Appendix 1 to the order of
Kazakhtelecom JSC dated
_____No _____

Regulations for managing information security incidents in Kazakhtelecom JSC

Almaty, 2024

Contents

Section 1. Destination

1. This document "KT/R-31-01 Regulations for information security incident management in Kazakhtelecom JSC" (hereinafter referred to as the Regulation) establishes a unified procedure for managing information security incidents in Kazakhtelecom JSC.

2. The Regulation has been developed in accordance with the requirements of international standards ISO 27001:2022, ISO 9001:2015, ISO 14001:2015, ISO 45001:2018 and their national analogues ST RK ISO/IEC 27001, ST RK ISO 9001-2016, ST RK ISO 14001-2016, ST RK ISO 45001-2019, as well as legislative acts of the Republic of Kazakhstan.

Section 2. Application domain

3. Requirements of the Regulation are aimed at increasing the level of information security in Kazakhtelecom JSC (hereinafter referred to as the Company) by increasing the security of information infrastructure and information systems of the Company. The Regulation is mandatory for application in all structural subdivisions and the Central Office of Kazakhtelecom JSC.

Section 3. Terms, Definitions and Abbreviations

4. The terms and definitions used in the Regulation comply with ISO 27001:2022, ISO 9001:2015, ISO 14001:2015, ISO 45001:2018 standards and their national analogues ST RK ISO/IEC 27001, ST RK ISO 9001-2016, ST RK ISO
14001-2016, ST RK ISO 45001-2019:

1) IS&SPU Unit– Information Security and Special Projects Unit DIT;
2) Incoming information is a material or informational object or service included in the process stage;
3) DIT– Information Technology Division– a branch of the Company;
4) DDEMS– Department for the Development of Enterprise Management Systems DIT;
5) DFD– Data Factory Department of DIT;
6) Application– an electronic document in the form of an InfraManager database account describing the problem that has arisen in the IT asset and the history of actions to solve it;
7) IS– Information Security;
8) ISI- Information Security Incident (one or more undesirable or unexpected information security events that have a significant probability of compromising business operations and the implementation of an information security threat);
9) InfraManager is a system for automating information technology management processes in the Company. It provides automation of the processes of managing incidents and requests

for service, accounting and movement of IT assets and other processes;
10) Outgoing information– a material or information object or service that is the result of a stage of the process;
11) IT asset – computer equipment, servers, network devices, software and other technological components. Provide the physical infrastructure for storing and processing data;
12) IT system– an information system. A system designed for storage, processing, search, distribution, transfer and provision of information with the use of appropriate organizational resources (human, technical, financial, etc.);

13) Firewall ;
14) NCCIB– National Coordination Center for Information Security of the Republic of Kazakhstan;
15) OIBK– Department of Information Security and Control of DIT, 2nd line of response and processing of ISI OCIB;
16) OS– operating system;
17) SOC – an operational center of information security, carrying out protection of electronic information resources, information systems, telecommunication networks and other objects of informatization of the Company and responding to IIS;

18) Software– software;
19) Problem ticket - an electronic document in the form of an ARS Remedy database account describing the problem that has arisen in the IT asset and the history of actions to solve it;
20) ISS– Information Security Service of Kazakhtelecom JSC;
21) SM&A– Monitoring and Analysis Service of ITD, 1st line of response and processing of ISI of the CIB;
22) SOK3– Operational Control Service of the 3rd level of Association "Division "Network"– branch of Kazakhtelecom JSC;
23) SP– Structural subdivision of the Central Office/branch of the Company;
24) ISMS– ASR Remedy Problem Ticket Management System;
25) TB– Technical Unit of DIT;
26) Step– Part of a process step, used to detail a process step;
27) EBDR – an electronic database of the Company's realized risks and incidents at the consolidated level, a risk management tool used for the purpose of continuous monitoring of realized risks;
28) ASR Remedy – Problem Ticket Management System;
29) OSS&IT – OSS and IT Management Systems Service and IT Association "Network Division"– branch of "Kazakhtelecom" JSC;
30) SOAR – system for orchestration, automation and response to IIS;
31) WEB IM interface– a web interface of the Support Service module in the InfraManager system, which allows users to independently create requests and track the progress of their solution, executors– to work out requests by area of responsibility;

32) WEB-platform of the NCCIB– the web-platform of the NCCIB, which provides operational interaction on the development of the ISI between the NCCIB and the SSC.

