Annex 2
to the order of DIT - branch
Kazakhtelecom JSC from
"07___"08.2024___ № 172___

Integrated management system/ Service management system/ Information security management system

Plan of measures to ensure continuous operation and asset recovery, related to information processing facilities

DIT/PL 05-28-45

Table of Contents

Chapter 1: Purpose

1. This document "Plan of measures to ensure continuous operation and restore serviceability of assets related to information processing facilities" (hereinafter - the Plan) is a part of the information technology (hereinafter - IT) management system of the Information Technologies Division - Kazakhtelecom JSC's branch (hereinafter - DIT).

2. The present Plan defines preventive organisational and technical measures, providing reduction of risks of emergencies occurrence and impact of consequences of emergencies on DIT activity, as well as order of actions of Employees in case of emergencies, to ensure timely recovery of critical IT services of DIT.

3. The objectives of this Plan are:

1) ensuring the safety of DIT employees;

2) ensuring continuous provision of IT services to DIT;

3) reducing the risks of untimely restoration of critical IT services in case of emergency.

4. Integrated Management System documents relating to the Company's operations in accordance with ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 50001:2018, and their national counterparts ST RK ISO 9001-2016, ST RK ISO 14001-2016, ST RK ISO 45001-2019, ST RK ISO 50001:2019 (hereinafter referred to as the Company's IMS)", as well as Service Management System (SMS) in accordance with ISO 20001:2018/ ST RK ISO/IEC 20000-1-2016, Information Security Management Systems (ISMS) in accordance with the requirements of ST RK ISO/IEC 27001-2023.

Chapter 2: Scope of application

5. This Plan applies to DITs and is advisory in nature for the formation of their own IT business continuity and critical resource recovery plans.

Chapter 3: Terms, definitions and abbreviations

6. The terms and definitions used in this Documented Procedure comply with ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 50001:2018, ISO/IEC 20000-1:2018, and their national counterparts ST RK ISO 9001-2016, ST RK ISO 14001-2016, ST RK ISO 45001-2019, ST RK ISO 50001:2019, ST RK ISO/IES 20000-1-2016, and ST RK ISO 27001:2023.

7. The following designations and abbreviations are used in this document:

Critical Resource Recovery is the aggregate process performed by the DIT to recover processes.

Critical resources - types of business processes that are necessary for the provision of basic products and services, which allow achieving the most important goals (fulfilment of obligations to customers, settlements, etc.), the loss of which may have a maximum negative impact on the Company in the short term and must be restored as soon as possible.

Recovery Team - a team responsible for technical and property analysis of the emergency and taking measures to restore infrastructure and/or services as soon as possible.

Business continuity - strategic and tactical ability of the Company to plan its actions and react to critical events in order to continue critical processes at a certain acceptable level.

Business Continuity Plan - a plan defining the goals, objectives, procedure, methods and terms of implementation of a set of measures applied in time and/or after a critical event for emergency resumption of critical business processes of the Company at a pre-agreed minimum (emergency) level, as well as regulating exclusively the restoration of activities of structural subdivisions and/or business processes of the Company.

Resource Business Continuity Procedures - procedures applied by the Company that realise the Company's business continuity within the framework of the requirements of these Rules.

Testing is an activity in which all or part of the actions in accordance with the Plan are practised.

8. Abbreviations used:

DIT - Information Technology Division;
DTD - Deputy Technical Director.
IS - Information Security;
IT - Information Technology;
A&CD- Analysis and Control Division;
DNA - Division Network Association;
The Company - Joint Stock Company Kazakhtelecom;
OMD – Operational Management Division;
TMS - Problem Ticket Management System;
TD - Technical Director.

Chapter 4: Responsibility and authority

9. The DIT Technical Director is responsible for the implementation of this Plan.

Chapter 5: Plan Description

§1. General provisions

10. This Plan is an internal document of DIT and shall not be transferred to third parties without the authorisation of DIT Management.

11. All detailed information, such as contact information and recovery procedures (as well as other technical information) is "Confidential" and shall not be shared with persons/Employees who are not directly involved in the DIT IT Business Continuity and Critical Resource Recovery Plan process.

§2. Prioritise recovery of critical IT services and their components

12. Critical IT services and their target recovery time were determined within the framework of interviews with representatives of DIT structural subdivisions. Based on the obtained data, all critical IT services provided by DIT are distributed by recovery priorities (Table 1. IT service recovery priorities).

