users.

19. For specification of technical requirements, the following key parameters of workstations shall be distinguished:

1) performance, including:

processor fast performance parameters;

the necessary amount of RAM;

Internal data bus speed;

graphics subsystem performance;

performance of input / output devices;

monitor matrix parameters;

2) reliability provided through the use of fault-tolerant hardware and software, determined basing on the average no failure operating time;

3) scalability provided by the architecture and design of the personal computer due to the possibility of increasing:

processor numbers and performance;

RAM and external memory volumes;

capacity of internal drives.

20. To ensure information security:

1) the technical documentation on information security shall define:

ways of placing workstations of SB and LEB servants;

ways to protect workstations against failures in the power supply system and other breaches caused by failures in the utilities;

procedures and frequency of workstations maintenance to ensure continuous accessibility and integrity;

ways to protect the workstations of mobile users outside the SB or LEB, factoring in various external risks;

methods for guaranteed destruction of information during reuse of workstations or decommissioning of data storage media;

rules for moving workstations outside the workplace;

2) accounting of workstations shall be carried out regularly with a configuration check, as well as electronic storage media with unique identifying data;

3) installation and use at the workstations of remote control software or hardware outside the internal LAN circuit shall be excluded. Remote control inside the LAN internal circuit shall be allowed in cases explicitly provided for in the SB or LEB legal act;

4) unused input-output ports of workstations and mobile computers of SB and LEB servants shall be disabled or blocked, with the exception of workstations of IS unit staff.

Footnote. Clause 20 as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

21. The issue of input-output operations with the use of external electronic data storage media at the workstations of SB and LEB servants shall be regulated in accordance with the IS policy adopted by the SB or LEB.

22. To optimize equipment placement at the SB and LEB servant's work station, the use of specialized equipment shall be permitted that ensures the use of one unit of a monitor, a manual manipulator (mouse) and a keyboard for several workstations, without using network interfaces.

23. To use the services of the EG ICP, the workstation connected to the internal circuit LAN of the SB or LEB shall be provided with a network connection to the EG ICP infrastructure.

24. Processing and storage of service information of the HE and LEB are carried out at workstations connected to the local area network of the internal loop and the external loop of the SB or LEB.

Service information of SB and LEB with limited access shall be processed at workstations connected to the local area network of the internal loop of SB or LEB and not having an Internet connection.

Footnote. Paragraph 24 as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

25. Access to the Internet for SB and LEB shall be provided from workstations connected to the LAN of the external circuit of SB and LEB, located outside the sensitive premises, determined in accordance with the Instruction on the protection of state secrets of the Republic of Kazakhstan.

Footnote. Paragraph 25 as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

25-1. When organizing access to the Internet from local area networks of the external circuit, availability of anti-virus tools and updates of the operating systems at workstations connected to the Internet is mandatory.

Footnote. Chapter 2 was supplemented with clause 25-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 06/18/2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

26. Telephone service:

1) shall be both based on digital telephone networks for general use, and IP-telephony technology;

2) shall provide user switching with telephone network subscribers via the following channels:

the use of subscriber connections through the existing local network of internal and external circuits and departmental data transmission network;

the use of communication services of public telephony operator on the E1 stream;

the use of mobile operators;

the use of long-distance and international call services.

27. For conferences, presentations, meetings, teleconference bridges, the SB and LEB conference room shall be equipped with:

1) sound amplification conference system, with a microphone, loudspeaker at the participant's place, and light indicator of the participant's request and presentation.

2) information input-output device.

To organize a teleconference with geographically distributed participants who are in other cities or countries, the conference system can be optionally supplemented by the audio and video conferencing system of the EG ICI operator.

28. Printing service:

1) is implemented by means of printing, copying and scanning equipment connected to the local network of the SB internal circuit using a network interface or direct connection to the print server;

2) is provided by software that carries out:

centralized user and device management;

accounting of printed documents, copies, e-mailed faxes and scans by user identification numbers with the possibility of distributing costs between departments and users;

a system of reports graphically illustrating print, copy, and scan activity;

user identification before the print service use;

authorization of the SB servant on the printing device in the ways regulated in the IS technical documentation;

forming a print queue that prints using a single print queue with the ability to receive printed documents on an available print device.

Paragraph 2. Requirements for information security organization

29. When organizing, providing and managing information security in SB, LEB or organization, it shall be necessary to be guided by the provisions of the standard of the

Republic of Kazakhstan ST RK ISO/IEC 27002-2015 "Information technology. Methods and means of ensuring security. Code of rules for information security management tools".

Footnote. Paragraph 29 - as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

29-1. To implement the requirements for ensuring information security for the defense of the country and the security of the state, software and products of the electronic industry shall be purchased in the form of goods and information and communication services from the register of trusted software and products of the electronic industry in accordance with the Law and legislation of the Republic of Kazakhstan on public procurement, procurement individual subjects of the quasi-public sector.

The register of trusted software and products of the electronic industry shall be maintained by the authorized body in the field of electronic industry in accordance with the Rules for the formation and maintenance of the register of trusted software and products of the electronic industry, as well as the criteria for including software and products of the electronic industry in the register of trusted software and electronic products industry, approved by the authorized body in the field of electronic industry in accordance with paragraph 7 of Article 7-6 of the Law.

Therewith, in the absence of the necessary products in the register of trusted software and products of the electronic industry, it shall be allowed to purchase them in accordance with the legislation of the Republic of Kazakhstan on public procurement, and procurement of individual entities of the quasi-public sector.

Owners and possessors of software included in the register of trusted software and products of the electronics industry shall ensure the transfer of source program codes to the operator for accounting and storage.

Footnote. The unified requirements were supplemented by paragraph 29-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

30. To delineate responsibilities and functions in the field of IS maintenance, an IS subdivision shall be created, which is a structural subdivision, separate from other structural subdivisions involved in the creation, maintenance and development of informatization objects, or an official responsible for ensuring IS shall be determined.

Employees responsible for ensuring information security shall take specialized courses in the field of information security at least once every three years with the issuance of a certificate.

Footnote. Paragraph 30 - as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

31. TD IS is created in the form of a four-level system of documented rules, procedures, practices or guidelines, which are guided by the SB, MPR or organization in their activities.

TD IS is developed in Kazakh and Russian languages, approved by a legal act of the SB, MPR organization and is communicated to all employees of the SB, MPR or employees of the organization.

TD IS is revised in order to analyze and update the information contained in them at least once every two years.

Footnote. Clause 31 as amended by the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

32. The IS policy of the SB, LEB or organization is a first-level document and it shall define goals, objectives, guidelines and practical methods in the field of IS maintenance.

32-1. The list of internal documents of a financial organization detailing the requirements of the IS policy shall be determined in accordance with the regulatory legal acts of the authorized body for regulation, control and supervision of the financial market and financial organizations that regulate the activities of financial organizations to ensure information security.

Footnote. The unified requirements are supplemented by paragraph 32-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated January 18, 2021 No . 12 (shall be enforced ten calendar days after the day of its first official publication).

33. The list of the second level documents shall comprise the documents detailing the requirements of the IS policy of SB, LEB, or organization, including:

1) methodology for assessing information security risks;

2) rules of identification, classification and labeling of assets associated with information processing facilities;

3) rules of ensuring continuous operation of assets relating to information processing facilities;

4) rules of inventory and certification of the hardware, telecommunications equipment and software;

5) rules of conducting IS internal audit;

6) rules of using data encryption tools;

7) rules of differentiation of access rights to electronic information resources;

8) rules of using Internet and email;

9) rules of organizing authentication procedure;

10) rules of organizing anti-virus control;

11) rules of using mobile devices and data storage media;

12) rules of organizing safeguards of information processing facilities and safe environment for the information resources operation.

34. Third level documents shall contain description of the processes and procedures for ensuring information security, including:

1) a catalog of IS threats (risks);

2) action plan on processing the IS threats (risks);

3) regulations on the information backup and recovery;

4) action plan on ensuring continuous operation and restoration of the operability of assets associated with information processing facilities;

5) the administrator's guide on maintenance of the informatization object;

6) instruction on the procedure for users to respond to IS incidents and emergency (crisis) situations.

35. The list of documents of the fourth level includes working forms, journals, applications, protocols and other documents, including electronic ones, used for registration and confirmation of the procedures and works performed, including:

1) a log of information security incidents and accounting for emergency situations;

2) a log of visiting server rooms;

3) report on the assessment of the vulnerability of network resources;

4) cable connection log;

5) journal of accounting of backups (backup, recovery), testing of backups;

6) a logbook for recording changes in the configuration of equipment, testing and recording changes in PPS and FPP, registration and elimination of software vulnerabilities ;

7) test log of diesel generator sets and uninterruptible power supplies for the server room;

8) log of testing systems for providing microclimate, video surveillance, fire extinguishing server rooms.

Footnote. Clause 35 as amended by the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

36. To ensure the assets security, the following actions shall be taken:

1) inventory of assets;

2) classification and labeling of assets in accordance with the classification system adopted by the SB or LEB;

3) assignment of assets to servants and defining the range of their responsibilities in the IS assets management;

4) regimentation in the IS TD of:

the use and return of assets;

identification, classification and labeling of assets.

