Appendix
to the Order of Kazakhtelecom JSC
dated "__" _____ 2024
№ _____

INSTRUCTION
on the procedure of users' actions to respond to IS incidents and in emergency (crisis) situations of Kazakhtelecom JSC

Almaty, 2024

CONTENTS.

Chapter 1: General provisions

1. The Instruction on the procedure of users' actions to respond to information security incidents and emergency (crisis) situations of Kazakhtelecom JSC (hereinafter - the Instruction) determines the procedure of users' actions to respond to information security incidents and emergency (crisis) situations of Kazakhtelecom JSC (hereinafter - the Company).

2. The Instruction is developed in accordance with the legislation of the Republic of Kazakhstan and the Information Security Policy of the Company, other internal documents of the Company.

3. This Instruction shall apply to all employees of the Company.

Chapter 2: Terms, definitions and abbreviations

4. The following terms, definitions and abbreviations are used in this Instruction:

1) IS - information security;

2) information security incident (hereinafter referred to as IS incidents) - a single or series of failures in the operation of information and communication infrastructure or its separate objects, which create a threat to their proper functioning and (or) conditions for illegal acquisition, copying, distribution, modification, destruction or blocking of electronic information resources;

3) InfraManager - A system for automating information technology management processes in the Company. Provides automation of incident and service request management, accounting and movement of IT assets and other processes;

4) information and communication infrastructure (hereinafter referred to as ICT) - a set of information and communication infrastructure facilities designed to ensure the functioning of the technological environment for the purpose of creating electronic information resources and providing access to them;

5) user - an employee of the Company who has access to PKI;

6) SVT - computer facilities;

7) SUPB - ASR Remedy's Problem Ticket Management System;

8) the Company's business process management system - software designed to collect, distribute requests and efficiently support corporate users;

9) structural unit responsible for IS (hereinafter referred to as is SP) - a unit exercising internal control over IS provision in the Company;

10) object of informatization (hereinafter - OI) - electronic information resources, software, Internet resource and information and communication infrastructure;

11) SOAR - System for Orchestration, Automation and Response to ISI

12) information system (hereinafter referred to as IS) - A system designed to store, process, search, disseminate, transfer and provide information using appropriate organizational resources (human, technical, financial, etc.);

13) information resource (asset). (hereinafter referred to as IR) - An ordered set of information presented in electronic form (files, databases, algorithms, computer programs, applications, etc.) contained, stored, processed, transmitted and used in the Company's information systems (data transmission networks, systems for storage, processing,

transmission, visualization of information, etc.).

Chapter 3: Procedures for dealing with IS incidents at the Society's I.C.I.

§1. IS incidents

5. IS incidents can occur as a result of intentional actions of an attacker or unintentional actions of users, accidents or natural disasters.

6. IS incidents are categorised in terms of severity and consequences into the following categories:

1) high - IS incidents resulting in complete failure of the information system, information resources, PKI and inability to fulfil their functions, as well as in destruction, blocking, unlawful modification or compromise of the most important information;

2) medium - IS incidents resulting in the failure of individual components of IS, IR, ICI (partial loss of operability, loss of performance).

7. IS incidents of the "High" category include: failures and failures of the Company's IS services, unauthorised access to the Company's IS, unauthorised change of the IS configuration.

8. IS incidents of the "Medium" category include: failure of a workstation with loss of information; failure of OI software; detection of malicious objects in the Company's ICT; non-compliance with the established requirements of regulatory and technical documentation on the Company's IS.

9. The sources of information on the occurrence of IS incidents (hereinafter referred to as the Source) are:

1) users who have detected discrepancies, other suspicious changes in the operation, configuration of IS, IR, PKI or its protection means;

2) technical and software means of information protection;

3) system logs of operating systems and telecommunication equipment that contain records indicating the occurrence or potential occurrence of an IS incident;

§2. Duties and actions of the Company's responsible employees

10. In case an employee independently detects an IS incident, all identified IS incidents are reported to the Information Security Unit and special projects of the Information Technologies Division - Kazakhtelecom JSC's branch through the InfraManager/SUPB system.

