On approval of risk assessment criteria and checklists in the field of informatization in terms of ensuring information security

Unofficial translation

Joint order of the Deputy Prime Minister of the Republic of Kazakhstan - Minister of Defense and Aerospace Industry of the Republic of Kazakhstan dated January 29, 2019 No. 13 / НҚ and Minister of National Economy of the Republic of Kazakhstan dated January 29, 2019 No. 12. Registered in the Ministry of Justice of the Republic of Kazakhstan on February 6, 2019 No. 18269.

Unofficial translation

In accordance with paragraph 3 of Article 141 and paragraph 1 of Article 143 of the Entrepreneurial Code of the Republic of Kazakhstan dated October 29, 2015, **WE HEREBY ORDER**:

1. To approve:

1) Excluded by joint order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 20.01.2023 № 21/НҚ and the Minister of National Economy of the Republic of Kazakhstan dated 23.01.2023 № 8 (shall enter into force dated 01.01.2023).

2) Excluded by joint order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 20.01.2023 № 21/НҚ and the Minister of National Economy of the Republic of Kazakhstan dated 23.01.2023 № 8 (shall enter into force dated 01.01.2023).

3) a checklist in the field of informatization in terms of ensuring information security in relation to state legal entities, entities of the quasi-public sector, possessors and owners of non-state information systems that are integrated with information systems of state bodies or intended to form state electronic information resources, as well as possessors and owners of critically important objects of information and communication infrastructure in accordance with Appendix 3 to this joint order.

2. The Committee on Information Security of the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan, in the manner prescribed by the legislation of the Republic of Kazakhstan, to ensure:

1) state registration of this joint order in the Ministry of Justice of the Republic of Kazakhstan;

2) within ten calendar days from the date of registration of this joint order, its sending in the Kazakh and Russian languages to the Republican state enterprise on the basis of the right of economic management “Republican Legal Information Center” for official publication and

inclusion in the Reference Control Bank of regulatory legal acts of the Republic of Kazakhstan;

3) placement of a copy of this joint order on the Internet resource of the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan.

3. The supervising vice minister of the defense and aerospace industry of the Republic of Kazakhstan shall be authorized to oversee the execution of this joint order.

4. This joint order shall come into force upon expiry of ten calendar days after the day of its first official publication.

Deputy Prime Minister of the
Republic of Kazakhstan –
Minister of defense and aerospace
industry of the Republic of Kazakhstan _____ *A. Zhumagaliyev*
Minister of national economy of the
Republic of Kazakhstan _____ *T. Suleimenov*

"AGREED"
Committee for legal statistics and
special accounting of the
General Prosecutor's Office of the
Republic of Kazakhstan

Appendix 1
to the joint order of the Deputy
Prime Minister of the Republic of
Kazakhstan – Minister of defense
and aerospace industry of the
Republic of Kazakhstan dated
January 29, 2019 № 13/НҚ
and Minister of national economy
of the Republic of Kazakhstan
dated January 29, 2019
№ 12

Risk assessment criteria in the field of informatization in terms of ensuring information security

Footnote. Annex 1 recognized as invalid by joint order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 20.01.2023 № 21/NҚ and the Minister of National Economy of the Republic of Kazakhstan dated 23.01.2023 № 8 (shall enter into force dated 01.01.2023).

Appendix 2
to the joint order of the Deputy
Prime Minister of the Republic of
Kazakhstan – Minister of defense
and aerospace industry of the
Republic of Kazakhstan
dated January 29, 2019 № 13/НҚ
and Minister of national economy

of the Republic of Kazakhstan
dated January 29, 2019 № 12

Checklist in the field of informatization in terms of ensuring information security in relation to the state and local executive bodies

Footnote. Annex 1 recognized as invalid by joint order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 20.01.2023 № 21/NQ and the Minister of National Economy of the Republic of Kazakhstan dated 23.01.2023 № 8 (shall enter into force dated 01.01.2023).

Appendix 3
to the joint order of the Deputy
Prime Minister of the Republic of
Kazakhstan – Minister of defense
and aerospace industry of the
Republic of Kazakhstan
dated January 29, 2019 № 13/HQ
and Minister of national economy
of the Republic of Kazakhstan
dated January 29, 2019 № 12

Checklist in the sphere of informatization regarding ensuring information security

_____

pursuant to Article 138

Footnote. Annex 3 - as amended by the joint order of the Minister of Digital Development , Innovation and Aerospace Industry of the Republic of Kazakhstan dated 20.01.2023 № 21/ NQ and the Minister of National Economy of the Republic of Kazakhstan dated 23.01.2023 № 8 shall enter into force dated 01.01.2023).