37. In order to manage risks in the field of ICT in a civil society or MPR the following is carried out:

1) selection of a risk assessment methodology in accordance with the recommendations of the standard of the Republic of Kazakhstan ST RK 31010-2010 "Risk management. Risk assessment methods" and development of a risk analysis procedure;

2) identification of risks in relation to the list of identified and classified assets, including:

identification of IS threats and their sources;

identification of vulnerabilities that can lead to the implementation of threats;

identification of information leakage channels;

formation of a model of the intruder;

3) selection of criteria for accepting identified risks;

4) formation of a catalogue of IS threats (risks), including assessment (reassessment) of identified risks in accordance with the requirements of the Republic of Kazakhstan ST RK ISO/IEC 27005-2013 "Information technologies. Security methods. Information security risk management";

5) development and approval of a plan for processing IS threats (risks), containing measures to neutralize or reduce them.

Footnote. Clause 37 as amended by the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); No. 12 dated January 18, 2021 (shall be enforced upon the expiration of ten calendar days after the day of its first official publication).

38. In order to control the events of information security violations in an SB, MPR or organization:

1) monitoring of events related to IS violation and analysis of monitoring results;

2) events related to the state of information security are recorded, and violations are identified by analyzing the event logs, including:

operating system event logs;

event logs of database management systems;

anti-virus protection event logs;

application software event logs;

event logs of telecommunication equipment;

event logs of systems for detecting and preventing attacks;

content management system event logs;

3) synchronization of the time of event logs with the infrastructure of the time source is provided;

4) event logs are stored for the period specified in the IS TD, but not less than three years and are available online for at least two months;

5) logs of events are kept in accordance with the formats and types of records defined in the rules for monitoring information security of objects of informatization of "electronic

government" and critical objects of information and communication infrastructure, approved by the authorized body in the field of information security in agreement with the national authorities safety in accordance with subparagraph 7) of Article 7-1 of the Law;

6) provides protection of event logs from interference and unauthorized access. System administrators are not allowed to have the authority to modify, delete, or disable logs. For confidential IS, the creation and maintenance of a backup storage of logs is required;

7) implementation of a formalized procedure for informing about information security incidents and responding to IS incidents is ensured.

Footnote. Clause 38 as amended by the decrees of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); dated 31.12.2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

39. To protect critical processes of SB, LEB or organizations against internal and external threats:

1) an action plan shall be developed, tested and implemented to ensure continuous operation and restoration of the operability of assets associated with information processing facilities;

2) instruction shall be communicated to the SB and LEB or organization servants on the procedure for users to respond to IS incidents and in emergency (crisis) situations.

The action plan for ensuring continuous operation and restoring operability of assets associated with information processing facilities shall be regularly updated.

40. The functional responsibilities for ensuring IS and obligations to fulfill the requirements of the IS TD for SB and LEB or organization’s servants shall be included in their work descriptions and (or) the employment contract terms.

Obligations in the IS maintenance, which are in force after termination of the employment contract, shall be fixed in the labor contract of the SB and LEB or organization’s servants.

41. In the event of involving third-party organizations in maintaining the information security of EIR, information systems, ICI, their owner or holder shall enter into agreements that establish conditions for the operation, access or use of these facilities, and also liability for their violation.

42. Content of the procedures in dismissal of the SB and LEB or organization’s servants who have obligations in the field of IS maintenance, shall be defined in the IS TD.

43. Upon dismissal or amending the terms of the employment contract, the right of access of an employee of the SB, MPR or an employee of the organization to information and information processing facilities, including physical and logical access, access identifiers, subscriptions, documentation that identifies him as an active employee of the SB, MPR or an employee of the organization, are canceled after the termination of his employment contract or are changed when changes are made to the terms of the employment contract.

Footnote. Clause 43 as amended by the Resolution of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

44. The human resources service shall organize and maintain records on the SB and LEB or organization's servant's training in the field of informatization and IS maintenance.

45. When initiating the creation or development of informatization objects of the first and second classes in accordance with the classifier of informatization objects approved by the authorized body in the field of informatization in accordance with subparagraph 11) of Article 7 of the Law (hereinafter referred to as the Classifier), as well as confidential IS, protection profiles shall be developed for composite components and security task in accordance with the requirements of the Republic of Kazakhstan ST RK ISO/IEC 15408-2017 "Information technology. Security methods and means. Criteria for assessing information technology security".

Footnote. Paragraph 45 - as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

46. In order to ensure IS during the operation of informatization objects, requirements are established for:

1) methods of authentication;

2) applied ISC;

3) ways to ensure availability and fault tolerance;

4) monitoring of information security, protection and safe operation;

5) the use of information security tools and systems;

6) registration certificates of certification centers.

Footnote. Clause 46 as amended by the Resolution of the Government of the Republic of Kazakhstan dated 06/18/2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

46-1. For signing, the objects of informatization of "electronic government" use registration certificates of accredited certification centers in accordance with the Rules for issuing and revoking a certificate of accreditation of certification centers, approved by the authorized body in accordance with subparagraph 2) of paragraph 3 of Article 5 of the Law of the Republic of Kazakhstan "On electronic document and electronic digital signatures".

Footnote. Paragraph 2 is supplemented by paragraph 46-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

47. When accessing objects of informatization of the first and second classes, in accordance with the classifier, multifactor authentication is applied, including using EDS.

Footnote. Clause 47 as amended by the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

48. To protect the restricted service information, confidential information systems, confidential EIR and the EIR containing personal data of limited access, data encryption tools (software or hardware) shall be applied with parameters meeting the requirements of the cryptographic information protection system in accordance with the standard of the Republic of Kazakhstan ST RK 1073-2007 Means of Cryptographic Protection of Information. General Technical Requirements for Informatization objects of:

first class in accordance with the classifier - the third level of security;

second class in accordance with the classifier - the second level of security;

third class in accordance with the classifier - the first level of security.

49. To ensure availability and fault tolerance, the owners of EG informatization objects shall provide:

1) own or leased backup server room for EG informatization objects of the first and second classes in accordance with the classifier;

2) backup of hardware and software for data processing, data storage systems, components of data storage networks and data transmission channels, including for EG informatization objects of:

first class in accordance with the classifier - loaded (hot) in the backup server room;

second class, in accordance with the classifier - not loaded (cold) in the backup server room;

third class in accordance with the classifier - storage in a warehouse close to the main server room.

49-1. The integration of "electronic government" informatization objects shall be carried out in accordance with the Rules for the integration of "electronic government" informatization objects, approved by the authorized body in accordance with subparagraph 13) of Article 7 of the Law, and subject to the information security requirements determined by the protection profile and drawn up by the contract of joint work on information security of the state and non-state information systems, and shall be based on ensuring:

1) a unified integration environment - ensuring the technological possibility of interdepartmental and departmental information interaction of informatization objects;

2) one-time integration - ensuring a single connection of objects of informatization of " electronic government" to the system of interaction and subsequent repeated use to minimize financial and time costs in the transfer and receipt of information;

3) a single information space - ensuring the compatibility and comparability of data during transmission based on the use of standard data transmission formats.

Footnote. Paragraph 2 is supplemented by paragraph 49-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

50. EG informatization objects of the first and second classes in accordance with the classifier shall be connected to the system of IS monitoring, protection and safe operation no later than one year after they are put into operation.

50-1. Owners or possessors of non-state information systems intended for the formation of state electronic information resources, the implementation of state functions and the provision of public services, before integrating with information systems of state bodies, shall create their operational information security center and shall ensure its functioning or purchase the services of an operational information security center from third parties in accordance with the Civil Code of the Republic of Kazakhstan, and also ensure its interaction with the National Coordinating Center for Information Security.

The owners of critically important information and communication infrastructure facilities shall create their operational information security center and ensure its operation or purchase the services of an operational information security center from third parties in accordance with the Civil Code of the Republic of Kazakhstan.

Owners or possessors of critically important information and communication infrastructure facilities, with the exception of state bodies, LEBs, state legal entities, quasi-public sector entities, within a year from the date of inclusion in the list of critically important information and communication infrastructure facilities, shall create their own operational information security center and shall ensure its functioning or acquire the services of the operational information security center from third parties in accordance with the Civil Code of the Republic of Kazakhstan, and shall also ensure its interaction with the National Information Security Coordination Center.

Footnote. The unified requirements are supplemented by paragraph 50-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication); as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

50-2. A unified integration environment shall be based on the following requirements:

1) implementation of integration into a single integration environment in accordance with a service-oriented architecture;

2) implementation of interstate information interaction of informatization objects of several states through the national gateway of the Republic of Kazakhstan;

3) implementation of the creation, modification and deletion of data by interfacing them with the relevant processes for the implementation of public functions and the provision of public services initiated by the owners of the data or on their behalf;

4) the use of uniform approaches and standards in ensuring the unambiguous identification of the interacting parties and the scope of their rights in the course of interaction ;

5) priority implementation of synchronous interaction between the objects of informatization of "electronic government";

6) ensuring the use of information from the repository of electronic documents and a unified system of regulatory and reference information of the "electronic government" gateway in the process of information interaction and the provision of public services;

7) ensuring fixation of the date, time, content and participants of all actions and operations carried out within the framework of information interaction, as well as information that allows restoring the history of information interaction;

8) providing technical feasibility for access to data stored in organizations;

9) ensuring the legitimacy and integrity of information interaction by signing the request and transmitted EDS data.

Footnote. Paragraph 2 is supplemented by paragraph 50-2 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

51. SB, MPR or organization monitors:

actions of users and staff;

use of information processing facilities.