11. From the moment information is received from sources, IS SP workers and, if necessary, in conjunction with workers, perform the following actions:

1) determine whether the IS event detected or reported by the employee is an IS incident;

2) localise the area of the ICI involved in the IS incident;

3) restrict access to OI, if necessary, involved in an IS incident;

4) collect information about a live IS incident in progress;

5) engage competent specialists for consultation and co-operation, if necessary;

6) ensure that evidence is preserved and properly processed (taking memory dumps, imaging discs if necessary, etc.);

7) when a malicious object is detected, conduct an initial analysis, and interact with the National Coordination Centre for Information Security of the Republic of Kazakhstan if in-depth analysis is required;

8) analyse all IS incidents recorded in the SOAR;

9) based on the results of the analysis, develop proposals for improving protective measures and preventing the recurrence of an IS incident;

10) Maintain records of IS incidents in SOAR;

11) issue a memo to the Managing Director for Security on the fact of an IS incident.

12. Responsible administrators of server and network equipment, as well as employees carry out work to eliminate the IS incident in their area of responsibility.

§3. Requirements for the development of procedures for restoring operations in the event of a work stoppage

13. Below are the situations on possible emergency (crisis) situations and corrective actions.

I	**Technogenic threats**	
1	**Power outages**	
1.1.	Disruption of power supply	Transferring the operation of main servers and critical workplaces to a backup power supply source
2	**Failure of computer equipment**	
2.1	Server failure	Switching to a backup server, restoring the primary server and switching to the restored server
2.2	Failure of workstations	Switching to a backup workstation, restoring the primary workstation and switching to the restored workstation
3	**Failure of communication equipment**	
3.1	Failure of communication equipment	Switching to standby equipment, restoring the main equipment to serviceability and switching to restored equipment
3.2	Failure of the provider's communication channel	Switching to a backup communication channel, restoring the main communication channel and switching to the restored communication channel
3.3	Failure of telephone communication	Switching to redundant telephone channels, restoring the functionality of the main communication channels and switching to restored communication channels
4	**Intruder attacks**	
4.1	Server failure	Elimination of the vulnerability in the defence and migration to the backup server, restoration of the primary server and migration to the restored server
4.2	Failure of workstations	Elimination of the vulnerability in the defence and migration to the backup workstation, restoration of the main workstation and migration to the restored workstation
4.3	Failure of communication equipment	Elimination of vulnerability in the defence and transfer to backup equipment, restoration of the main equipment operability and transfer to restored equipment

5	**Computer viruses**	
5.1	Server failure	Virus elimination and migration to the backup server, restoration of the primary server and migration to the restored server
5.2	Failure of workstations	Virus eradication and migration to a backup workstation, restoration of the main workstation and migration to the restored workstation
6	**Accidents of life support systems**	
6.1	Failure of sanitary equipment	Calling an equipment repair specialist. In case of equipment damage, transfer to backup equipment, restoration of the main equipment operability and transfer to repaired equipment
6.2	Failure of air-conditioning equipment	Calling an equipment repair specialist. In case of equipment failure, transfer to backup equipment, restoration of the main equipment operability and transfer to the main equipment
6.3	Heating system failure	Calling a repair specialist. In case of equipment failure, transfer to backup equipment, restoration of the main equipment operability and transfer to the main equipment
6.4	Failure of water supply equipment	Calling an equipment repair specialist. In case of equipment damage, transfer to backup equipment, restoration of the main equipment operability and transfer to the restored equipment
II	**Natural hazards**	
1	**Hurricanes**	
1.1	Damage to premises	Organisation of evacuation of employees, visitors, equipment from the premises. In the event of equipment damage, transfer to backup equipment, restore the main equipment and transfer to the restored equipment.
1.2	Evacuation of employees	Organisation of evacuation of employees
1.3	Equipment evacuation	Organisation of equipment evacuation
2	**Earthquakes**	
2.1	Evacuation of employees	Organisation of evacuation of employees
2.2	Equipment evacuation	Organisation of equipment evacuation
III	**Natural and man-made threats**	
1	**Fire**	
1.1	Evacuation of employees	Organisation of evacuation of employees
1.2	Equipment evacuation	Organisation of equipment evacuation

14. Actions on elimination of the causes of malfunctioning, resumption of processing and restoration of damaged (lost) data shall be determined by the functional duties of the responsible employees of structural subdivisions.

15. The event shall be registered by the employee on duty, indicating the exact time of the IS incident, a brief description of the occurrence of the IS incident, and the full names of the notified employees.

16. Removal and removal of equipment from the premises, if the development of an emergency (crisis) situation requires it, shall be carried out by the Company's employees, within the framework of their assigned tasks, only upon agreement with the Company's management.

17. The organisation of work and actions in emergency (crisis) situations is carried out within the framework of the tasks assigned to them.