Table 1. IT service recovery priorities

Recovery priority	Reference period
Critical	Up to six hours
High	Until twelve o'clock.
Medium	Up to two days
Low	Up to four days

13.For each critical IT service the list of components on which its provision depends was determined and analysed. The results of prioritisation of critical IT services are presented in the Appendix "Prioritisation of recovery of DIT critical IT services and their components".

§3. plan of organisational and technical measures

14. Taking into account the redundancy of key infrastructure elements, the following organisational and technical measures have been developed:

1)common activities for all recovery priorities;

2)activities for a critical recovery priority;

3)activities for high priority recovery;

4)activities for medium priority recovery;

5)activities for low priority recovery.

15. When developing organisational and technical measures, the following factors affecting the continuity of IT services components are considered:

1)security and life support systems;

2)fault tolerance systems;

3)backup and storage systems;

4)organisational arrangements.

16. The results of the definition of the organisational and technical action plan are presented

§4. Recovery teams and responsibilities of workers

17. A recovery team is defined in DIT for recovery of each critical IT service. The list of IT services and their corresponding recovery teams are given in the Appendix "Recovery Teams and Key Providers of Critical IT Services".

18. The recovery team is managed by the Recovery Team Manager appointed from among DIT employees. In case of unavailability of the Recovery Team Manager, his functions are performed by the Deputy Recovery Team Manager.

19. The leader of the recovery teams is the DIT Technical Director.

20. The Team Leader is responsible for:

1) operational management of recovery teams and coordination of their actions to restore critical IT services and engineering infrastructure equipment (power supply system, uninterruptible power supply (hereinafter - UPS) and climate control equipment) in the DIT area of responsibility;

2) Operational participation with the structural divisions of the DNA in the restoration of engineering infrastructure equipment (power supply system, UPS and climate engineering), which are in the area of responsibility of the DNA.

§5. Responsibilities of the recovery team leader

21. The Recovery Team Leader's responsibilities include:

1)Liaising with higher management within the DIT;

2)Coordination and management of recovery teams;

3)Ensuring that recovery team members are trained in the application of this Plan;

4)Organising the testing of this Plan;

5)Organising regular updates of this Plan;

6)Making decisions on the need to engage key suppliers.

§6. responsibilities of the recovery team manager

22. The Recovery Team Manager has the same responsibilities for administering, coordinating, training, testing, and supporting the Plan as the Recovery Team Leader. However, his/her area of responsibility extends only directly to the recovery team being supervised and the issues within the team's immediate area of responsibility.

§7. Duties of a member of the recovery team

23. Recovery Team Members are responsible for the proper and prompt execution of the Recovery Team Leader's orders, the instructions of the Recovery Team Manager to which the employee belongs, and the proper execution of system recovery procedures.

§8. External data storage

24. External storage should be provided for the following list of data and documents. It is recommended to provide storage at least 10 kilometers away from the office:

1) DIT's business continuity plan for IT resources;
2) Prioritize the recovery of critical DIT IT services and their components;
3) Recovery teams and key suppliers of critical IT services;
4) Procedure for conducting a planned exercise.

25. The geographically remote vault may be a fireproof safe deposit box located at an external DIT service provider or a rented safe deposit box.

§9. Sources of information in the event of an emergency

26. The sources of information on the occurrence of an emergency are:

1) External signs clearly indicating the occurrence of an emergency (fire, flooding, smoke, flames, ignition, etc.);

2) Hardware-software means of protection and monitoring (triggering of fire alarms, etc.);

3) System logs that contain records indicating the occurrence or potential occurrence of an emergency;

4) Users who detected abnormal behaviour in the nature of DIT IT services operation.

§10. Responding to an emergency

27. Upon receipt of information on emergency situation, an employee of the Operational Management Department (hereinafter referred to as the OMS) should fix a problem ticket in the Problem Ticket Management System (hereinafter referred to as the TMS) and further fulfil the duties of the OMS set forth in the Regulation on the process of troubleshooting of resources of Kazakhtelecom JSC's telecommunications networks.

28. In case of obvious signs of an emergency situation (fire, flooding, etc.), the employee of the EIU shall notify the relevant emergency services, according to Annex 3 to this Plan "Contact details" and notify the Technical Director of DIT.