Footnote. Clause 51 as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

51-1. One-time integration shall be based on the following requirements:

1) integration and provision of access to the functionality and EIR (data) of informatization objects based on a set of universal information interaction services published on the e-government gateway;

2) ensuring the reuse of information interaction services by including them in the register of services of the "electronic government" gateway;

3) ensuring the creation of information interaction services based on standard technologies , formats and data transfer protocols used in the Republic of Kazakhstan;

4) distribution of data through a single virtual data source with access rights management for information recipients;

5) implementation of the development of a new service of information interaction in cases of absence of a similar or similar service in the register of services of the "electronic government" gateway;

6) providing technical feasibility for the formation of composite services based on information interaction services;

7) ensuring the operability of the "electronic government" gateway, regardless of ongoing technical, administrative, organizational and other changes in the "electronic government" informatization objects connected to the "electronic government" gateway;

8) ensuring the possibility of independent development of the object of informatization of the "electronic government" of the information provider without the need to refine all related consumers of information by ensuring the invariance of the interfaces of the information exchange service.

Footnote. Paragraph 2 is supplemented by paragraph 51-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

52. In SB, MPR or organization in the framework of monitoring the actions of users and personnel:

1) when detecting abnormal activity and malicious actions of users, these actions:

the administrator is registered, blocked and promptly notified for the objects of informatization of the first class ES in accordance with the classifier;

registered and blocked for objects of informatization of electronic signatures of the second class in accordance with the classifier;

are registered for objects of informatization of electronic signatures of the third class in accordance with the classifier;

2) the actions of the maintenance personnel are recorded and controlled by the IS department.

Footnote. Clause 52 as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

52-1. The unified information space shall be based on compliance with data management requirements, including taking into account the requirements for:

1) ensuring data compatibility in the process of information interaction by syntactic, semantic and spatial correspondence of the transmitted data and interfaces of information interaction services;

2) ensuring the distribution of a certain type of data by using reference sources of information and comparing them in the case of using data from several sources;

3) unambiguous and unique identification of the disseminated data;

4) distribution of publicly available data in a structured, machine-readable and linked format through an open data portal;

5) ensuring the possibility of confirming the reliability and relevance of data, identifying inaccurate data, as well as informing interested participants in information interaction about cases of identifying inaccurate data and changes made in the process of updating it;

6) the use of a single scheme for converting data from the data format of the information consumer to the data format of the information provider when interacting with the objects of informatization of the "electronic government" using the "electronic government" gateway.

Footnote. Paragraph 2 is supplemented by paragraph 52-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

53. IS events identified as critical for confidentiality, accessibility and integrity, according to the information security events monitoring and event log analysis:

1) shall be defined as IS incidents;

2) shall be accounted for in the catalog of information security threats (risks);

3) shall be registered in the computer incident response service of the state technical service.

53-1. If the IS has the function of signing electronic documents, the IS user shall be allowed to upload an electronic document from the IS, both signed by the user's EDS, and other electronic documents available to him, along with all the EDS that certify such electronic documents, to get the IS user the ability to verify the authenticity of the electronic document without using this IP in other ways available to them.

Footnote. Paragraph 2 is supplemented by paragraph 53-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

53-2. If the IS has the function of signing electronic documents, the IS user shall be allowed to upload a previously signed electronic document to the IS along with all the digital signatures that certify such an electronic document, including if such an electronic document was signed without using this IS.

Footnote. Paragraph 2 is supplemented by paragraph 53-2 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

53-3. If the IS has the function of working with electronic documents, the IS shall check the powers of the person who signed the document in accordance with the Rules for verifying the authenticity of an electronic digital signature, approved by the authorized body in accordance with subparagraph 10) of paragraph 1 of Article 5 of the Law of the Republic of Kazakhstan "On electronic document and electronic digital signature".

Footnote. Paragraph 2 is supplemented by paragraph 53-3 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

53-4. If the IS has the function of working with electronic documents, the IS must store electronic documents unchanged along with all the EDS with which they are certified, time

stamps and information about the status of checking registration certificates for revocation (cancellation) at the time of signing during the entire period of storage of the electronic document in IS.

Footnote. Paragraph 2 is supplemented by paragraph 53-4 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

53-5. If the IS has the function of working with electronic documents, the IS must support work with all types of EDS key stores supported by certification centers with which this IS works.

Footnote. Paragraph 2 is supplemented by paragraph 53-5 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

54. At the stage of pilot and industrial operation of informatization objects, the following tools and systems shall be used:

detection and prevention of malicious code;

monitoring and management of information security incidents and events;

intrusion detection and prevention;

monitoring and management of information infrastructure.

Footnote. Paragraph 54 - as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

54-1. Data leakage prevention systems (DLP) shall be used to protect the objects of informatization of SB, LEB and critically important objects of information and communication infrastructure.

This shall provide:

visual notification of the user about the ongoing control of actions;

placement of the control center and servers of the data leakage prevention system within the local area network.

Footnote. Paragraph 2 is supplemented by paragraph 54-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced ten calendar days after the day of its first official publication); as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

55. The registration certificates of the Root Certification Authority of the Republic of Kazakhstan are subject to recognition in trusted lists of software products of world software manufacturers for authentication purposes in accordance with the standards of ST RK ISO / IEC 14888-1-2006 Information Technology. Information Protection Methods. Digital Signatures with Appendix. Part 1. General Provisions, ST RK ISO / IEC 14888-3-2006, Information Technology. Security Techniques, Digital Signatures with Appendix. Part 3.

Certificate-Based Mechanisms, GOST R ISO / IEC 9594-8-98, Information Technology. Open Systems Interconnection. The directory. Part 8: Authentication Framework.

56. Certification authorities of the Republic of Kazakhstan, excepting the Root Certification Authority of the Republic of Kazakhstan, are recognized in trusted lists of software products of world software manufacturers by accreditation of the certification authority in accordance with the rules of accreditation of certification authorities.

Certification authorities of the Republic of Kazakhstan shall place their registration certificate with a trusted third party of the Republic of Kazakhstan to ensure verification of EDS of the citizens of the Republic of Kazakhstan in foreign countries.

56-1. The owner of critically important objects of information and communication infrastructure, which processes data containing secrets protected by law, shall conduct an information security audit at least once a year. The information security audit of second-tier banks shall be carried out in accordance with the requirements of the banking legislation of the Republic of Kazakhstan.

Footnote. The unified requirements are supplemented by paragraph 56-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated January 18, 2021 No . 12 (shall be enforced ten calendar days after the day of its first official publication).

Chapter 3. Requirements for informatization objects Paragraph 1. Requirements for electronic information resources and Internet resources

57. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

58. Requirements for creation or development of IR shall be defined in the technical specification for the acquisition of goods, works and services in the field of informatization.

59. The owner and (or) holder of the IR shall provide creation of publicly available IR in the Kazakh, Russian and, if necessary, in other languages, with the possibility for the user to choose the interface language.

60. Creation or development of IR shall be carried out with regard to requirements of the standards of the Republic of Kazakhstan ST RK 2190-2012 Information Technologies. Web Sites of State Bodies and Organizations. Requirements, ST RK 2191-2012 Information Technologies. Availability of Internet for Physically Challenged People, ST RK 2192-2012 Information technologies. Web Site, Web Portal, Intranet Portal. General Descriptions, ST RK 2193-2012 Information Technologies. Recommended Practice of Development of Portable Web-Applications, ST RK 2199- 2012 Information Technologies. Safety Requirements for Web-based Applications in State Bodies.

61. Preparation, placement, updating of EIR on the IR of SB or LEB shall be carried out in accordance with the rules of content and requirements for the maintenance of IR of the SB, approved by the authorized body.

62. The IR of the central executive body, structural and territorial units of the central executive body, local executive body shall be placed on the SB UPIR and registered with the gov.kz and мем.қаз. domain zones.

SB UPIR shall be placed on the EG ICP.

62-1. An Internet resource with a registered.KZ and (or) .ҚАЗ domain name shall be hosted on a hardware and software complex located on the territory of the Republic of Kazakhstan.

Footnote. The unified requirements are supplemented by paragraph 62-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated January 18, 2021 No . 12 (shall be enforced ten calendar days after the day of its first official publication).

62-2. The use of .KZ and (or) .ҚАЗ domain names in the space of the Kazakhstan segment of the Internet when transmitting data by Internet resources shall be carried out using security certificates.

Footnote. The unified requirements are supplemented by paragraph 62-2 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

63. IR management, placement and updating of EIR of the central executive body, structural and territorial units of the central executive body, local executive body shall be carried out from the external circuit of the EG ICI local network by the operator on the basis of a request from the owner and (or) holder of the IR.

63-1. Industrial operation of IR SB and MPR is allowed provided there is an act with a positive test result for compliance with information security requirements.

Footnote. Chapter 3 was supplemented with clause 63-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

64. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

65. In case of non-use of the EIR, the SB or LEB shall ensure its transfer to the archive in the manner prescribed by the Law of the Republic of Kazakhstan "On the National Archival Fund and Archives" (hereinafter referred to as the Law on Archives).

Footnote. Paragraph 65 as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

66. To ensure IS of IR, the following actions shall be applied:

1) registration of certificates for authentication of the domain name and cryptographic protection of the contents of the communication session with the use of DET;

2) content management system (content), performing:

authorization of operations of EIR placement, change and deletion;

registration of authorship when placing, changing and deleting EIR;

checking of downloaded EIR for malware;

security audit of executable code and scripts;

integrity control of the placed EIR;

maintaining of a log of EIR changes;

monitoring of anomalies in users and software robots activity.

