Appendix
to the Order of Kazakhtelecom JSC
dated __ _____ 2022
No. _____

Network Security Policy of Kazakhtelecom JSC

Almaty, 2022

Contents

1 Terms, abbreviations and definitions

Authorization - granting access rights to a subject, as well as granting access in accordance with the established access rights;
IS administrator - a privileged user who has extended powers (privileges) to configure and operate the IS, as well as to manage access to the IS;
Authentication - verification of access subject's belonging to the identifier presented by him; confirmation of authenticity;
IR Business Owner – a subject, structural subdivision, department, service that exercises the powers of ownership, use and disposal of IR information in accordance with its functions, tasks and within the limits established by law. The IR Business Owner is determined at the IR creation stage;
IS – information security. The state of security of information resources and systems, which ensures their confidentiality, integrity, authenticity and availability, which is achieved by a whole range of organizational and technical measures aimed at protecting data;
IR - information resource (asset). For the purposes of this Policy, it means an ordered set of information presented in electronic form (files, databases, algorithms, computer programs, applications, etc.) and contained, stored, processed, transmitted and used in the Company's information systems (data transmission networks, systems for storage, processing, transmission, visualization of information, etc.);
IS - information system. A system designed to store, process, search, distribute, transmit and provide information using appropriate organizational resources (human, technical, financial, etc.);
IT - information technologies, process of creation, storage, transmission, perception of information and methods of realization of such processes;
RD - regulatory documentation of the Company (policies, standards, orders, regulations, guidelines, instructions, etc.);
Company - Kazakhtelecom Joint Stock Company;
Policy – this Policy on access control to the information resources of Kazakhtelecom JSC, approved by the Company;
User - the Company's employee or third party representative working with the Company's IS and using its IR in accordance with the established rights and rules of access to information;
SS – a structural subdivision of the Company;
IT SS - a structural subdivision of the Company responsible for IT, technical maintenance and operation of the Company's IR and IS;
Third Party, third person - an individual or legal entity interacting with the Company on the basis of contractual relations;
Access subject - a person or process whose actions are regulated by the rules of access differentiation. Access subject may mean both users and administrators of the Company's IR and service accounts required for the Company's IR functioning.

2 Purpose of the Policy and its scope

1. This policy defines the general principles of the provisions, rules and practices that establish the organization's approach to the use of network resources and determine how to ensure the protection of the Company's network infrastructure and services.

2. The policy is a regulatory document and is intended for mandatory use within the Society.

3. The provisions of this Policy are aimed at:

1) creation of a unified approach to IS provision when protecting the Company's network infrastructure and services in order to control access to information;

2) preventing unauthorized access;

3) ensuring authorized access to the IR, operating systems and information in application systems;

4) determining the procedures and requirements, the implementation of which is mandatory to ensure the efficiency of the Company's operations, preserve its reputation and fulfill the Company's obligations to counterparties;

5) delimitation of powers and determination of responsibility for IS provision when ensuring protection of the Company's network infrastructure and services.

4. Provisions of this Policy are intended to reduce potential danger (risks) for the Company from damage that may be caused by unauthorized use of the Company's IS.

5. The Policy applies to all the Company's IR, as well as to all persons (employees of the Company, third parties, etc.) having electronic (digital) access to the Company's IR.

6. The Policy regulates the procedure for ensuring protection of the Company's network infrastructure and services, the procedure for controlling compliance with the provisions of the Policy and responsibility for non-compliance.

7. The Policy is intended for distribution within the Company and provision to all Managers, Employees of the Company and other interested parties - participants of the Company's business processes.

8. All exceptions to the rules and requirements of this Policy shall be agreed with the IS SS.

3 General provisions and requirements of the Policy

9. The Policy is developed in accordance with the legislation of the Republic of Kazakhstan in the field of IS, RD of the regulator (regulatory and supervisory authorities), IS Policy of the Company, IS Concept of the Company, a series of international standards on IS ISO/IEC 27000, COBIT, ITIL, the current state and near-term prospects of development of the Company's information structure and the possibility of modern organizational and technical methods of information protection.