§4. Requirements for monitoring the implementation of preventive actions to prevent the emergence of emergency (crisis) situations

18. Continuity of the process of ICI functioning and timely restoration of its operability is achieved:

1) Organisational measures, development and updating of documents on the issues of continuity, redundancy and recovery of IS, IR, ICI;

2) regulating the process of information processing with the use of IT systems and the actions of employees;

3) appointment and training of officials responsible for the organisation and implementation of practical measures to ensure redundancy and recovery of information;

4) clear knowledge of and strict compliance by all employees using the IT systems with the requirements of the guiding documents on continuity, redundancy and recovery;

5) application of various methods of resource backup, software benchmarking and information resource backup;

6) effective control over compliance with the requirements of this Instruction;

7) analysing the effectiveness of measures and means to ensure continuity, redundancy and recovery of IS, IR, ICI serviceability, and, if necessary, developing and implementing proposals for their improvement.

§5. Requirements for investigation of incidents and other out-of-order (crisis) situations

18. If necessary, by the decision of the Company's management, a commission shall be appointed and an internal investigation shall be conducted into the fact of occurrence of an IS incident in order to clarify its causes, assess the damage caused, identify the persons involved and take appropriate action.

19. The composition of the committee is determined by the Managing Director for Safety of the Company, and its activities are carried out in a confidential manner.

20. The Commission shall conduct:

1) analysing and identifying the causes of an IS incident and determining the persons involved;

2) Determination of damage caused by an extraordinary (crisis) situation;

3) planning measures to prevent recurrence, neutralise consequences (if possible);

4) analysing and preserving evidence, traces of the IS incident, evidence and testimonies;

5) Determination of penalties to be imposed on those involved;

6) liaising with law enforcement agencies where necessary.

21. When evidence is preserved, if possible, the responsible structural unit shall back up the protected information, technical means involved in the IS incident, including events (logs).

22. Based on the results of the commission's activities, an act describing the situation shall be drawn up. Explanatory materials (copies of the screen, printouts of the event log, etc.) are attached to the act. Based on the results of the investigation, measures are organised to implement the measures proposed by the commission.

23. When conducting investigations, the following questions need to be answered:

1) could the emergency (crisis) situation have been prevented?
2) Is it caused by weaknesses in information security features?
3) is this the first emergency (crisis) situation of its kind?
4) Is the available reserve sufficient?
5) Is there a need to review the defence system?
6) is there a need to revise this Instruction?

Chapter 4: Liability

24. The IS Service of the Company and heads of responsible structural subdivisions of the Company shall control the fulfilment of the requirements of this Instruction.

25. The responsibility for keeping the Rules up-to-date, as well as for making amendments thereto, lies with the IS Service of the Company.

26. The IS SP analyses IS incidents on violations of information protection requirements on an ongoing basis.

27. Heads of SPs are responsible for timely communication of the Instruction requirements to their employees as they relate to them and for fulfilment of the Instruction requirements by employees of subdivisions.

28. Employees of the Company shall be liable in accordance with the legislation of the Republic of Kazakhstan for non-fulfilment or improper fulfilment of the requirements of the Instruction, and reporting of IS incidents in the course of their activities.

29. The Company's IS SP is responsible for administrative and supervisory functions on organisational and methodological management of IS incident response processes.

Chapter 5. Procedure for revision of Instructions

30. The revision of the Instruction shall be carried out on an ongoing basis, but at least once every two years.

31. Amendments and additions to the Instruction shall be made on the basis of a decision of the Managing Director for Safety.

32. Unscheduled revision of the Instruction shall be carried out in case of:

1) changes in regulatory legal documents of the Republic of Kazakhstan, NSD regulator (regulatory and supervisory authorities), the Company's internal documents defining IS requirements;

2) identification of a decrease in the general and/or private level of the Company's IS (based on the results of internal or external audit);

3) significant changes in the Company's organisational activities and/or infrastructure, resources and business processes;

4) identification of material deficiencies or contradictions of this Instruction with other internal documents of the Company.

5) upon identification of deficiencies in the Company's business processes, directly or indirectly related risks or systematically occurring incidents resulting in loss of information assets.

33. The content of this Instruction may be supplemented, but not cancelled (replaced), by provisions of other private IS rules of the Company and documents developed on their basis

Chapter 6. Entry into force. Term of validity

34. This Instruction shall come into force upon its approval by the Chairman of the Management Board and shall be enforced by his respective order.

35. This Instruction shall be binding on all Employees.

Chapter 7. Reference

36. ISO 27005-2010 Information security risk management.
37. ST RK ISO/IEC 31010-2010 Risk assessment methods
38. ISO 9001:2015 Quality management systems. Requirements.
39. ST RK 9001-2016 Quality Management Systems. Requirements.