Paragraph 2. Requirements for developed or acquired application software

67. At the stage of initiating creation or development of application software (AS), the software class shall be determined and recorded in the project documentation in accordance with the rules for classifying informatization objects and informatization objects classifier, approved by the authorized body in accordance with subparagraph 11) of article 7 of the Law.

68. Requirements for the created or developed IP application software are determined in the terms of reference created in accordance with the requirements of the standard of the Republic of Kazakhstan ST RK 34.015-2002 “Information technology. Set of standards for automated systems. Terms of reference for the creation of an automated system ", these ET and the rules for the preparation and consideration of technical specifications for the creation and development of objects of informatization of" electronic government ", approved by the authorized body in the field of information security in accordance with subparagraph 20) of Article 7 of the Law.

Footnote. Clause 68 as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

69. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

69-1. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

70. Requirements for AS that is being acquired shall be defined in the technical specifications for the purchase of goods, works and services in informatization area, with regard to requirements of these UR.

71. In the purchase of off-the-shelf AS the priority of free software (FS) shall be taken into account, provided that its characteristics are identical with commercial software.

72. When forming requirements for development or acquisition of software, the EIR class and information of the EIR catalog shall be taken into account.

73. Developed or acquired off-the-shelf AS shall:

1) provide a user interface, input, processing and output of data in Kazakh, Russian and other languages, if necessary, with the possibility to select a user interface language;

2) take into account the requirements such as:

reliability;

maintainability;

ease of use;

effectiveness;

universality;

functionality;

cross-platform operation;

3) provide full-functional virtualization technology support;

4) support clustering;

5) shall be provided with technical documentation for operation in the Kazakh and Russian languages.

74. Creation and development or acquisition of software is provided with technical support and maintenance.

Planning, implementation and documentation of technical support and software maintenance are carried out in accordance with the specifications of the manufacturer, supplier or the requirements of the IS TD.

Footnote. Clause 74 as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

75. The process of creating and developing application software:

1) provides:

creation of an information base of algorithms, source codes and software;

testing and testing of software modules;

typification of algorithms, programs and information security tools that ensure information, technological and software compatibility;

use of licensed development tools;

2) includes procedures for acceptance of applied software, providing for:

the transfer by the developer of the source codes of programs and other objects necessary for the creation of application software to the owner and (or) the owner;

control compilation of the transferred source texts, with the creation of a fully functional version of the application software;

running a test case on a given version of the software.

Footnote. Clause 75 as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

76. Control over authorized changes to the software and access rights to it is carried out with the participation of employees of the department of information technology SB, MPR or organizations.

Footnote. Clause 76 as amended by the Decree of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

77. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

78. In order to ensure IS:

1) at the software development stage, recommendations shall be taken into account of the standard of the Republic of Kazakhstan ST RK GOST R 50739-2006 Computers Technique. Information Protection against Unauthorised Access to Information. General Technical Requirements;

2) requirements for the AS that is being developed or acquired shall include the use of tools such as:

identification and authentication of users, if necessary, EDS and registration certificates;

access control;

integrity control;

logging of user actions that affect information security;

online transaction protection;

cryptographic protection of information using DET of confidential information systems in storage, processing;

logging of critical software events;

3) IS TD shall determine and apply during operation:

rules for installing, updating and deleting software on servers and workstations;

management procedures of change and analysis of AS in the event of a change in the system software;

4) licensed software shall be used and acquired only in the availability of a license.

79. Measures to control proper use of software are defined in the IS TD, and shall be carried out at least once a year and include:

defining of actually used software;

determination of the software use rights;

comparison of actually used software and available licenses.

80. The application software shall perform verification of the ownership and validity of the EDS public key and the registration certificate of the person who signed the electronic

document, in accordance with the Rules for verifying the authenticity of electronic digital signature, approved by the authorized body in accordance with subparagraph 10) of paragraph 1 of Article 5 of the Law of the Republic of Kazakhstan "On electronic document and electronic digital signature".

Footnote. Paragraph 80- as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

Paragraph 3. Requirements for information and communication infrastructure

81. Requirements for ICI shall be formed with regard to the facilities comprised in it, in accordance with subparagraph 25) of Article 1 of the Law.

82. UR establishes requirements for the following ICI objects:

1) information system;

2) technological platform;

3) hardware and software complex;

4) telecommunication networks;

5) systems of uninterrupted functioning of technical means and information security;

6) server room (data center).

Footnote. Clause 82 as amended by the Decree of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

Paragraph 4. Information System Requirements

83. Information system of SB or LEB shall be created and developed in the manner specified by paragraph 1 of Article 39 of the Law, and with regard to requirements of Article 38 of the Law.

Mandatory requirements for the means of processing, storage and backup of EIR in the information system of SB or LEB are determined by Article 42 of the Law.

84. Before starting a trial operation by the developer:

1) a set of tests, test scripts and test methods shall be created for all functional components of the information system;

2) bench tests of the information system shall be carried out;

3) for the staff:

of information system of SB or LEB of the first class, training is mandatory in accordance with the classifier;

of information system of SB or LEB of the second class - creation of video, - multimedia training materials in accordance with the classifier;

for information system of SB or LEB of the third class - creation of a help system and (or) operating instructions in accordance with the classifier.

85. Trial operation of SB IS or LIE shall include:

documentation of procedures for trial operation;

optimization and elimination of identified defects and shortcomings with their subsequent correction;

registration of an act on the completion of trial operation of the IS;

the period of trial operation should not exceed one year.

Footnote. Paragraph 85 - as amended by Decree of the Government of the Republic of Kazakhstan dated January 18, 2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

85-1. The introduction of the object of informatization of "electronic government" shall be carried out in accordance with the standards in force in the territory of the Republic of Kazakhstan.

Footnote. The unified requirements are supplemented by paragraph 85-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated January 18, 2021 No . 12 (shall be enforced ten calendar days after the day of its first official publication).

86. Before entering into industrial operation of an IS in an SB, MPR or organization, the criteria for the acceptance of the created IS or new versions and updates of the IS are determined, agreed, documented.

Footnote. Clause 86 as amended by the Decree of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

87. Putting into industrial operation of IS SB or MPR is carried out in accordance with the requirements of technical documentation, subject to the positive completion of trial operation, the presence of an act with a positive test result for compliance with IS requirements, signing of an act on putting into industrial operation of IS by an acceptance committee with the participation of representatives of the authorized body , interested SB, MPR and organizations .

Footnote. Clause 87 as amended by the Decree of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after its first official publication)

87-1. Tests for compliance with information security requirements are carried out in accordance with Article 49 of the Law.

Footnote. The unified requirements are supplemented by paragraph 87-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

88. Submission for accounting and storage to the electronic government’s service integrator the developed software, source software codes (if available) and a set of settings for

licensed software of the information system of the SB, LEB or organizations, is mandatory and shall be carried out in accordance with the procedure determined by the authorized body.

Modification, disclosure and (or) use of source software codes, software products and software shall be carried out with the permission of its owner.

89. During the industrial operation of IS SB or M&E, the following shall be provided:

1) safety, protection, and restoration of EIR in case of failure or damage;

2) redundancy and control over the timely updating of the EIR;

3) automated accounting, preservation and periodic archiving of information about calls to the SB IS or LEB;

4) fixing changes in the configuration settings of software, server and telecommunications equipment;

5) control and regulation of functional performance characteristics;

6) maintenance of IP;

7) technical support of the used licensed IP software;

8) warranty service by the IS developer, including the elimination of errors and shortcomings of the IS identified during the warranty period (Warranty service shall be provided for a period of at least a year from the date of putting the IS into commercial operation);

9) the connection of users to the IS, as well as the interaction of the IS, shall be carried out using domain names;

10) system maintenance;

11) reduction (exclusion) of the use of paper documents, as well as requirements for their submission in the performance of public functions and the provision of public services.

Footnote. Paragraph 89 - as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

90. Integration of the SB or LEB information system, including with SB or LEB information system, which is in trial operation, shall be carried out in accordance with the requirements specified in Article 43 of the Law.

Integration of non-state information system with SB or LEB information system shall be carried out in accordance with the requirements defined by Article 44 of the Law.

90-1. At the fulfillment of functions of integration interaction of informatization facilities or components of informatization facilities through a gateway, integration bus, integration component or integration module, the following actions shall be provided:

1) registration and verification of sources (connection points) of legitimacy requests;

2) verification of the legitimacy of requests for:

password or EDS;

connection point;

presence of connection blocking;

permitted types of requests defined in the regulation on integration interaction;

the allowed request frequency defined in the regulation on integration interaction;

presence in requests of signs of information security violations;

presence of malicious code on signatures;

3) connection blocking upon detection of violations in the messaging protocols in the events of:

absence of connection during the time defined in the regulation on integration interaction;

excess of the allowed frequency of requests for the time specified in the regulation of integration interaction;

presence in requests of signs of information security violations;

excess in the number of authentication errors defined in the regulation of integration interaction;

detection of anomalous user activity;

detection of attempts to upload data arrays;

4) regular change of connection passwords according to the duration of time defined in the regulation of integration interaction;

5) replacement of the login when identifying IS incidents;

6) concealment of internal circuit LAN addressing;

7) event logging, including:

recording of events of transmission / receipt of information messages;

recording of file transfer / receipt events;

recording of service messages transfer / receipt events;

the use of IS incident and event management system for monitoring of event logs;

automation of procedures for analyzing event logs for the presence of IS events;

storage of event logs on a specialized log server, accessible for administrators only for viewing;

separate event logging (if necessary) by:

a) the current day;

b) connection (communication channel);

c) to a state body (legal entity);

d) integrable informatization objects;

8) provision of time synchronization service for integrable informatization objects;

9) software and hardware cryptographic protection of connections made through data transmission networks;

10) storage and transmission of encrypted passwords;

11) automation of notifying the responsible persons of integrated informatization objects of IS incidents.