§11. Responding to an emergency

29. The decision on the need to activate the Recovery Plan for critical IT services shall be made by the Recovery Team Leader or, in case of his/her unavailability, by his/her deputy, based on the analysis of the nature of the emergency and its consequences.

30. If the Recovery Team Leader decides to activate the plan:

1) The recovery team leader (or his/her deputy) informs the DIT Management about the emergency, planned activities and expected timeframe for their implementation;

2) As agreed, the Team Leader or deputy will communicate this decision and the necessary information to the relevant Recovery Team Managers, as per the Recovery Teams and Key Critical IT Service Providers Annex;

3) Upon agreement, the Recovery Team Managers or a CBO employee shall notify the recovery team members according to the Annex on the form **"**Recovery Teams and Key Critical IT Service Providers", provide them with the necessary information and inform them of the time and place of the meeting and, if necessary, involve key external IT *service* providers;

4) Considering that information on emergency situations may be confidential, its transfer to third parties without the authorisation of the Recovery Team Leader or DIT Technical Director is prohibited.

31. The mobile phones of Team Leaders, Managers and members of the recovery teams are switched on 24x7 days a week. If contact details change, the GTC will update the information and notify all interested parties of the changes.

§12. Recovery of critical IT services

32. Simultaneously with the commencement of restoration work, users of missing IT services should, where possible, be notified of the start and expected duration of the restoration work. This will allow users to switch to alternative ways of performing their duties.

33. The sequence of IT services restoration should be performed in strict compliance with the approved restoration priorities, which are given in Appendix No.1 "Priority of restoration of DIT critical IT services and their components".

In the process of restoring IT services, recovery teams must consider the need to restore the components corresponding to the IT services.

34. During recovery, additional resources (people, transport, software and hardware, etc.) may be required. The task of the Recovery Team Leader and Managers is to take note of the needs of the structural units and inform the DIT Management about the required resources and related costs.

§13. Procedure of recovery teams' actions in case of any situation resulting in full or partial suspension of IT services provision

35. IT services are assumed to have been completely or partially destroyed as a result of the situation.

36. In general, the actions of recovery teams in a situation resulting in complete or partial destruction of IT services should be as follows:

1) Analysing the consequences of an emergency;
2) Detailed recovery planning;
3) Restoration of IT services according to priorities;
4) Reporting to DIT Management.

37. The detailed procedure for recovery from a situation resulting in a complete or partial interruption of IT services is provided in Appendix 4 to this Plan "Recovery Procedure for a Situation Resulting in a Complete or Partial Interruption of IT Services".

§14. Recovery teams' procedures in case of breach of information security policies and procedures

38. It is believed that a breach of information security policies and procedures may have occurred:

1) Compromising information security and gaining unauthorized access to DIT IT services;
2) Compromising the DIT corporate network.

39. In the event of a compromise to the information security of the DIT IT infrastructure, recovery team actions include, but are not limited to, the following list of steps:

1) blocking/disabling access to the attacked IT service, or stopping IT services;
2) analysing and identifying the possible source of the attack;
3) analysing the consequences of the emergency (investigation);
4) analysing the causes and developing a corrective action plan to restore IT services;
5) informing the DIT Management and, if necessary, competent authorities;
6) implementation of corrective measures aimed at restoring IT services;
7) reporting to DIT Management on the results of the work performed.

40. In case of compromise of information security of the DIT corporate network, the recovery procedures remain identical, with the only difference that the actions of recovery commands are performed jointly with the external provider of services of hosting and support of the DIT corporate network.

41. The detailed procedure for recovery from compromise of information security of IT infrastructure and DIT corporate network is presented in Appendix 5 to this Plan "Recovery Procedure for Breach of Information Security Policies and Procedures".

§15. Testing the plan and analysing test results

42. The plan on ensuring continuity of DIT activity in the field of IT resources should be subject to regular testing, but at least once a year, selectively in structural subdivisions of DIT.

43. Testing the Recovery Plan for critical IT services involves applying the following types of tests:

1) testing using questionnaires;
2) testing without stopping IT services;
3) testing with partial and complete shutdown of IT services.

44. The testing process shall be documented in accordance with Annex 4 to this Plan "Recovery Procedure for a Situation Involving Full or Partial Interruption of IT Services", Annex 5 to this Plan "Recovery Procedure for Violation of Information Security Policies and Procedures".