Section 4. Responsibilities and Authority

5. The Unit is responsible for organizing the ISI management process IS&SPU.
6. Participants in the IIS management process shall be responsible for the implementation of the Regulations.
7. Third parties, including employees of contractors responsible for the operation of the Company's IT asset and IT system, are responsible for the timely response and elimination of the identified ISI, and the responsibility must be taken into account in the contracts (agreements) concluded with them. The responsibility for including the requirements of the provisions of the Regulation, in terms of response and elimination of ISI, in contracts/agreements lies with the curator/initiator of the contract, the draft of such treaties must be agreed with the SIB.

8. Employees of the Company who have violated the provisions of the Regulations may be subject to disciplinary measures in accordance with the procedure established by the legislation of the Republic of Kazakhstan and internal documents of the Company.

Section 5. Information Security Incident Management

Chapter 1. General Provisions

9. All IT assets and IT systems of the Company are subject to ISI management, if there is a technical possibility to collect data.
10. In order to increase the efficiency and efficiency of the process, all communications and operations carried out within the framework of the implementation of the Regulation should be documented electronically in the relevant systems specified in the Regulation.

11. The ISI Department provides for the following actions:
1) identification and analysis of the ISI;
2) creation of an action plan for the elimination of the ISI;
3) elimination of ISI;
4) preparation of a report on the identified and eliminated ISI;
5) corrective measures and preventive measures to prevent ISI.
12. For the purposes of the Regulation, in order to confirm the procedure for documenting transactions and communications in the process, the following shall be recognized as equivalent:
1) messages sent by e-mail with documents attached in electronic form;

2) memos in the corporate electronic document management system with the attachment of documents in electronic form;
3) the availability of information in the relevant systems.

13. Target state of the process: obtaining information about information security events of all information resources connected to the Company's information infrastructure in real time.

14. Employees of the Company, third parties responsible for the operation of IT assets and IT systems, in case of independent detection of an information security event, are obliged to inform the head of the Information Security and Information Security Department, the Head of the IBC, who, in turn, inform the Director for Information Security and Special Projects of the IT Department and the Head of the ISS.

Chapter 2. Functional delineations between structural divisions for information security incidents

15. The CM&A shall:

1) identification of ISI, i.e. collects available information from employees' workplaces, network devices and other IT assets and IT systems in order to timely detect and respond to possible ISI;
2) conducting an initial analysis of the IS event for the presence of IS and the threat of IS and determining the nature and degree of IS hazard;
3) response to IIS – taking immediate measures to eliminate the ISS and minimize its impact, including initiating measures to isolate compromised systems, block access and other actions;
4) registration of ISI in the EBDR in accordance with the approved Rules for accounting and analysis of realized risks and incidents of Kazakhtelecom JSC;
5) investigation and analysis of the IIS- the IIS should be investigated in order to find out its cause, scope and consequences, which allows for measures to be taken to eliminate the IIS and to prevent the recurrence of the IIS in the future.

16. The ISI shall:

1) collection of clarifying information from the workplaces of employees, network devices and other objects of information infrastructure, in order to supplement the data collected by the SM&A to detect and eliminate the possibility of the development of the IIS;
2) assessment of the nature of the IIS, its scale and potential threats to the IT asset/IT system, analysis of the causes of the IIS and identification of vulnerabilities that could be used in illegal actions;
3) taking measures to localize and terminate the IIS, blocking (disabling) nodes that have signs of malware infection and (or) use by intruders, changing security settings or temporarily disabling services, in agreement with the ISS and the owner of the IT asset/IT system, depending on the scale and significance of the node to be disconnected;

4) development of measures for the elimination (localization) of the identified sources of the ISS by organizational, organizational, technical or technical measures, using hardware and software protection tools;
5) providing awareness, forming an expert opinion based on the results of the IIS review to coordinate efforts to restore the IT asset/IT service and prevent future IIS;

6) IIS analysis– development and submission of recommendations to the ISS to strengthen IS Policies and procedures.