Footnote. Chapter 3 was supplemented with clause 90-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

91. Warranty service of the information system at the industrial operation stage with involvement of third parties shall require:

IS regulation in warranty service agreements;

ICT risk management in the process of warranty service.

92. Management of software and hardware IS SB and MPR is carried out from the PP of the internal circuit of the owner of the IS.

The software and hardware of the IS SB or PP and non-state IS integrated with the IS SB or MPR is located on the territory of the Republic of Kazakhstan, except for cases related to interstate information exchange, carried out using the national gateway, within the framework of international treaties ratified by the Republic of Kazakhstan.

Footnote. Clause 92 as amended by the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

92-1. To organize the work of the SB or LEB information system, it shall be allowed to use cloud services (hardware and software systems, information system providing resources with the use of virtualization technology), the control centers and servers of which are physically situated on the territory of the Republic of Kazakhstan.

Footnote. Chapter 3 was supplemented with clause 92-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

92-2. The hardware and software of the information system of critical informatization facilities and ICI containing personal data of citizens of the Republic of Kazakhstan shall be placed on the territory of the Republic of Kazakhstan.

Footnote. Chapter 3 was supplemented with clause 92-2 in accordance with the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

92-3. Possessors and owners of information systems of a state body shall create their operational information security center and ensure its functioning or purchase the services of an operational information security center from third parties in accordance with the Civil Code, and shall also ensure its interaction with the National Information Security Coordination Center.

Footnote. The unified requirements are supplemented by paragraph 92-3 in accordance with the Decree of the Government of the Republic of Kazakhstan dated January 18, 2021 No . 12 (shall be enforced ten calendar days after the day of its first official publication).

92-4. Possessors, owners and users of SB IS and LEB shall carry out filling, ensure the reliability and relevance of the EIR.

Footnote. The unified requirements are supplemented by paragraph 92-4 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

93. The owner or holder of the SB or LEB information system shall make a decision on the termination of the information system operation in the absence of the need for its further use.

The service integrator shall be notified of the cessation of operation of the SB or LEB information system, with the publication on the architectural portal of the "electronic government" of the informatization subjects whose information systems are integrated with the decommissioned information system of SB or LEB, and the SB or LEB that are users of this information system.

94. The SB or LEB shall draw up a plan for decommissioning of the SB or LEB information system operations and coordinate it with the SB or LEBs that are users of the information system of the SB or LEB.

95. After the IS is decommissioned, the SB or LEB shall submit to the departmental archive electronic documents, technical documentation, journals and an archived database of the decommissioned SB IS or LEB in accordance with the Rules for the receipt, storage, accounting and use of documents of the National Archival Fund and other archival documents by departmental and private archives approved by the Decree of the Government of the Republic of Kazakhstan in accordance with subparagraph 3) of paragraph 1-1 of Article 18 of the Law on Archives.

Footnote. Paragraph 95 - as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

96. Upon receipt of an application for terminating operation of the SB or LEB information system, the service integrator shall cancel the electronic registration certificate of the SB or LEB information system and place the relevant information on the architectural portal of the " electronic government".

97. Withdrawal and (or) disposal of the decommissioned information system of the SB or LEB shall be carried out in accordance with the legislation of the Republic of Kazakhstan on accounting and financial reporting.

If the operation of the information system of the SB or LEB is terminated, but the information system of the SB or LEB is not withdrawn in the prescribed manner, this information system shall be considered to be in conservation.

After decommissioning the information system of the SB or LEB shall not be used.

98. To maintain IS:

1) at the stages of bench tests, acceptance tests and test operation the following actions shall be carried out:

testing of information system software based on developed test suites configured for specific classes of programs;

full-scale testing of programs under extreme loads with simulated exposure to active defects (stress testing);

testing of the information system's software to identify possible defects;

bench tests of the information system's software to determine unintended software design errors, identify potential problems for performance;

Identification and elimination of vulnerabilities in software and hardware;

development of protection tools against unauthorized exposure;

2) before putting the information system into trial operation, it shall be required to provide :

control of adverse effects of the new information system on the functioning information systems and components of the EG ICI, especially during maximum loads;

analysis of the new information system impact on the condition of the information system of the EG ICI;

organization of staff training for the operation of the new information system;

3) separation of the environments of the pilot or industrial operation of the information system from the environments of development, testing or bench testing. The following requirements shall be implemented:

transfer of the information system from the development phase to the testing phase shall be recorded and documented;

transfer of the information system from the testing phase to the trial operation phase shall be recorded and documented;

transfer of the information system from the pilot operation phase to the industrial operation phase shall be recorded and documented;

development tools and tested software of the information system shall be located in different domains;

compilers, editors and other development tools in the operating environment shall not be located or shall not be available for use from the operating environment;

the test environment of the information system shall correspond to the operating environment in terms of hardware and software and architecture;

for tested information systems, it shall not be allowed to use real user accounts of the systems that are in industrial operation;

data from the information system in industrial operation shall not be subject to copying into the test environment;

4) during the information system decommissioning the following steps shall be provided:

archiving of information contained in the information system;

destruction (erasing) of data and residual information from computer storage media and (or) destruction of computer storage media. Upon decommissioning of machine storage media

on which information was stored and processed, physical destruction of these storage media shall be carried out with execution of the relevant act.

98-1. The information system of critical objects of ICI is also subject to the requirements of the standard of the Republic of Kazakhstan IEC / PAS 62443-3-2017 “Industrial communication networks. Security (cybersecurity) of the network and system. Part 3. Security (Cybersecurity) of the industrial measurement and control process ”.

Footnote. The uniform requirements were supplemented by clause 98-1 in accordance with the Decree of the Government of the Republic of Kazakhstan No. 1047 dated December 31, 2019 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

Paragraph 5. Technology platform requirements

99. The choice of a technological platform is carried out taking into account the priority of equipment with the ability to support virtualization technology.

Footnote. Clause 99 as amended by the Resolution of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

100. In the choice of equipment that implements virtualization technology, the need to ensure the following functions shall be taken into account:

1) decomposition:

computing resources distributed between virtual machines;

many applications and operating systems coexisting on the same physical computing system;

2) isolation:

virtual machines completely isolated from each other, and an emergency failure of one of them not affecting the others;

data is not transferred between virtual machines and applications, except when using shared network connections;

3) compatibility:

applications and OS are provided with computing resources of equipment that implements virtualization technology.

101. EG ICP shall be placed on the equipment located in the server center of the SB.

EG ICP shall ensure:

automated provision of IC services with a single entry point for their management;

virtualization of computing resources of server equipment with the use of various technologies;

uninterrupted and fault-tolerant functioning of the provided IC services with utilization ratio of at least 98.7%;

exclusion of a single point of failure at the logical and physical levels by the means of used equipment, telecommunications and software;

separation of computing resources at the hardware and software levels.

Reliability of the virtual infrastructure is provided by the built-in virtualization software and virtual environment management software.

101-1. Industrial operation of the ICP is allowed provided there is an act with a positive test result for compliance with information security requirements.

Footnote. Chapter 3 was supplemented with clause 101-1 in accordance with the Decree of the Government of the Republic of Kazakhstan No. 355 dated June 18, 2018 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

102. To maintain IS using virtualization technology, the following measures shall be implemented:

1) identity management requiring:

authentication of IC services clients and privileged users;

federated user identification within the same technology platform;

saving of authentication information after deleting the user ID;

the use of control tools for the procedures of assigning the user authority profiles;

2) access control requiring:

separation of powers of the information system administrator and the virtualization environment administrator;

restrictions on access rights of the virtualization environment administrator to the IC service user data. Access rights are limited to the specific procedures defined in the SB TD and the service agreement for maintenance, and shall be subject to regular updating;

multi-factor authentication for privileged and critical operations;

restrictions on the use of roles with full authority. Information system administrator profile settings shall exclude access to the virtualization environment components;

definition of minimum privileges and implementation of the role-based access control model;

remote access via secure gateway or the list of allowed network addresses of the senders;

3) encryption key management, requiring:

control of access restrictions to data on encryption keys of data encryption tools (DET);

control over organization of the root directory and key subscription;

blocking of compromised keys and their safe destruction;

4) conducting an audit of IS events, requiring:

obligatory and regular procedures defined in the IS TD;

conducting audit procedures for all the operating systems, client virtual machines, network components infrastructure;

maintaining an event log and storing in a storage system inaccessible to the administrator;

checking the correct operation of the event logging system;

determining duration of the event logs storage in the IS TD;

5) registration of IS events, requiring:

logging of administrators' actions;

applying a system for monitoring incidents and IS events;

alerting based on automatic detection of a critical event or information security incident;

6) IS incident management, requiring:

determining the formal process of detecting, identifying, evaluating and responding to IS incidents with updating once every six months;

reporting at the intervals specified in the IS TD, based on the results of detection, identification, evaluation and response to IS incidents;

notifications of responsible persons of the SB, LEB or organizations about IS incidents;

recording of IS incidents in the computer incident response Service of the State technical service;

7) applying protective measures of hardware and software components of the virtualization environment infrastructure that carry out:

physical shutdown or blocking of unused physical devices (removable drives, network interfaces);

disabling of unused virtual devices and services;

monitoring of the interaction between guest operating systems;

control of virtual and physical devices association (mapping);

the use of certified hypervisors;

8) physical separation of operating environments from development and testing environments;

9) definition in the IS TD of change management procedures for informatization objects;

10) determination in the IS TD of the recovery procedures after failures and malfunctioning of the equipment and software;

11) implementation of network and system administration procedures requiring:

provision of the safety of virtual machine images, monitoring of integrity of the operating system, applications, network configuration, software and data of the SB or organization for the presence of malicious signatures;

separation of the hardware platform from the operating system of the virtual machine in order to exclude access of external users to the hardware;

logical isolation between various functional areas of the virtualization environment infrastructure;

physical isolation between EIR and information system virtualization environments of various classes according to the IS level.

