On approval of the Rules for monitoring information security events of the objects of informatization of state bodies

Unofficial translation

Order of the acting and Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan dated August 16, 2019 года no. 199/НҚ. Registered with the Ministry of Justice of the Republic of Kazakhstan on August 23, 2019 no. 19286.

Unofficial translation

In accordance with subparagraph 5-1) of Article 7-1 of the Law of the Republic of Kazakhstan "On Informatization" **I HEREBY ORDER**:

Footnote. The preamble is in the wording of the order of the Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan dated 27.10.2022 No. 399/ НҚ (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

1. To approve the attached Rules for monitoring information security events of the objects of informatization of state bodies.

2. The Committee on Information Security of the Ministry of Digital Development, Innovations and Aerospace Industry in accordance with the procedure established by the legislation of the Republic of Kazakhstan shall ensure:

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

2) within ten calendar days from the date of state registration of this order, direction of it in Kazakh and Russian languages to the Republican State Enterprise on the right of economic management "Institute of Legislation and Legal Information of the Republic of Kazakhstan" of the Ministry of Justice of the Republic of Kazakhstan for official publication and placement in the Reference Control Bank of the Regulatory Legal Acts of the Republic of Kazakhstan;

3) posting this order on the Internet resource of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan after its official publication;

4) within ten working days after the state registration of this order, submission to the Legal Department Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan of information about implementation of measures stipulated by sub-clauses 1), 2) and 3) of this clause.

3. Control over execution of this order shall be entrusted to the supervising Vice-Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan.

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

Acting Minister of Digital Development,
Innovations and Aerospace Industry
of the Republic of Kazakhstan

"AGREED"
National Security Committee
of the Republic of Kazakhstan

Approved by the order
of the Acting Minister of Digital
Development, Innovations and
Aerospace Industry
of the Republic of Kazakhstan
dated August 16, 2019 no. 199/НҚ

Rules for monitoring information security events of informatization objects of state bodies

Footnote. The Rules are in the wording of the order of the Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan dated 27.10.2022 No. 399/ НҚ (shall be enforced upon expiry of ten calendar days after the day of its first official publication).

Chapter 1. General provisions

1. These Rules for monitoring information security events of informatization objects of state bodies (hereinafter - the Rules) have been developed in accordance with subparagraph 5-1) of Article 7-1 of the Law of the Republic of Kazakhstan “On Informatization” (hereinafter - the Law) and shall determine the procedure for monitoring information security events of informatization objects of state bodies.

2. These Rules use the following concepts and definitions:

1) objects of informatization - electronic information resources, software, Internet resource and information and communication infrastructure;

2) information security in the field of informatization (hereinafter - information security) - the state of security of electronic information resources, information systems and information-communication infrastructure from external and internal threats;

3) monitoring of information security events - constant monitoring of the informatization object in order to detect and identify information security events;

4) information security event (hereinafter – an IS event) - the state of information objects, indicating a possible violation of the existing security policy or a previously unknown situation that may be related to the security of an information object;

5) information security incident (hereinafter - IS incident) - individual or serial failures in the operation of the information and communication infrastructure or its individual objects,

creating a threat to their proper functioning and (or) conditions for illegal receipt, copying, distribution, modification, destruction or blocking electronic information resources;

6) state technical service (hereinafter – JSC "STS") – a joint-stock company created by decision of the Government of the Republic of Kazakhstan;

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

8) a system for collecting event logs - a hardware and software complex that provides centralized collection of event logs of informatization objects, their storage and further transfer to the IS event management system;

9) information security coordinator - an employee of JSC "STS", located on a permanent basis in a state body and carrying out coordination of activities aimed at maintaining the state of security of informatization objects of state bodies.

Other concepts used in these Rules shall be applied in accordance with the Law.

3. Monitoring of information security events of informatization objects of state bodies (hereinafter - MISE) shall be carried out by JSC "STS", which implements the tasks and functions of the National Information Security Coordination Center (hereinafter - NISCC).

4. The MISE objects shall be the objects of informatization of state body (hereinafter - SB).

The MISE objects shall not include:

1) electronic information resources containing information constituting state secrets;

2) protected 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 governmental, classified, encrypted and coded communications;

3) informatization objects of the National Bank of the Republic of Kazakhstan that are not integrated with the objects of the information and communication infrastructure of "electronic government".

6. Within the framework of the MISE, the sources of IS events shall be:

means of protecting information in the information and communication infrastructure (hereinafter - ICI) of the MISE objects, including those installed and maintained by JSC "STS " (hereinafter - IS events sources);

IS events management system of the NISCC.