10. The provisions of the Policy shall be revised on a permanent basis, but at least once every two years.

11. Unscheduled revision of the Policy shall be carried out in case of:

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

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

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

4) identification of significant deficiencies or contradictions of the Policy provisions with other internal documents of the Company;

5) upon identification of deficiencies in the Company's business processes directly or indirectly related to information security, as well as realization of corporate risks or systematic incidents resulting in loss of information assets.

12. The provisions of the Policy may be supplemented, but not canceled (replaced), by the provisions of other internal IS policies of the Company and documents developed on their basis.

13. Additional information on safe operation and information protection in the Company's IS can be obtained from other internal IS policies of the Company.

14. Agreed, formalized processes of access management to the Company's IS are one of the basic mechanisms of information protection in the Company.

15. All the Company's IS shall be identified, accounted for, systematized, categorized in the form of an IS register and shall have their business owners.

16. Procedures (instructions, rules, requirements, etc.) for the work of IS users and administrators agreed with the IS SS shall be developed and kept up to date for each IR of the Company.

17. The software and technical component of each Company's IR shall be maintained by one or another authorized operational (operational) SS.

18. The creation and maintenance of the Company's IS register shall be assigned to the SS responsible for the IS in accordance with the established procedure,

19. An up-to-date IR register shall be available to all users at any moment of time.

20. Information on the new IR (changes in the existing IR) shall be communicated by the SS - business owner of the IR to the SS authorized to maintain the IR register within two business days of its appearance in the form of a memo or in another official form accepted by the Company, e.g. by means of an automated electronic system, etc., agreed and signed by the head of the SS - business owner of the IR.

21. Amendments to the IR register shall be made by the SS authorized for maintenance of the IR register within two business days from the date of appearance in the form of a memo or in another official and accepted form in the Company, e.g. by means of an automated electronic system, etc., agreed and signed by the head of the SS - business owner of the IR.

22. The use of the IR shall be carried out in accordance with the operating instructions for software and hardware, and other internal RDs.

23. It is forbidden to intentionally disable the IR, block access to it and any other actions that prevent the regular operation mode of the IR.

24. Users or other responsible person (unit) shall report all facts (incidents) related to violation of IS requirements and provisions of the Policy, violation of the rules of access to the Company's IRs, detection of a failure in the operation of IRs, etc. to the IS.

25. The IS connected to the Company's network shall have anti-virus software installed with configured automatic signature updates where permissible and technically feasible.

26. Network devices in the Company's network shall ensure fault tolerance of service provision and provide for the possibility of operational recovery.

27. Data transmission network bandwidth shall be continuously monitored to enable prompt response to DDoS attacks using targeted attack defenses and infrastructure intrusion prevention techniques.

28. There shall be defined rules for access to Internet network services to which the Company's employees shall have limited access.

29. Rules for access to the Company's IR and IS shall be defined.

30. In order to filter (skip or block) the data flow, firewalls should be used with the application of access rules necessary and sufficient for the operation of the service.

31. It is necessary to ensure disabling of unused services on all IS and IR.

32. Ensuring that the state of data flows is analyzed for breaches and hacks, through intrusion detection systems that detect and prevent various types of hacks.

33. Conducting effectiveness testing of information security tools.

34. Provision of access to the IR and IS may be made only for legitimate purposes that do not contradict the interests of the Company and the laws of the Republic of Kazakhstan.

35. Actions of users and administrators of the Company's IR shall be logged within the framework of provided access to the IR.

36. Audit logs of information/network security events of the Company's IR and IS shall be informative, protected from modification and stored for the period of time potentially necessary for use for investigation of possible incidents related to IS violation, but not less than three years and shall be available for operational access for at least two months.

4 Procedure for ensuring network security

37. All users are granted access to the Company's IR only on the basis of requests documented and agreed upon, including with their business owners. No access is defined by default. Formalization, coordination and approval of applications when granting access to the IR shall be carried out in accordance with the established procedure and subject to the requirements of the provisions of this Policy.