Paragraph 6. Requirements for hardware-software complex

103. Requirements for configuration of server equipment of the HSC are determined in the requirements specification for creation or development of the information system and (or) technical specifications for the purchase of goods, works and services in the field of informatization.

104. The HSC server equipment of typical configuration shall be selected with regard to priority of servers:

1) with multiprocessor architecture;

2) enabling scaling of resources and increase of productivity;

3) supporting virtualization technology;

4) including controls, changes and redistribution of resources;

5) compatible with the used information and communication infrastructure.

105. To ensure high availability of the server, the embedded systems shall be used:

1) hot-swappable redundant fans, power supplies, drives and I / O adapters;

2) dynamic clearance and redistribution of memory pages;

3) dynamic redistribution of processors;

4) alerts about critical events;

5) supporting continuous monitoring of critical components and measuring monitored indicators.

106. Acquired server hardware shall be provided with technical support of the manufacturer. Discontinued server hardware shall not be acquirable.

107. To ensure IS on a regular basis, as defined in the TD IS, an inventory of server equipment shall be carried out with a check of its configuration.

108. To ensure the security and quality of service with the execution of an IS joint work agreement in the manner prescribed by the legislation of the Republic of Kazakhstan, the server equipment of the agro-industrial complex of the objects of informatization of SB and LEB:

first class - located only in the server center of SB;

second class - located in the server center of the SB, the server room of the SB and local authorities or the involved legal entity, equipped in accordance with the requirements for server rooms established in these UT.

Footnote. Paragraph 108 - as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

108-1. To ensure the availability and fault tolerance of the agro-industrial complex of objects of informatization of SB and LEB, reservation of hardware and software for data

processing, data storage systems, and components of data storage networks shall be carried out with the execution of an agreement for joint work on information security in the manner established by the legislation of the Republic of Kazakhstan for objects of informatization of the first and second classes in the reserve server room of the SB, LEB or involved legal entity , equipped in accordance with the requirements for server rooms established in these UR.

Footnote. Unified requirements are supplemented by paragraph 108-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication); as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

109. Requirements for data storage systems shall be defined in the requirements specification for creation or development of the information system and (or) technical specifications for the purchase of goods, works and services in the field of informatization.

110. The data storage system shall provide support for:

single tools for data replication;

scalability by data storage volume.

111. For highly loaded information systems, requiring high availability, the following shall be applied:

1) data storage networks;

2) data storage systems that support virtualization system and (or) tiered data storage.

112. To ensure high availability, the storage systems shall include embedded systems:

1) hot-swappable redundant fans and power supplies;

2) hot-swap drives and I / O adapters;

3) alerts about critical events;

4) active controllers (at least two controllers);

5) storage network interfaces (at least two ports per controller);

6) support for continuous monitoring of the critical components status and measurement of monitored indicators.

113. The data storage system shall be provided by a backup system.

114. To maintain IS, safe storage and data recovery capabilities:

1) cryptographic protection shall be applied of the stored service information of limited use, information of confidential information systems, confidential EIR and EIR containing personal data of limited access with the use of DET in accordance with paragraph 48 of these URs;

2) a dedicated server shall be used for secure storage of encryption keys with a security level not lower than the security level of the used DET established for cryptographic keys in the rules for using data encryption tools;

3) recording and testing of backups shall be provided in accordance with the backup regulations defined in the IS TD.

115. When decommissioning storage media used in confidential information systems, confidential EIR and EIR containing personal data of limited access, software and hardware for guaranteed destruction of information shall be used.

116. When choosing system software for server hardware and workstations, the following are taken into account:

1) is excluded by the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023).

2) compliance with the type of operating systems (client or server);

3) compatibility with the used application software;

4) support for network services operating in the telecommunications network;

5) support for multitasking;

6) availability of standard means of obtaining and installing critical updates and security updates issued by the manufacturer of operating systems;

7) availability of diagnostic, audit and event logging tools;

8) support for virtualization technologies.

Footnote. Clause 116 as amended by the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); dated 10.02.2023 No. 112 (shall be enforced from 01.01.2023).

116-1. SB and LEB get access from the workstation to the "Digital Workplace of an Employee", designed to provide a single interface and access to all systems and services (components, software products) of "electronic government".

Footnote. Paragraph 3 is supplemented by paragraph 116-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

117. Acquisition of the system software shall be carried out with regard to priority of:

1) a licensing model that ensures decrease in the purchase cost, also aggregate cost of the license for the operation period;

2) software provided with technical support and maintenance.

118. To maintain IS, the system software shall enable:

1) access control with the use of:

identification, authentication and user password management;

recording of successful and failed accesses;

recording of the use of system privileges;

restriction of the connection time, if necessary, and blocking the session if the time limit is exceeded;

2) exceptions for users and restrictions for administrators in the use of system utilities that are able to bypass control mechanisms of the operating system.

119. Free software (FS) distribution shall be gratis, without licensing restrictions, which prevent the use in the SB with observance of the copyright law requirements.

120. FS shall be provided with open source code.

121. FS used in the SB shall be updated taking into account the support of information interaction formats through the EG external gateway (EGEG).

122. To maintain IS in the use of FS:

FS supported by the community of FS developers or through examination and certification of software code shall be permitted;

FS versions that were used shall be saved.

Paragraph 7. Requirements for telecommunication networks

123. Departmental (corporate) telecommunication networks shall be organized by integrating local networks held by one owner through dedicated private or leased communication channels.

Dedicated communication channels designed for integrating local networks shall be organized with the use of channel and network layer protocols.

124. When organizing a departmental (corporate) network by integrating several local networks, a radial or radial-node network topology is applied. At the anchor connection points, dedicated channels are connected to one border gateway. Cascading (serial) LAN connection is not used.

125. During designing, a documented scheme of a departmental (corporate) telecommunication network is created and maintained in operation.

126. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

127. Excluded by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

128. In order to ensure the IS of a dedicated communication channel:

1) software and hardware means of information protection shall be applied, including cryptographic encryption, using MCIP;

2) connect to the local area network through an edge gateway with prescribed routing rules and security policies. The Edge Gateway shall provide the following minimum functionality:

centralized authorization of network nodes;

configuration of administrator privilege levels;

recording the actions of administrators;

static network address translation;

protection against network attacks;

monitoring the status of physical and logical ports;

filtering of incoming and outgoing packets on each interface;

cryptographic protection of transmitted traffic using MCIP;

3) when connecting a departmental (corporate) telecommunications network and local SI networks, the following shall be used:

means of separation and isolation of information flows;

equipment with components that provide information security and secure management;

dedicated and integrated with access equipment firewalls installed at each connection point to protect the ETC SB perimeter;

4) when connecting a departmental (corporate) telecommunications network and local area networks to the Internet via SB EGEG, state legal entities, quasi-public sector entities, as well as Owners or possessors of critically important ICI facilities use the services of an operator or another telecom operator that has reserved communication channels on equipment UIAG.

Connection of a departmental (corporate) telecommunications network and local area networks to the Internet through the UIAG shall be carried out in accordance with the Rules for the functioning of a single gateway for accessing the Internet, approved by the authorized body in the field of information security;

5) employees of SB, LEB and employees of state legal entities, subjects of the quasi-public sector, as well as owners or possessors of critically important ICI facilities for the implementation of operational information exchange in electronic form in the performance of their official duties use:

departmental e-mail, instant messaging and other services;

e-mail, instant messaging service and other services, the control centers and servers of which are physically located on the territory of the Republic of Kazakhstan, unless otherwise established by the authorized body;

available online cloud videoconferencing services for communication with foreign individuals and legal entities;

6) the interaction of departmental e-mail of SB and LEB with external electronic mail systems shall be carried out only through a single e-mail gateway;

7) employees of SB, LEB and employees of state legal entities, subjects of the quasi-public sector, as well as owners or possessors of critically important ICI facilities access IR from the LAN of the external circuit only through the UIAG using a web browser that is an open source software and meets the requirements of the Rules for the functioning of the UIAG approved by the authorized body in the field of information security;

8) employees of SB, LEB and employees of state legal entities shall access to Internet resources through an Internet browser, the distribution kit of which has pre-installed registration certificates of the national certification center of the Republic of Kazakhstan and the root certification center of the Republic of Kazakhstan.

Footnote. Paragraph 128 - as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

129. Connection of SI to the SB UTE shall be carried out in accordance with the Rules for connecting to the SB UTE and providing access to an intranet resource through the SB UTE, determined by the authorized body.