7. MISE includes the following types of work:

1) installation of sources of IS events in the ICI of the MISE objects;

2) technical support for sources of information security events in the ICI of the MISE objects;

3) monitoring information security events of the MISE objects in order to detect information security incidents and subsequently respond to them.

8. MISE shall be carried out according to one of the following options:

1) for one type of works;

2) for several types of works.

9. MISE shall be carried out by JSC “STS” on the basis of contractual relations between the National Security Committee of the Republic of Kazakhstan (hereinafter - the NSC of the RK) and JSC “STS” in relation to the MISE objects located on the territory of the Republic of Kazakhstan.

Chapter 2. The procedure for monitoring information security events of informatization objects of state bodies

10. When conducting MISE, the JSC “STS” shall carry out:

1) as part of establishing sources of IS events:

study of ICI of the MISE objects;

deployment of a hardware and software complex of IS events sources in the ICI of the MISE objects;

setting up individual functioning mechanisms and security policies for IS events sources, as well as checking the correctness of their operation;

2) as part of technical support for IS events sources:

installing updates to IS events sources as they are released by the manufacturer;

monitoring the state of IS events sources, their parameters and protection modes, including eliminating errors and shortcomings in their functioning;

processing requests from SB regarding the functioning of IS events sources;

3) as part of tracking IS events of the MISE objects, in order to detect IS incidents and subsequently respond to them:

determining the list of events logs required for transfer to the NISCC IS events management system;

organization of events logging of IS events sources accompanied by JSC “STS”;

organization of systems for collecting NISCC event logs in the circuits of SB telecommunications networks in which the MISE objects operate;

organizing the collection of events logs of the MISE objects and sources of information security events into the system for collecting events logs of the NISCC;

organizing the transfer of events logs of the MISE objects and sources of IS events to the IS events management system of NISCC; their processing and analysis in order to identify IS events and IS incidents;

primary analysis of IS events or IS incidents identified at the MISE object;

notification of the SB or its authorized person about identified IS events and IS incidents within 30 minutes from the moment of detection of an IS event or IS incident, the National Security Committee of the Republic of Kazakhstan - within 3 hours;

issuing initial recommendations to stop the spread of an IS incident to the SB or an authorized person;

if technically possible, taking measures to stop the spread of an IS incident through sources of IS events;

sending, if necessary, an employee of JSC “STS” to the location of the MISE objects as part of the response to an IS incident (the need is determined by the National Security Committee of the Republic of Kazakhstan or JSC “STS” independently);

notification of the authorized body in the field of information security (hereinafter - the authorized body) and the National Security Committee of the Republic of Kazakhstan about the failure of the SB or its authorized person to eliminate the causes and consequences of the IS incident after 48 hours from the moment the IS incident was identified.

11. The information security coordinator shall carry out:

studying the information and communication infrastructure of SB in order to form recommendations for increasing the level of security of SB IO;

study of technical documentation on IS of SB in order to form recommendations for its updating and revision of the requirements of technical documentation;

coordinating measures to respond to IS incidents identified in the information and communication infrastructure of SB;

assistance in responding to IS incidents through information security tools installed by the employees of JSC “STS” (if technically possible);

assistance in carrying out activities to raise awareness in the field of IS among SB employees.

12. SB or a person authorized by it when conducting MISE shall:

provide physical and network access to the employees of JSC “STS” to the information and communication infrastructure of the SB and accounts with the necessary rights to install and maintain information security tools;

provide JSC "STS" with IP addresses in the circuits of telecommunications networks to organize the transfer of event logs of the MISE objects and sources of IS events to the IS events management system of the NISCC;

provide JSC “STS” with current information on a quarterly basis, in accordance with the appendix to these Rules;

update to the latest versions of the user and server operating systems;

notify JSC “STS” about the results of the analysis of the IS event and (or) about the measures taken to eliminate the IS incident within 48 hours from the receipt of notification from JSC “STS” about the identification of the IS event or IS incident, respectively.

13. JSC "STS", in accordance with the contracts for the provision of MISE services, shall quarterly send to the National Security Committee of the Republic of Kazakhstan summary information on identified IS threats, IS events and IS incidents, as well as information on the measures taken by SB on them.

14. The National Security Committee of the Republic of Kazakhstan shall quarterly send to the authorized body summary information on identified IS incidents, as well as information on the measures taken by SB on them.

Appendix
to the Rules
for monitoring events
of information security
of state bodies
informatization objects

Information about the MISE object

№	Name of the state body	Structural unit (department)	Physical location (floor, office)	Full name of the user/ responsible person	Network name of the workstation/ server equipment	IP address	Name of the operating system
1	2	3	4	5	6	7	8
Local network of subpath							
Local network of outside path							