45. Conduct semi-annual A&CD analysis of identified irregularities/ deficiencies, identify root causes to further improve the testing plan and procedure with report to DIT Technical Director.

§16. Employee training and dissemination of the Plan

46. Heads of structural subdivisions of the technical block, on a regular basis conduct training and informing of DIT Employees, but not less than once a year.

47. Employees involved in the recovery process are required to familiarize themselves with the Plan and, where appropriate, to obtain independent professional certification in business continuity management.

48. The Plan shall be communicated only to Recovery Team Members and Recovery Team Managers. A copy of the Plan shall be provided to the DIT DTDs, TSOs and regions.

§17. Monitoring the implementation of organisational and technical measures

49. The results of the implementation of organisational and technical measures should be monitored regularly, but at least quarterly.

50. The results of monitoring should be formalised and carefully analysed. Based on the results of the analysis, a corrective action plan is developed, aimed at full implementation of organisational and technical measures.

51. It is recommended that the implementation of organisational and technical measures should be monitored by a party independent of their implementation.

§18. Approval and amendment procedure

52. This Plan shall be approved by the General Director of DIT. Annexes of this Plan shall be subject to regular updating by the MA. Revision and updating of this Plan is performed on an annual basis, as well as in case of changes in the list of annexes, Annexes to this Plan "List of critical IT services", "Organizational structure of DIT", etc.

53. The work on revision of this Plan shall be included in the annual work plan of the MA. All interested parties of DIT structural subdivisions shall be notified about changes of this Plan.

Chapter 6. Documentation

54. Plan of organizational and technical measures (Annex 1 to the Plan).

55. List of critical IT services (Annex 2 to the Plan).

56. Contact Information" form (Appendix 3 to the Plan).

57. Recovery procedure in case of a situation resulting in full or partial suspension of IT services (Annex 4 to the Plan).

58. Recovery Procedure for Violation of Information Security Policies and Procedures (Appendix 5 to the Plan).

Chapter 7. References

59. ISO 9000:2015 Quality management systems. Basic provisions and glossary.

60. ISO 9001:2015 Quality management systems. Requirements.

61. ISO 14001:20015 Environmental management systems. Requirements and guidance for application.

62. ISO 45001:2018 Occupational safety and health management systems. Requirements.

63. ST RK 9001-2016 Quality Management Systems. Requirements.

64. ST RK 14001-2016 Environmental Management Systems. Requirements and guidelines for application.

65. ST RK ISO 45001-2019 Occupational safety and health management systems. Requirements.

66. ST RK ISO/IES 20000-1-2016 "Information technologies. Service management. Part 1. Requirements for service management system".

67. DIT/DP-05-08-01 "Documented Information Management".

68. DIT/DP -05-28-50 "Procedure for Conducting Scheduled Exercises."

69. ST RK ISO 50001-2019 Environmental management systems. Requirements and guidelines for application.

70. ISO 50001:2018 Energy management systems. Requirements and guidelines for application.

71. ISO/IEC 20000-1:2018 Information technology. Service management. Part 1. Requirements for a service management system.

72. ST RK ISO/IEC 27001-2023 "Information security, cybersecurity and privacy protection. Information security management systems".

Annex 1
to "DIT/PL-05-28-45 "DIT IT Resources Business Continuity Plan"
in the approved by the order of Kazakhtelecom JSC from _____ № ___

Organisational and technical action plan

№	Activities
1	Ensure and fulfil the requirements of data backup (back-up) regulations for systems operated in DIT.
2	Provide notification when an alarm message is received in the BMS or manually by the DOT analyst for DIT employees.
3	Provision of automatic shutdown of IT services servers with obligatory notification of users in case of main power supply disconnection and diesel generator failure/stoppage.
4	Providing workstations with uninterruptible power supplies with voltage stabilisation capability.
5	Organise a ring topology of the corporate data network, where all active network devices have two independent connections.
6	It is recommended to provide external storage, at least 10 kilometres away, of the following data: - of the backups; - "DIT's IT Business Continuity and Recovery Plan for Critical IT Resources".
7	Organisation of a backup data centre in data centres with the ability to duplicate the following components of IT services: Hardware, Software and Data. Measures for critical recovery priority.
8	Organisation of Internet access channel redundancy by means of last mile redundancy (communication channel to the Internet provider's access node) with the possibility of duplicating the final active network equipment.
9	Interventions for high priority recovery.
10	Organisation of telephone communication from two administrators. The main administrator should ensure that incoming calls can be forwarded to the second administrator if necessary.
11	Ensuring replacement of hardware and components in the warehouse. Warehouses should not be combined with server and communication rooms.
12	Providing images (master copies) of server operating systems with installed applications.
13	Ensuring that images on external media are stored in a fireproof safe.
14	Providing automatic monitoring of website content and, if compromising information is present, automatically updating content from backups.
15	Appointment and training of officials responsible for the organisation and implementation of the following activities: - notifying the hosting provider of the lack of availability of the corporate website; - hardware replacement and application recovery via images; - restore IT services from master copies.