At the request of the SI, the operator shall perform:

distribution, registration and re-registration of IP addresses of SI local area networks connected to the SB UTE, upon SI requests;

registration of domain names in the Internet domain zones gov.kz and мем.қаз at the request of SI;

registration of domain names in the ETS SB network at the request of SI;

provision of DNS service in the ETS SB network.

Footnote. Paragraph 129 - as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

130. In SB or LEB it shall be allowed to use devices for organizing wireless access only to publicly available EIRs of the "electronic government" and places permitted for SB or LEB visitors staying in the "guest zone".

131. It shall be prohibited to connect to the SB UTE, the local area network SI, as well as the technical means that are part of the SB UTE, the local area network SI, devices for organizing remote access via wireless networks, wireless access, modems, radio modems, modems of networks of cellular operators, cellular subscriber devices and other wireless network devices, except for ETS SB wireless communication channels organized by the EG ICP operator, using MCIP in accordance with clause 48 of these UR.

Footnote. Paragraph 131 - as amended by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

131-1. It shall be necessary to control the connection of subscriber devices of cellular communication, modems of networks of cellular operators, as well as electronic media that are not allowed by the information security policy adopted in the SB or LEB.

Footnote. The unified requirements are supplemented by paragraph 131-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

132. The operator of the EG ICP, at the request of the SI, shall perform:

distribution, registration and re-registration of IP addresses of SI local area networks connected to the SB UTE, upon SI requests;

registration of domain names in the Internet domain zones gov.kz and mem.қаз at the request of SI;

registration of domain names in the ETS SB network at the request of SI;

provision of DNS service in the ETS SB network.

Footnote. Paragraph 132 - as amended by the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

133. SB and MPR annually:

1) request from the state technical service a list of categories of Internet resources used on the equipment of SGIA;

2) choose from the above list the categories of Internet resources, access to which is allowed for employees of the civil society and local authorities by means of SGIA, and make a list of them;

3) send to the state technical service the above list and lists of network addresses of information and communication networks of civil society and their territorial subdivisions, MPRs that get access to the Internet, for use on SGIA equipment;

4) send to the state technical service, in case of operational need to organize VPN channels, technical information on the required VPN channels (source and destination IP addresses, ports, protocol), agreed with the authorized body in the field of information security.

Footnote. Clause 133 as amended by the Resolution of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); No. 12 dated January 18, 2021 (shall be enforced upon the expiration of ten calendar days after the day of its first official publication).

133-1. It shall be prohibited to install and use at informatization objects located in the LAN of the external circuit of the SB or LEB, software or hardware for remote control of them from outside the LAN of the external circuit of the SB or LEB.

Footnote. The unified requirements are supplemented by paragraph 133-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

134. Excluded by Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

134-1. The State Technical Service shall apply the policy of blocking the following categories of IRs and software on the UIAG equipment (by default):

- VPN;
- remote access;
- p2p;
- game resources;

- unknown applications that are not included in the list of IR and software categories by default;

- malicious IR and software.

Footnote. The unified requirements are supplemented by paragraph 134-1 in accordance with the Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced ten calendar days after the day of its first official publication).

134-2. The possibility of unlocking certain categories of IR and software specified in paragraph 134-1 shall be considered by the state technical service on the basis of an official request received from SB, LEB, government organizations, subjects of the quasi-public sector , as well as owners of critical ICI objects.

Footnote. The unified requirements are supplemented by paragraph 134-2 in accordance with the Decree of the Government of the Republic of Kazakhstan dated January 18, 2021 No . 12 (shall be enforced ten calendar days after the day of its first official publication).

135. Requirements for the created or developed local network shall be defined in the technical specification for the purchase of goods, works and services in the field of informatization.

When designing a cabling system for a local network, requirements shall be observed of the state standard SN RK 3.02-17-2011 Structured Cabling Networks. Design Standards.

136. During the design, a documented scheme of the local network shall be created, which is kept up to date during operation.

137. All the cabling system elements shall be subject to marking in accordance with requirements of paragraph 13.1.5 of the State standard SN RK 3.02-17-2011 Structured Cabling Networks. Design Standards.

All the cabling connections shall be recorded in the cabling connection log.

138. Active equipment of local networks shall be fed with electric power from uninterruptible power supplies.

139. To ensure the IS of local area networks:

1) unused LAN cabling ports shall be physically disconnected from the active equipment;

2) TD IS shall be developed and approved, including the rules of:

use of networks and network services;

connections to international (territorial) data transmission networks;

connections to the Internet and (or) telecommunications networks, communication networks with access to international (territorial) data transmission networks;

use of wireless access to network resources;

3) service information of limited distribution, information of confidential IS, confidential EIR and EIR containing personal data of limited access, shall not be transmitted via unprotected wired communication channels and radio channels that are not equipped with appropriate MCIP.

The transfer of official information of limited distribution shall be carried out in compliance with special requirements for the protection of information of limited distribution in accordance with the Rules for classifying information as official information of limited distribution and working with it, established by the Government of the Republic of Kazakhstan;

4) the following means shall be applied:

identification, authentication and user access control;

equipment identification;

protection of diagnostic and configuration ports;

physical segmentation of the local area network;

logical segmentation of the local area network;

network connection management;

firewall;

hiding the internal address space of the local area network;

integrity control of data, messages and configurations;

cryptographic protection of information in accordance with paragraph 26 of these URs;

physical protection of data transmission channels and network equipment;

registration of IS events;

monitoring and analysis of network traffic;

network management;

5) the interaction of the local area networks of SB, as well as the LEB among themselves, shall be carried out only through the UTS of SB, except for special-purpose telecommunications networks and/or government, classified, encrypted and coded communications;

6) the local area networks of the central executive state body and its territorial divisions shall interact with each other only through the SB UTE, except for special-purpose telecommunications networks and/or government, classified, encrypted and coded communications;

7) interfacing of the LAN of the internal circuit and the LAN of the external SI circuit with each other shall be excluded, except for organized communication channels using MCIP, in accordance with paragraph 48 of these UR for institutions of the Republic of Kazakhstan located abroad or organized using a shielded subnet;

8) the connection of the LAN of the internal circuit of the SI to the Internet shall be excluded;

9) the LAN of the external SI circuit shall be connected to the Internet only through the UIAG. Connection to the Internet in any other way is not shall be prohibited, except for special and law enforcement SB for operational purposes. The interaction of the EGEG with the Internet shall be carried out through the UIAG;

10) IS SIs that implement information interaction via the Internet shall be placed in a dedicated LAN segment of the SI outer loop and interaction with IS SI located in the local area network of the SI inner loop shall be carried out through the HSEP, except for cases where a shielded subnet is used;

11) information interaction of IS located on the Internet with IS SI located in the local area network of the SI internal circuit shall be carried out only through the HSEP, except for cases when a shielded subnet is used;

12) servers of the top-level time source infrastructure are synchronized with the time and frequency standard reproducing the national UTC(kz) coordinated universal time scale.

The Time Infrastructure servers shall be synchronized with the top-level Time Infrastructure server.

Time infrastructure servers shall provide access to clients for time synchronization;

13) open unused network ports shall be disabled.

Footnote. Paragraph 139 - as amended by Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced ten calendar days after the day of its first official publication).

140. The requirements provided for in subparagraphs 10), 11) of paragraph 139 UR are not applicable to IS SB and MPR, put into commercial operation before January 1, 2016 and not subject to development until January 1, 2018.

The procedure for information interaction of data from IS SB or MPR with non-state IS is determined by the Rules for the integration of objects of informatization of "electronic government", approved by the authorized body in the field of informatization in accordance with subparagraph 13) of Article 7 of the Law.

Footnote. Clause 140 as amended by the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

Paragraph 8. Requirements for systems of uninterrupted functioning of technical facilities and information security

141. Server equipment of HSC and data storage systems shall be placed in the server room.

142. The server room shall be located in separate, closed to admissions premises without windows. If there are window openings, they must be closed or sealed with non-combustible materials.

For the surface of walls, ceilings and floors, materials are used that do not emit and do not accumulate dust. For flooring, antistatic materials are used. The server room shall be protected from contaminants.

The walls, doors, ceiling, floor and partitions of the server room shall provide hermetic state of the premises.

143. The doors of the server room must be at least 1.2 meters wide and 2.2 meters high, open outward or move apart. The door frame must be without a threshold and a central pillar.

144. The server room must have a false floor and (or) false ceiling to accommodate cable systems and utility lines.

145. Laying of any transit communications through the server room shall be excluded. Routes of ordinary and fire water supply, heating and sewage shall be withdrawn from the server room and shall not be located above the server room on the upper floors.

146. Installation of communication channels for laying power and low-current cable networks of a building is carried out in separate or separated by partitions cable trays, ducts or pipes spaced from each other. Low-current and power cabinets shall be installed separately and locked.

Cables through inter-floor covering, walls, partitions are laid in sections of fireproof pipes , and are hermetically sealed by non-combustible materials.

147. The server room shall be reliably protected from external electromagnetic radiation.

148. When placing equipment:

1) the implementation of the Rules for the technical operation of electrical installations of consumers, approved by the authorized body in the field of energy in accordance with subparagraph 27) of Article 5 of the Law of the Republic of Kazakhstan "On Electricity" (hereinafter referred to as the Law on Electricity), shall be ensured;

2) compliance with the requirements of suppliers and (or) equipment manufacturer for installation (assembly), load on floors and raised floors shall be ensured, taking into account the weight of equipment and communications;

3) the availability of free service passages for equipment maintenance shall be ensured;

4) the organization of air flows of the microclimate system shall be taken into account;

5) the organization of the system of raised floors and false ceilings shall be taken into account.