17. The ISS supervises the Company's information security issues by:

1) analysis of the security of information systems and resources, periodic audit (at least 1 time per quarter) by available information security tools, with the provision of reports on the state of information security to the Managing Director for Security;

2) control over the implementation of measures on the IIS management process, according to the Flowchart of the process "Information security incident management in Kazakhtelecom JSC" and the Matrix of risks and controls of the process "Information security incident management in Kazakhtelecom JSC";

3) implementation of an initiative to conduct training courses for the Company's employees in order to prevent recurrence of ISI.

18. SAFETY, DFD, DDEMS, OSS&IT, SOK3, third parties responsible for the operation of the information infrastructure and information systems of the Company shall:

1) in case of independent detection of ISI, informing the ISSP Unit about all identified ISI through the InfraManager/ISMS system;

2) response to the IIS by taking immediate measures to stop the ISS and minimize its impact, in accordance with the action plan for the elimination of the IIS, indicating the specific actions received from the ISSP and ISS Unit;

3) liquidation (localization) of the identified sources of the ISS by organizational, organizational, technical or technical measures, in accordance with the requirements and specific actions received from the IS&SPU and ISS Unit.

Chapter 3. Identification and analysis of an information security incident

19. Registration of the ISI: Responsible– Head of the Maintenance and Automation Department; Deadline– 1 business day from the date of receipt of the message about the IS event; Incoming information: Information security event Detailed description of actions during the identification and analysis of the ISI:

Step 1. Obtaining information about an information security event from the relevant sources (system for collecting and correlating information security events, anti-virus software, ITSM application, WEB platform of the National Center for Securities Security, etc.).

Step 2. Within 15 minutes, register the information security event in SOAR.

Step 3. Analysis of the IS event. At this stage, the initial analysis takes place and the event is defined as "IS incident"/"non-IS incident":

1) if the event is defined as a "non-information security incident", the event is closed in SOAR;

2) if the event is defined as an "information security incident", the IIS is registered in SOAR, the WEB-platform of the NSCI and the EBDR.

Outgoing information: Registered ISI in SOAR, the WEB-platform of the NCCIB and EBDR. 20. ISI analysis: Responsible – Director for

Information Security and Special Projects of the Information Information Department; Deadline– 1 business day from the date of registration of the ISI; Incoming information: Registered ISI in SOAR.

Detailed description of actions in the analysis of ISI:

Step 1. Analysis of the ISI and determination of the scope (number of nodes affected by the ISI) and the degree of impact on the nodes (objects affected by the ISI).

The assessment of the degree of impact on nodes (facilities subject to ISI) should be carried out in accordance with Appendix 1 to the Regulation.

Step 2. Action plan for the elimination of ISI.

At this stage, the IBC develops an action plan for the elimination of the ISI.

The action plan should include:

1) a detailed description of the ISI;
2) a list of vulnerable nodes;
3) the sequence of actions to eliminate the ISI or aimed at reducing the impact of the ISI;
4) a list of actions to assess the impact of these measures on the IT asset exposed to the ISI as a whole.

The list of measures is given in Appendix 2 to the Regulation, but is not limited to it and can be supplemented depending on the degree of impact of the IIS. At this stage, the results of scanning of IT assets/IT systems (subject to IIS) are analyzed, the results of scanning from all means of identifying vulnerabilities are compared and the vulnerabilities found are confirmed as a result of comparing versions, software settings and OS. determined by the results of the scan and the versions, settings of the software and OS actually used in the system affected by the IIS.

Step 3. Registration of the application in the WEB interface of the IM/Problem Ticket in ASR Remedy with the work plan for the elimination of the ISI.

Outgoing information: Application/Problem ticket in the InfraManager/ISMS system with a detailed Work Plan for the elimination of IIS.