_____

Entrepreneurial Code of the Republic of Kazakhstan
in relation to: state legal entities, entities
quasi-public sector, owners and owners of non-state
information systems integrated with information systems
state bodies or intended for the formation of state
electronic information resources, as well as owners and proprietors
Critical Information and Communications Infrastructure

_____

name of a homogeneous group of control subjects (objects)

_____

_____

The state body that appointed the audit _____

_____

Inspection Assignment Certificate _____

№, date

Name of the subject (object) of control _____

(Individual Identification Number), Business Identification Number subject (object) of control _____

Address of residence _____

№	Requirement list	Conforms to requirements	Does not meet the requirements
1	2	3	4
1	Compliance with the requirement to connect local, departmental and corporate telecommunication networks of state bodies, local executive body, state legal entities, entities of the quasi-public sector, as well as owners of critical information and communication infrastructure (hereinafter referred to as ICI) to the Internet by telecom operators through a unified gateway to the Internet		
2	Compliance with the requirement to notify the owner of critical information and communication infrastructure facilities of the National coordination center for information security about information security incidents and the results of response to them		
3	Compliance with the requirements for the use of means: User identification, authentication, and access control equipment identification; protection of diagnostic and configuration ports; Physical segmentation of local network Logical segmentation of local network		

	Management of network connections firewalling; concealing the internal address space of the local network; Control the integrity of data, messages, and configurations cryptographic information protection		
4	Compliance with the requirements for information security monitoring, protection and safe functioning during operation of informatization objects		
5	Availability of anti-virus tools, updates of operating systems on workstations connected to the Internet when organizing access to the Internet from local networks of the outer outline		
6	Availability of information security subdivision, which shall be a structural subdivision separated from other structural subdivisions dealing with the creation, maintenance and development of informatization objects, or determination of an official responsible for information security, with the passage of specialized courses in the field of information security at least once every three years with the issuance of a certificate		
	Availability and compliance with regulatory and technical documentation (hereinafter referred to as TD) on information security, in the form of a four-level system of documented rules, procedures, practices or guidelines that guide state		

	bodies (hereinafter referred to as the SB), local executive body (hereinafter referred to as the LEB) or organization in its activities . IS TD shall be developed in Kazakh and Russian languages, approved by the legal act of the Civil Defense, LEB or organization and communicated to all employees of the Civil Defense, LEB or organization employees. IS TD shall be revised in order to analyze and update the information set forth therein at least once every two years. 1. The information security policy of a civil defense, IS SB LEB or organization is a first-level document and defines the goals, objectives, guidelines and practices in the field of information security. 2. The list of documents of the second level shall include documents detailing the requirements of the information security policy of the Civil Defense, LEB or organization, including: 1) IS risk assessment methodology; 2) rules for identification, classification and marking of assets related to information processing means; 3) rules for ensuring the continuous operation of assets related to information processing means; 4) rules for inventory and certification of computer equipment, telecommunications equipment and software;		

7		5) IS internal audit rules; 6) rules for the use of cryptographic information protection tools (hereinafter referred to as CIPT); 7) rules for delimiting access rights to electronic information resources; 8) rules for using the Internet and e-mail; 9) rules for organizing the authentication procedure; 10) rules for organizing anti-virus control; 11) rules for the use of mobile devices and storage media; 12) rules for organizing physical protection of information processing means and a safe environment for the functioning of information resources. 3. The third level documents contain description of information security processes and procedures, including: 1) IS threat (risk) catalogue ; 2) IS threat (risk) processing plan; 3) information backup and recovery regulations; 4) a plan of measures to ensure the continuous operation and restoration of the operability of assets related to information processing means; 5) administrator's guide to maintaining the informatization object; 6) instructions on the procedure for users to respond to information security incidents and in emergency (crisis) situations. 4. The list of documents of the fourth level shall		