Annex 2
to "DIT/PL-05-28-45 "DIT IT Resources
Business Continuity Plan"
in approved by the order of Kazakhtelecom JSC dated 07.08.2024_ № 172_

A list of critical IT services.

№	IT services	Criterion for successful recovery
1	ABACUS	Successful transmission of an email between two recovery team co-conspirators
2	Active Directory Microsoft	The user sees the main system window and the system provides a response to the request for information
3	ASAP	The user sees the main system window and the system provides a response to the request for information
4	BigData	The user sees the main system window and the system provides a response to the request for information
5	CRM (CRM 2.0, Siebel CRM of branches, Siebel CRM DKB)	The user sees the main system window and the system provides a response to the request for information
6	Cramer NRI	The user sees the main system window and the system provides a response to the request for information
7	GENESYS	The user sees the main system window, and the system allows the problem ticket to be logged and searches for previously logged problem tickets.
8	EDMS	The accountant can open the general ledger
9	ISMET.KZ	The administrator sees the main system window and the system provides a response to the request for information
10	MoneyMap	The administrator sees the main system window and the system provides a response to the request for information
11	Remedy ARS (SUPB, UTO, SUZTORS, REMOTE, SUIST1, SUIST2, CBR, NOVO, PPUA, Contour Reporter)	The user sees the main window of the system and it provides a response to the request for information
12	T-Interconnect	The administrator sees the main system window and the system provides a response to the request for information

13	SAP ERP	The administrator sees the main system window and the system provides a response to the request for information
14	SOA platform	The administrator sees the main system window and the system provides a response to the request for information
15	Telecom.kz	The user sees the main window of the system and it provides a response to the request for information
16	VCIP DBA	The administrator sees the main system window and the system provides a response to the request for information
17	AISTU Sputnik	The administrator sees the main system window and the system provides a response to the request for information
18	SmallWorld GIS	The administrator sees the main system window and the system provides a response to the request for information
19	InfraManager	The administrator sees the main system window and the system provides a response to the request for information
20	IS MTP	The user sees the main system window and the system allows the user to log incidents/requests and searches for previously logged incidents/requests.
21	Automated monitoring system	The user sees the main window of the system and it provides a response to the request for information
22	Billing system (ACP 1.3 branches, ACP 1.3.5 DIS, ACP 1.3.5 DKB, ACP KKM, ACP Channel Lease, ACP BiMEG, Help Megaline)	The administrator sees the main system window and the system provides a response to the request for information
23	Reporting system	The administrator sees the main system window and the system provides a response to the request for information
24	SSPOT MD	Successful creation of a file/directory on the file server
25	STPMS	The user sees the main window of the system and it provides a response to the request for information
26	Netcool JUST	The administrator sees the main system window and the system provides a response to the request for information

27	SUSTF	The user sees the main window of the system and it provides a response to the request for information
28	CheckPoint PAC	Providing access to the vCloudDirector control panel
29	CBS Amdocs	Availability of video.telecom.kz portal, access to viewing video from cameras and archive (if available).
30	IDHost	Portal accessibility
31	VDC	Portal accessibility
32	Intelligent platform	Portal accessibility
33	SDP	Portal accessibility
34	SmartCity	Accessibility of ismet.kz portal
35	IAB	Portal accessibility
36	OFD KKM	Portal accessibility
37	Wi-Fi Target	Portal accessibility
38	Wi Fi SOHO	Portal accessibility
39	ARIS	Portal accessibility
40	SUPP	Portal accessibility
41	Idport.kz	Portal accessibility
42	CEPS	Portal accessibility
43	mail.telecom.kz	Portal accessibility
44	DNS	Portal accessibility
45	EPR	Portal accessibility
46	PBD web module	Portal accessibility
47	4telecom.kz	Portal accessibility
48	Cisco UCM	Portal accessibility
49	FTP	Portal accessibility
50	TJSATS	Portal accessibility
51	OpenAPI	The user sees the main window of the system and it provides a response to the request for information
52	NRI Router	The user sees the main window of the system and it provides a response to the request for information
53	VCS - Telepresence	The user sees the main window of the system and it provides a response to the request for information
54	CMP	The user sees the main window of the system and it provides a response to the request for information
55	IOT	The user sees the main window of the system and it provides a response to the request for information