Chapter 4. Troubleshooting an information security incident

21. Taking measures to eliminate the ISI.

Supervision of measures to eliminate IIS is carried out by the ISS. Responsible for monitoring the elimination of the ISI is the Director for Information Security and Special Projects of the DIT. Responsible for the organization and execution of work on the elimination of the ISI are the heads of the joint venture or third parties responsible for the operation and maintenance of the IT asset and IT systems where the ISI is recorded, together with the IBS Unit.

The deadline for the implementation of measures to eliminate the IIS is up to 7 working days from the date of registration of the Application/Problem Ticket in the InfraManager/ISMS system;
Incoming information:
Application/Problem Ticket in the InfraManager/ISMS system with a detailed Action Plan for the elimination of the IIS.

Detailed description of the ISI elimination operation:
Upon receipt of the action plan in the Application/Problem Ticket, it must be executed.
In this case, the following should be assessed:
1) risk of software version compatibility problem;
2) the risk of new vulnerabilities in the IT system or information infrastructure object;
3) labor intensity of pre-testing of ISI elimination measures;

Outgoing information:
Executed Request/Problem ticket in the InfraManager system/ISMS with the results of actions to eliminate the ISI;

22. Control over the implementation of the IIS Action Plan Responsible – Director for Information Security and Special Projects of the DIT;
Deadline– 1 business day from the date of execution of the Request/Problem Ticket in the InfraManager/ISMS system;
Incoming information:
Executed Request/Problem Ticket in the InfraManager System/ISMS with a detailed Action Plan to eliminate the IIS; Detailed description of the implementation of the IIS
Step 1. Conducting a re-examination of the IT asset/IT system.
At this stage, a re-examination of the IT asset/IT system takes place.

Step 2. Analysis and comparison of the results of the repeated study with the initial with data on the ISI.
At this stage, the correctness of the corrections made to the IT asset/IT system is confirmed:
1) information on the current state of the IT asset/IT system;
2) confirmation of the elimination of the ISI.
Step 3. Closure of the ISI in SOAR, the WEB-platform of the NCCIB and EBDR with a detailed description of the elimination of the ISI.
Outgoing information: Closed ISI in SOAR, on the WEB-platform of the NCCIB and EBDR.

Chapter 5. Corrective and preventive actions on identified and eliminated information security incidents

23. Generation of a report on the identified and eliminated ISI.
Responsible – Director for Information Security and Special Projects of the Information Information Department; Deadline– 1 business day from the date of closing of the ISI
Incoming information: Closed application to SOAR.

Detailed description of the operation: An information security incident report is generated in accordance with Appendix 3 to the Regulations.

Outgoing information: Information security incident report.

24. Corrective and preventive actions on identified and eliminated ISI.
Responsible – Director for Information Security and Special Projects of the Information Department; Deadline– 7 working days from the date of closure of the ISI.

Incoming information: Information security incident report.
Detailed description of the operation:
Step 1. Analytical/statistical analysis of the elimination of ISI. At this stage, the analysis and comparison of the identified eliminated ISI is carried out.
Step 2. Formation of corrective and preventive measures to prevent the recurrence of the ISI in the future, indicating the deadlines and responsible persons.

Outgoing information:
Plan of corrective and preventive measures.

Chapter 6. Control

25. Control over compliance with the provisions of the Rules of Procedure shall be carried out by the IRS.

26. As part of the IIS identification and analysis procedures, employees of the IS&SPU Unit shall have the right to use all necessary software and hardware, including those that are prohibited from being used by the Company's internal documents, but not prohibited by the regulatory legal acts of the Republic of Kazakhstan.

27. In case of detection of violations of the provisions of the Regulations, arising in connection with the unfair performance by employees of their duties under the Regulations or resulting from violation of the provisions of the Company's internal documents in the field of information security, the ISS shall report these facts to the immediate and

supervising supervisor of the employee who violated the provisions of the Regulations, for appropriate measures to be taken.

Section 6. Documentation

28. Appendix 1 - Assessment of the degree of risk of an information security event.
29. Appendix 2 – Actions to be taken when an information security event is detected.
30. Appendix 3 - Information Security Incident Report.