	include working forms, logs, applications, protocols and other documents, including electronic ones, used to register and confirm the performed procedures and works, including: 1) log of information security incidents and recording of emergency situations; 2) server room visit log; 3) report on network resource vulnerability assessment; 4) cable connection logbook; 5) log of accounting of backups (backup, recovery), testing of backups; 6) register of introduction of amendments in equipment configuration, testing and accounting of changes in free software (hereinafter referred to as FSW) and application software (hereinafter referred to as ASW) of information systems (hereinafter referred to as IS), registration and elimination of software vulnerabilities (hereinafter referred to as software); 7) test log of diesel generator sets and uninterruptible power supplies for the server room; 8) test log for microclimate , video surveillance, fire extinguishing systems in server rooms		
8	Compliance with the requirements for access to informatization objects of the first and second classes in accordance with the classifier for the use of			

	multifactor authentication, including using an electronic digital signature		
9	Compliance with the requirement to include in the job descriptions and (or) the terms of the employment contract functional duties to ensure IS and obligations to fulfill the requirements of the IS TD of the employees of the civil defense, LEB or employees of the organization		
10	Compliance with CIPT application requirements		
11	Compliance with the requirements for storage, restoration of state electronic information resources contained in the information system, safety of state electronic information resources		
12	Compliance with the requirements for information security of information resources (hereinafter referred to as the IS IR) for use content management systems, which shall perform: authorization of placement, modification and deletion operations in electronic information resources (hereinafter referred to the EIR); registration of authorship when posting, changing and deleting EIR; checking the downloaded EIR for malicious code; Audit the security of executable code and scripts monitoring the integrity of the placed EIR; keeping a log of EIR amendments;		

	monitoring of abnormal activity of users and software robots		
13	Compliance with the requirement for the use of registration certificates to verify the authenticity of the domain name and cryptographic protection of the contents of the communication session using CIPT when ensuring IS IR		
14	Compliance with requirements of management identification when using virtualization technology authentication of information and communication services clients and privileged users ; federated user identification within the same technology platform storing authentication information after deleting the user ID; applying controls over procedures for assigning user authorization profiles		
15	Compliance with the requirement to audit information security events when using virtualization technology: mandatory and regular procedures defined in IS IR ; Audit procedures for all operating systems, client virtual machines, and network component infrastructure logging of events and storage in a storage system inaccessible to the administrator; Verify that the event logging system is working correctly.		

	determining the duration of storing event logs in information security DP		
16	Compliance with the requirement for registration of information security events when using virtualization technology: logging of administrator actions; use of information security incidents and events monitoring system; alerts based on automatic recognition of a critical event or information security incident		
17	Compliance with the requirements for the implementation of network and system administration procedures: Ensuring the integrity of virtual machine images, monitoring the integrity of the operating system, applications, network configuration, software and data of the PG or organization for the presence of malicious signatures; separating the hardware platform from the virtual machine operating system to prevent external users from accessing the hardware		
18	Compliance with the requirements ensuring storage systems by backup system		
19	Compliance with the requirements for the use of software and hardware for information protection, including cryptographic encryption, using CIPT when organizing a dedicated communication channel connecting local networks		

20	Compliance with the requirement to exclude interfacing of the internal loop local network and the external loop local network with each other, with the exception of organized communication channels using CIPT		
21	Compliance with the use requirement of departmental e-mail, instant messaging and other services; e-mail, instant messaging services and other services whose control centers and servers shall be physically located in the Republic of Kazakhstan, unless otherwise established by the authorized body, for the implementation of operational information exchange in electronic form by employees of the Civil Defense, LEBs and employees of state legal entities, entities of the quasi-public sector, as well as owners of critical objects of information and communication infrastructure (hereinafter referred to as the ICI) in the performance of their official duties		
22	Availability of uninterruptible power supply for active equipment of local networks		
23	Compliance with the requirement to physically disconnect unused local network cabling ports from active equipment		
24	Compliance with the requirement for the use of firewalling		
	Availability of documentation during technical support of		