56	AntiCovid	The user sees the main window of the system and it provides a response to the request for information
57	Wi-fi B2B	The user sees the main window of the system and it provides a response to the request for information
58	Clickhouse AIS DBMS	The user sees the main window of the system and it provides a response to the request for information
59	PTC "Automation of the educational process"	The user sees the main window of the system and it provides a response to the request for information
60	HSE Telecom	The user sees the main window of the system and it provides a response to the request for information
61	IVA MCU	The user sees the main window of the system and it provides a response to the request for information
62	Anti-DDoS AIC	The user sees the main window of the system and it provides a response to the request for information
63	Mirapolis HCM	The user sees the main window of the system and it provides a response to the request for information
64	IS "PostMonitoring"	Portal accessibility
65	IS "Metrological Laboratory"	Portal accessibility
66	IS "Reference Guide"	Portal accessibility
67	IS "Activation of GPON resources"	Portal accessibility

Contact details.

Emergency service	Contact details
Fire Service	101
Police station	102
ambulance	103
Gas Service	104
Rescue Service	112

Annex 4
to "DIT/PL-05-28-45 "DIT IT Resources Business Continuity Plan"
in approved by the order of Kazakhtelecom JSC dated 07.08.2024___ № _172

Recovery procedure in the event of a situation resulting in a complete or partial interruption of IT services.

Recovery actions	Responsible for implementation	Done (Yes/No)
1. Inform the emergency services, see Annex No. 3	EI employee on duty	
Inform the Recovery Team Leader, see Annex No. 2 *(to this Order)*	EI employee on duty	
3. Inform the Recovery Team Managers, see Appendix No. 2 *(to this Order)*	EI employee on duty	
4. Inform the key members of the recovery team and organise their delivery to the recovery site, see Appendix No. 2 *(to this Order)*.	EI employee on duty	
5. Inform DIT Management.	Recovery Team Leader	
6. Obtain all possible information about the nature and extent of the emergency, including: 6.1 Check the list of IT services and determine which services are not available.	Members of the recovery team	
IT service	Mark unavailable IT services	
ABACUS		
Active Directory Microsoft		
ASAP		
BigData		
CRM (CRM 2.0, Siebel CRM of branches, Siebel CRM DKB)		
Cramer NRI		
GENESYS		
EDMS		
ISMET.KZ		
MoneyMap		
Remedy ARS (SUPB, UTO, SUZTORS, REMOTE, SUIST1, SUIST2, CBR, NOVO, PPUA, Contour Reporter)		
T-Interconnect		
SAP ERP		
SOA platform		
Telecom.kz		
VCIP DBA		

Recovery actions	Responsible for implementation	Done (Yes/No)
AISTU Sputnik		
SmallWorld GIS		
InfraManager		
IS MTP		
Automated monitoring system		
Billing system (ACP 1.3 branches, ACP 1.3.5 DIS, ACP 1.3.5 DKB, ACP KKM, ACP Channel Lease, ACP BiMEG, Help Megaline)		
Reporting system		
SSPOT MD		
STPMS		
Netcool JUST		
SUSTF		
CheckPoint PAC		
CBS Amdocs		
IDHost		
VDC		
Intelligent platform		
SDP		
SmartCity		
IAB		
OFD KKM		
Wi-Fi Target		
Wi Fi SOHO		
ARIS		
SUPP		
Idport.kz		
CEPS		
mail.telecom.kz		
DNS		
EPR		
PBD web module		
4telecom.kz		
Cisco UCM		
FTP		
TJSATS		
OpenAPI		
NRI Router		
VCS - Telepresence		
CMP		
IOT		