Footnote. Paragraph 148- as amended by Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

149. In technical support of the equipment installed in the server room, the following shall be documented:

1) equipment maintenance;

2) elimination of problems arising during the operation of hardware and software complex (HSC);

3) facts of failures and malfunctions, also restoration work results;

4) post-warranty service of critical equipment after the warranty service period expiry.

The form and method of documentation shall be determined independently.

150. Maintenance of critical equipment shall be performed by certified engineering staff.

151. In close proximity to the server room, a warehouse of spare parts for critical equipment shall be created, containing a stock of components and equipment for operational replacement during remedial measures.

152. Intervention in the work of equipment in operation shall be possible only with the permission of the head of the information technology unit or of a person replacing him.

153. The main and backup server rooms have to be located at a safe distance in the buildings that are remote from each other. Requirements for redundant (backup) server rooms are identical to the requirements for primary server rooms.

154. In order to ensure IS, fault tolerance and operational reliability:

1) in the server room, methods of equipment location are used to reduce the risks of threats, dangers and opportunities for unauthorized access;

2) excluded by the Decree of the Government of the Republic of Kazakhstan dated February 10, 2023 No. 112 (shall be enforced from January 1, 2023);

3) the list of persons authorized to support the ICI objects installed in the server room is kept up to date;

4) the server room is equipped with systems:

access control and management;

providing a microclimate;

security alarm;

video surveillance;

fire alarm;

fire extinguishing;

guaranteed power supply;

grounding;

5) the fault tolerance of the server room infrastructure is at least 99.7%.

Footnote. Clause 154 as amended by the Decree of the Government of the Republic of Kazakhstan No. 1047 dated December 31, 2019 (shall be enforced upon expiry of ten calendar days after the day of its first official publication); dated 10.02.2023 No. 112 (shall be enforced from 01.01.2023).

155. The access control and management system shall provide authorized entry into the server room and authorized exit from it. The blocking devices and design of the front door shall prevent the possibility of transmitting access identifiers in the opposite direction through the front door.

The central control device of the access control and management system shall be installed in separate service rooms, premises of the security post, protected from access by unauthorized persons. Access of the security personnel to the software of the access control and management system that influences the system’s operating modes shall be excluded.

Power supply to the access control and management system is provided from a free group of standby lighting panels. Access control and management system shall be provided with redundant power supply.

156. The microclimate provision system includes air conditioning, ventilation and microclimate monitoring systems. The server room microclimate systems are not combined with other microclimate systems installed in the building.

The temperature in the server room is maintained in the range from 20 ° C to 25 ° C with a relative humidity of 45% to 55%.

The capacity of the air conditioning system must exceed the total heat generated by all equipment and systems. The air conditioning system is redundant. The power supply of air conditioners in the server room is carried out from a guaranteed power supply system or an uninterruptible power supply system.

The ventilation system provides fresh air inflow with filtration and heating of incoming air in winter. The server room is pressurized to prevent contaminated air from entering the adjacent rooms. On the air ducts of the supply and exhaust ventilation, safety valves are installed, controlled by the fire extinguishing system.

Air conditioning and ventilation systems are turned off automatically by a fire alarm signal.

Microclimate monitoring system controls climatic parameters in server cabinets and telecommunication racks:

air temperature;

air humidity;

dustiness of the air;

smoke in the air;

opening (closing) cabinet doors.

Footnote. Clause 156 as amended by the Decree of the Government of the Republic of Kazakhstan dated December 31, 2019 No. 1047 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

157. The security system of the server room shall be separate from the building security systems. Alerts are displayed in the premises of the round-the-clock security on a separate display console. All the inlets and outlets of the server room, as well as the internal volume of the server room, are subject to control and protection. The alarm system has its own redundant power supply.

158. Location of the video surveillance system cameras shall be selected with regard to control of all the entrances and exits to the server room, the space and passages near the equipment. The viewing angle and resolution of cameras must enable face recognition. The image from the cameras is displayed on a separate remote control in a 24-hour security room.

159. The fire alarm system of the server room shall operate separate from the fire alarm of the building. Two types of sensors shall be installed in the server room: of temperature and smoke.

The sensors control the total space of the server room and the volumes formed by the false floor and / or false ceiling. Alerts of the fire alarm system are displayed on the remote control in round-the-clock security premises.

160. The server room fire extinguishing system shall be supplied with an automatic gas fire extinguishing installation, independent of the building fire extinguishing system. A special non-toxic gas is used as a fire extinguisher in an automatic gas fire extinguishing installation. Powder and liquid fire extinguishers shall not be used. The gas fire extinguishing installation shall be located directly in or near the server room in a cabinet specially equipped for this purpose. The fire extinguishing system is launched from sensors of early fire detection, which react to the emergence of smoke, also from hand sensors located at the premises exit. The delay time for the extinguisher release shall be no more than 30 seconds. Alert on the fire extinguishing system actuation comes up on the display, placed inside and outside the room. The fire extinguishing system issues commands to close the protective valves of the ventilation system and turn off the power to the equipment. A server room with a fire extinguishing system shall be provided with exhaust ventilation to air away the extinguishing gas.

161. The guaranteed power supply system shall comprise two power supply inputs from different external power sources the voltage of ~ 400 / 230V, frequency of 50 Hz and an autonomous generator. All the electricity sources are fed to the power-transfer relay, which automatically switches to the backup power input when the main power input is interrupted or stopped. The parameters of the power lines and the core section are determined issuing from the planned total power consumption of the equipment and subsystems of the server room. Power lines are in a five-wire circuit.

The guaranteed power supply system shall provide for the power supply of equipment and systems of the server room through uninterruptible power sources. The power and configuration of uninterruptible power sources is calculated taking into account all the powered equipment and stock for perspective development. Run time from uninterruptible power supplies is calculated taking into account the needs, as well as the necessary time to switch to the backup lines and the time for the generator to start up in operating mode.

162. The grounding system of the server room shall be carried out separately from the protective grounding of the building. All metal parts and structures of the server room shall be grounded with a common ground bus. Each cabinet (rack) with equipment shall be grounded by a separate conductor connected to a common ground bus. Exposed conductive parts of information processing equipment must be connected to the main earth terminal of the electrical installation.

The earth conductors connecting the surge protectors to the main earth bus must be as short and straight as possible (no angles).

When constructing and operating a grounding system, it is necessary to be guided by:

Rules for the installation of electrical installations, approved by order of the authorized body in the field of energy in accordance with subparagraph 19) of Article 5 of the Law on Electricity;

standard of the Republic of Kazakhstan ST RK IEC 60364-5-548-96 "Electrical installations of buildings. Part 5. Selection and installation of electrical equipment". Section 548 "Grounding the device and system for equalizing electrical potentials in electrical installations containing information processing equipment";

the standard of the Republic of Kazakhstan ST RK IEC 60364-7-707-84 "Electrical installations of buildings. Part 7. Requirements for special electrical installations". Section 707 Grounding of Information Processing Equipment;

the standard of the Republic of Kazakhstan ST RK GOST 12.1.030-81 "OSSS. Electrical safety. Protective grounding, zeroing";

standard of the Republic of Kazakhstan ST RK GOST 464-79 "Grounding for fixed installations of wired communication, radio relay stations, radio broadcasting nodes of wire broadcasting and antennas of collective television reception systems. Resistance standards".

Footnote. Paragraph 162 - as amended by the Decree of the Government of the Republic of Kazakhstan dated 10.06.2022 No. 383 (shall be enforced ten calendar days after the day of its first official publication).

163. Switchgears of telecommunication networks are located in a cross room. The cross room is located closer to the center of the work area it serves.

The size of the cross room is selected based on the size of the served work area and the equipment to be installed.

The cross room must meet the following requirements:

availability of free service aisles for equipment maintenance;

absence of powerful sources of electromagnetic interference (transformers, electrical panels, electric motors, etc.);

lack of pipes and valves of the water supply system;

the presence of fire safety systems;

lack of easily flammable materials (wooden shelves, cardboard, books, etc.);

the presence of a separate power line from a separate machine for connecting the cabinet according to the project;

the presence of security alarm systems, access control;

the presence of an air conditioning system.

Footnote. Chapter 3 was supplemented with clause 163 in accordance with the Decree of the Government of the Republic of Kazakhstan dated June 18, 2018 No. 355 (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

Appendix
to Order No. 832 of the Government
of the Republic of Kazakhstan
dated December 20, 2016

List of certain orders of the Government of the Republic of Kazakhstan that lost force

1. Subparagraphs 5) and 6) of paragraph 1, paragraphs 2-1 and 2-2 of Order No. 965 of the Government of the Republic of Kazakhstan dated September 14, 2004 "On some measures to ensure information security in the Republic of Kazakhstan".

2. Order No. 244 of the Government of the Republic of Kazakhstan dated March 14, 2013 "On introducing amendments to Order No. 965 of the Government of the Republic of Kazakhstan dated September 14, 2004 "On some measures to ensure information security in the Republic of Kazakhstan ".

3. Order No. 706 of the Government of the Republic of Kazakhstan dated June 26, 2014 " On introducing amendments to Order No. 965 of the Government of the Republic of Kazakhstan dated September 14, 2004 "On some measures to ensure information security in the Republic of Kazakhstan".