25	equipment installed in the server room: 1) equipment maintenance; 2) elimination of problems arising during the operation of hardware and software; 3) facts of failures and failures, as well as the results of restoration work; 4) post-warranty maintenance of critical equipment after the expiration of the warranty service period		
26	Availability of access control and management system in the server room providing authorized entrance to the server room and authorized exit from it. Barriers and the design of the front door shall prevent access identifiers from being transmitted backwards through the front door vestibule. The central control device of the access control and management system shall be installed in separate office premises, premises of the security post, protected from access by unauthorized persons. The security personnel shall exclude access to the software of the access control and management system affecting the system operation modes. Power supply of the access control and monitoring system is provided from the free group of the standby lighting board. Access control and monitoring system is provided by backup power supply		
27	Availability of up-to-date list of individuals		

	authorized to maintain ICI objects installed in the server room		
28	Availability of a microclimate support system in the server room: microclimate support system shall include air conditioning, ventilation and microclimate monitoring systems; air conditioning system shall be backed up; server room air conditioners shall be powered from the guaranteed power supply system or uninterruptible power supply system; air conditioning and ventilation systems shall be switched off automatically upon fire alarm signal		
29	Availability of security alarm system in the server room: the security alarm system of the server room shall be performed separately from the building security systems; alarm signals shall be output to the 24-hour security room in the form of a separate console; all entrances and exits of the server room, as well as the internal volume of the server room are subject to control and protection; security alarm system shall have its own redundant power supply		
30	Availability of video surveillance system in the server room: location of CCTV cameras shall be selected taking into account the control of all entrances and exits to the server room, space and passages near the equipment;		

	the viewing angle and resolution of the cameras must provide face recognition; the image from the cameras is displayed on a separate console in the 24-hour security room		
31	Availability of fire alarm system in the server room: the server room fire alarm system shall be separate from the building fire alarm system; two types of sensors shall be installed in the server room: temperature and smoke; sensors monitor the total space of the server room and the volumes formed by the raised floor and (or) raised ceiling; alarm signals of the fire alarm system are displayed on the console in the 24-hour security room		
32	Availability of fire extinguishing system in the server room: the server room fire extinguishing system is equipped with an automatic gas fire extinguishing system independent of the building fire extinguishing system; special non-toxic gas shall be used as a fire extinguisher in an automatic gas fire extinguishing system; powder and liquid fire extinguishers shall not be used; the gas fire extinguishing unit shall be located directly in the server room or near it in a cabinet specially equipped for this; the fire extinguishing system shall be launched from early fire detection		

	sensors responding to the appearance of smoke, as well as manual sensors located at the exit from the room; notification of fire extinguishing system actuation shall be displayed on the annunciators located inside and outside the room .		
33	Availability of a guaranteed power supply system in the server room: all power sources shall be supplied to the automatic backup circuit breaker, which performs automatic switching to the backup power input in case of power supply interruption at the main input; the guaranteed power supply system provides power supply to the equipment and systems of the server room through uninterruptible power supplies		
34	Availability of grounding system in the server room: the server room grounding system shall be separate from the building protective grounding; all metal parts and structures of the server room shall be grounded with a common grounding bus. Each cabinet (rack) with equipment is grounded by a separate conductor connected to the common grounding bus; open current-conducting parts of information processing equipment shall be connected to the main earthing terminal of the electrical installation; earthing conductors connecting overvoltage protection devices to the		

	main earthing busbar shall be the shortest and straightest (without corners)		
35	Absence of powerful sources of electromagnetic interference (transformers, electric boards, electric motors, etc.) in the marshalling yard		
36	Absence of pipes and valves of the water supply system in the marshalling room		
37	Availability of fire safety systems in the marshalling room		
38	Absence of easily ignitable materials (wooden racks, cardboard, books, etc.) in the marshalling room		
39	Availability of a separate power supply line from a separate circuit breaker in the marshalling room for connection of the cabinet under the project		
40	Availability of intrusion alarm systems, access control systems in the cross room		
41	Availability of air conditioning system in the marshalling area		
42	At the stage of experimental and industrial operation of informatization objects, the following means and systems shall be used: monitoring and management of information security incidents and events; intrusion detection and prevention		
	Compliance with the requirements for the creation of its own information security operations center and		

43	ensuring its functioning or the acquisition of information security operations center services from third parties, as well as its interaction with the National information security coordination center		
44	Compliance with the requirement for placement on the Internet resource with the registered domain name .KZ and (or) KAZ on the hardware and software complex, which shall be located in the Republic of Kazakhstan. The use of domain names . KZ and/or KAZ in the space of the Kazakhstan segment of the Internet when transferring data by Internet resources shall be carried out using security certificates		
45	Compliance with the requirement to conduct a regular inventory of server equipment with verification of its configuration		
46	Compliance with the requirements for the purchase of goods in order to implement the requirements for ensuring information security for the country's defense and state security from the register of trusted software and electronic industry products. At the same time, in the absence of the necessary products in the register of trusted software and products of the electronic industry, the purchase of goods is allowed		
	Compliance with the requirements for monitoring information security violation events in		