Section 7. Links

31. ISO 9000:2015 Quality Management Systems. Basic Provisions and Dictionary.
32. ISO 9001:2015 Quality Management Systems. Requirements.
33. ISO 14001:20015 Environmental Management Systems. Requirements and Guidelines for Use.
34. ISO 45001:2018 Occupational Health and Safety Management Systems. Requirements.
35. ST RK 9001-2016 Quality Management Systems. Requirements.
36. ST RK 14001-2016 Environmental Management Systems. Requirements and Guidelines for Application.
37. ST RK ISO 45001-2019 Occupational Safety and Health Management Systems. Requirements.
38. Rules of Documentation and Document Management in Kazakhtelecom JSC.
39. ST RK ISO/IEC 27001:2022 Information technology Methods and means of ensuring the security of Information Security Management Systems. Requirements.

Appendix 1 to the Regulation on
information security incident management
in Kazakhtelecom JSC, approved by order
of Kazakhtelecom JSC _____
No _____

Information security event risk assessment

Risk	Characteristics
1	Single attempts to scan, collect information regarding the nodes of the internal network. Activities of known viruses or worms on individual (isolated) nodes.
2	Single attempts to scan, collect information regarding the nodes of the internal network. Attempts to exploit a vulnerability that is likely to be present on network hosts.
3	A large number of attempts to scan, collect information. Failed attempt at a DoS attack or "hacking". Controlled activity from known viruses or worms on a significant number of network hosts. Activity from new viruses or worms on individual (isolated) nodes.
4	Attempted DoS attack or "hacking" that had little impact on individual nodes. A partially successful attack with easily mitigated consequences. Difficult-to-control activity from known viruses or worms on a significant number of network hosts. Little risk of loss of reputation or financial loss.
5	A successful DoS attack or ‘hacking’ attempt that had a significant impact on hosts on the corporate network. Significant risk of reputational or financial loss. Significant spread of viruses or worms that are difficult to control.

Appendix 2 to Regulation on information security incident management in Kazakhtelecom JSC, approved by order of Kazakhtelecom JSC _____No _____

Actions taken when an information security event is detected

Risk	Actions
1	A record of activity related to the ISI. Update the nodes that are under attack. Updating antivirus software, changing filtering rules on firewalls.
2	A record of activity related to the ISI. Blocking communication with the attacker's node. Update the nodes that are under attack. Updating antivirus software, changing filtering rules on firewalls.
3	A record of activity related to the ISI. Blocking communication with the attacker's node. Update the nodes that are under attack. Updating antivirus software, changing filtering rules on firewalls
4	A record of activity related to the ISI. Node isolation Blocking communication with the attacker host. Collection of evidence for the investigation. Update the nodes that are under attack. Updating antivirus software, changing filtering rules on firewalls
5	A record of activity related to the ISI. Shutting down nodes or isolating them. Blocking communication with the attacker's node. Collection of evidence for the investigation. Update the nodes that are under attack. Updating antivirus software, changing filtering rules on firewalls.

Appendix 3 to the Regulation on
information security incident management
in Kazakhtelecom JSC, approved by order
of Kazakhtelecom JSC _____
No _____

Information Security Incident Report

Date of establishment of the ISI	
Type of ISI	
Description of the ISI	

Description of the ISI:

Contact information	
Full name of the employee who discovered the ISI	
Name of the joint venture	
email	
Telephone number	
Additional contact information	
Target of attack	

Hostname or IP address	
Host Assignment (Functions Performed)	
Source of attack	
Hostname or IP address	
Is the owner and/or provider of the owner of the IP address informed?	
Description of the ISI	
Date	
Attack method	
OS and application software versions on the attacked host	
Vulnerabilities exploited	
Other information	
Analysis result	

ISI analysis:

What threats does the ISI implement?	
Degree of influence on the Company's business activities	
Financial damage	
Damage to the Company's reputation	

Description of the chronology of changes in the nature of the ISI:

Date, time	Description of the nature of the ISI

Participants in the elimination of ISI

№	Post	NAME	Contact information

Interim measures taken to mitigate the impact of IIS:

Measures taken	Description	Date, time	Full name of the employee who took action

Measures taken to eliminate the causes of ISI:

Measures taken	Description	Date, time	Full name of the employee who took action