Recovery actions	Responsible for implementation	Done (Yes/No)
AntiCovid		
Wi-fi B2B		
Clickhouse AIS DBMS		
PTC "Automation of the educational process"		
HSE Telecom		
IVA MCU		
Anti-DDoS AIC		
Mirapolis HCM		
IS "PostMonitoring"		
IS "Metrological Laboratory"		
IS "Reference Guide"		
IS "Activation of GPON resources"		
6.2 Draw up a list of priority IT services to be restored immediately and identify the components of IT services to be restored immediately, see Appendix No. 1 *(to this Order).*	Members of the recovery team	
6.3 Restore IT services and their components independently (determine the general state and operability of the systems), otherwise proceed to step 6.4.	Members of the recovery team	
6.4 Identify and notify key suppliers on which IT service restoration depends, see Appendix No. 2 *(to this Order).*	Recovery Team Manager	
7. Make a management decision with DIT Management on the need to organise a reserve site.	Recovery Team Leader	
8. Organise access to a back-up site (if provided) for key recovery team personnel according to a dedicated list.	Recovery Team Manager	
9. Organise access to a back-up site (if provided) for key users according to a special list.	Recovery Team Manager	
10. Start a backup site: 10.1 Ensure that all workstations are ready 10.2 Redirect the required network traffic to support the required services. 10.3 Organise the work of the PA. The employee on duty at the EIU. 10.4 Organise a printing and printer support service. 10.5 Start supporting business applications. 10.6 Check the availability of applications.	Members of the recovery team	

Recovery actions	Responsible for implementation	Done (Yes/No)
10.7 Check and install the necessary optional equipment.		
11. Get up-to-date backup tapes from the nearest storage facility.	Members of the recovery team	
12. Start the recovery process according to the IT service recovery instructions (in case the IT service was recovered automatically (cluster, etc.), the recovery team members proceed to recovery of the next highest priority IT service).	Members of the recovery team	
13. Record any changes that are made.	Members of the recovery team	
14. Describe the situation in general to the DIT Management and for individual structural units.	Recovery Team Leader	
15. Prepare for DIT Management, as appropriate: • current situation report; • an hourly report of changes verbally.	Recovery Team Leader	
16. Analyse the readiness of IT services to return to the initial state and the possibility of transition to normal operation mode.	Recovery Team Leader	
17. Start the return to the initial state and transition to the normal operation mode of IT services.	Members of the recovery team	
18. Organise, if necessary, round-the-clock operation and accommodation of the recovery team (use hotel services). Provide the recovery team with food.	Recovery Team Manager	
19. Based on test results, ensure adjustments are made to the Recovery Plan for critical IT resources	Recovery Team Leader	

Annex 5
to "DIT/PL-05-28-45 "DIT IT
Resources Business Continuity Plan"
approved by Kazakhtelecom JSC's Order No. 172___ dated 07.08.2024_

Recovery procedure for breach of information security policies and procedures.

Recovery actions	Responsible for implementation	Done (Yes/No)
1.Inform the Information Security Manager/Service Provider of the hacking of the corporate website in order to block it.	EI employee	
2. block the attacker's access to the attacked service (account blocking, firewall configuration, isolation of the attacker's connection point on the network equipment, physical disconnection of the connection point or network segment on the network equipment)/ website.	Information Security Manager/ Website Service Provider	
3. Inform the Recovery Team Leader.	Information security manager	
4. Register the fact of the attack in the logbook.	Information security manager	
5. Obtain all possible information about the attack/hacking of the website, including: 5.1 System logs of operating systems 5.2 Active network equipment logs 5.3 Business application logs 5.4 Firewall logs 5.5 Intrusion detection system (IDC) logs	Recovery team members and Information Security Manager/Website Service Provider	
6. Assess the scope of the attack/website hack and the possible impact on the DIT.	Members of recovery teams and Information Security Manager/ Website Service Provider	
7. Inform the Recovery Team Leader of the incident.	Information security manager	
8. If necessary, inform: DIT management; the competent authorities.	Recovery Team Leader	
9. Start the process of restoring the stopped IT services/website according to the IT service recovery instructions	Recovery Team Members/ Website Service Provider	
10. Prepare reports for DIT Management (if necessary).	Recovery Team Leader	
11. Based on test results, ensure adjustments are made to the Recovery Plan and activities.	Recovery Team Leader	