47	the civil defense, individual training center or organization: 1) monitoring of events related to information security violation and analysis of monitoring results; 2) registration of events related to the information security state, and violations shall be detected by analyzing the event logs, including: Operating system event logs event logs of database management systems; antivirus event logs; application software event logs; event logs of telecommunication equipment; Event logs of attack detection and prevention systems content management system event logs; 3) ensuring synchronization of the time of event logs with the infrastructure of the time source; 4) storage of event logs for the period specified in the IS TD, but not less than three years and are in operational access for at least two months; 5) event logging 6) ensuring the protection of event logs from interference and unauthorized access. Do not allow system administrators to modify, delete, or disable logs. Confidential ISs require creation and maintenance of a backup log storage; 7) ensuring the implementation of a			

	formalized procedure for reporting information security incidents and responding to information security incidents		
48	The existence of an agreement that shall establish the conditions for the operation, access or use of these objects, as well as responsibility for their violation when involving third-party organizations in ensuring the information security of EIR, IS, ICI		
49	Compliance with the requirements when dismissing or introducing amendments the conditions of the employment contract of the right of access of an employee of the Civil Defense, MO or employee of the organization to information and information processing means, including physical and logical access, access identifiers, subscriptions, documentation that shall identify him as an active SB employee, LEB or an employee of the organization are canceled after the termination of his employment contract or change when amending the terms of the employment contract		
50	Compliance with the requirements of the personnel department of the organization and keeping records of the passage of training in the field of informatization and information security by employees of the SB, LEB or employees of organizations		
	Compliance with the requirement to register with the computer incident		

51	response service of the state technical service of events identified as critical for confidentiality, accessibility and integrity based on the results of IS events monitoring analysis and event log analysis		
52	Compliance with the requirement to conduct an IS audit at least once a year , to owners of critical ICI facilities that process data containing legally protected secrets, with the exception of second-tier banks		
53	Compliance with the requirement when writing off the IS, software or service software product to ensure the preservation of the structure and content of the database through the built-in functionality of the database management system of the decommissioned IS with the preparation of instructions for the restoration of the EIR		
54	Availability of certificate with positive test result for compliance with information security requirements		
55	Compliance with the requirement to ensure the development or purchase of finished application software user interface, input, processing and output of data in Kazakh, Russian and other languages, if necessary, with the possibility of user selection of the interface language		
56	Compliance with monitoring requirements: actions of users and personnel;		

	use of information processing facilities		
57	Compliance with the requirement to provide the developed or purchased ready-made application software with technical documentation for operation in Kazakh and Russian languages		
58	Meet embedded server high availability requirements: 1) hot-swappable redundant fans, power supplies, drives, and I/O adapters; 2) notification of critical events; 3) support for continuous monitoring of the state of critical components and measurement of monitored indicators		
59	Availability of software and hardware for guaranteed destruction of information during decommissioning of information carriers used in confidential ISs, confidential AIRs and EIRs containing personal data of limited access		
60	Availability of local network diagram		
61	Availability of hardware and software complex and data storage system in server room		
62	Compliance with the requirement for the location of the server room in separate, impassable rooms without window openings. If there are window openings, they are closed or closed with non-combustible materials. For the surface of walls, ceilings and floors, materials that do not emit		

	or accumulate dust shall be used. For flooring, materials with antistatic properties shall be used. The server room shall be protected from contaminants. Walls, doors, ceiling, floor and partitions of the server room ensure the tightness of the room		
63	Availability of false floor and/or false ceiling in the server room for placement of cable systems and utilities		
64	Compliance with the requirement to exclude any transit communications through the server room. Normal and fire water, heating and sewerage routes shall be located outside the server room and shall not be located above the server room on the upper floors		
65	Compliance with the requirement to locate the main and backup server rooms at a safe distance in remote buildings. Redundant server room requirements shall be identical to primary server room requirements		
66	Compliance with the requirement to exclude placement in a server room in one virtual environment, one server equipment, one mounting cabinet or rack of EIR, IR, MSR, IS related in accordance with the classifier of informatization objects of the first class with informatization objects of the second and third class		

Official (s)

_____ _____

position

signature

_____

full name (if any)

Head of control subject

_____ _____

position

signature

_____

full name (if any)