38. Network accessibility to the IR shall comply with the requirements and forms of implementation developed and adopted by the Company and shall contain the following minimum information:

1) data on the functional purpose of the IR;

2) name of the IR in accordance with the register;

3) list of ports, protocols and ip-addresses for interaction necessary and sufficient for operation of the IR;

4) logical and physical connection scheme of the IR;

5) business owner of the IR.

39. To grant access to/from the IR, one of the following conditions must be met:

1) access is necessary for the user to perform his/her job duties in accordance with his/her job description and authority;

2) access to/from the IR is necessary for interaction with other IRs;

40. The person initiating the granting of access shall be obliged to provide an appropriate justification of the need to grant access.

41. The general procedure for granting access to the Company's IR shall include the following stages:

1) the initiator, represented by the head (substitute person) of the interested joint venture, shall duly execute an application for granting access to/from the IR in accordance with the IR register.

2) the application is approved by the business owner(s) of the IR;

3) the application is approved by the IS SS, which within one business day verifies the existence of grounds for access to the IR according to the application. If access to the IR according to the application cannot be granted for any reason, the application is returned to the initiator, with a detailed description of the reason for refusal.

4) In case of necessity of temporary provision of access, the IS SS shall provide access for the established validity period;

5) Upon expiration of the established validity period of the granted access to the IR, the IS SS shall finalize the provision of access to the Company's IR with notification of the initiator and the business owner(s) of the Company's IR.

6) information on approved requests for granting access to the IR shall be recorded by appropriate logging tools (audit trail) used within the framework of the IR access management.

42. Provision of access to third parties' RI shall be made only on the basis of valid contracts and/or agreements.

43. Third-party access to the Company's IR shall be granted for the period and to the extent necessary to carry out work on the basis of IS compliance agreements, which shall contain confidentiality clauses, terms on compensation for damages arising from IS violations, as well as failures in the operation of IR and violation of its security caused by third-party interference.

44. Based on the assessment of the IS risk associated with the access of third party D&I, the IS SS shall provide for the following organizational and/or software and hardware measures to control the activities of third parties:

1) verification of the outcome of third party IR activities;

2) maintaining an audit trail on the actions of third-party IRs;

3) recording the session of access to information assets by special program-technical complexes.

45. The IS SS shall be obliged to conduct periodic monitoring (audit) of compliance with network security rules.

5 Procedure for changing access rules

46. In case it is necessary to provide additional rules on access to the IR it already uses, it should act in accordance with the provisions of this Policy regulating the procedure for granting access to the IR.

47. In case it is necessary to replace (fully or partially) the authority to access the IR already used by him/her, one should act in accordance with the provisions of this Policy regulating the procedure for revoking the access to the IR.

6 Procedure for canceling access rules

48. Access rights to/from the IR are cancelled and/or blocked in the following cases:

1) changes in the functional tasks of the IR;

2) expiration of the application validity period (access validity period);

3) changes in technological processes for processing information in such a way that access is no longer required;

4) violation of the rules for access to/from the IR;

5) absence of production necessity;

6) termination of contractual agreements with third parties;

7) at the request of other management of the Company.

49. Cancellation of access rights must be initiated within one business day from the moment of occurrence of the relevant event (fact).

50. The responsibility for initiating the cancellation of user access to the IR is assigned to the business owner of the IR.

51. Information about the initiation of access cancellation (indicating the reason) is communicated in the established official form accepted in the Company, for example, through an automated electronic system, etc. by the head of the interested SS to the SS IB.

52. The actual implementation of the cancellation of access to the IR is carried out by the authorized SS - the business owner of the IR, after receiving approval from the SS IB.

53. Information about the cancellation of access to/from the IR must be recorded by appropriate logging means (maintaining an audit trail) as part of the management of access to the IR.

7 Control of access rules

53. The IS SS shall periodically check (audit) compliance with the rules of access to/from the IR in accordance with the requirements of the Policy provisions.

54. To ensure effective access control, a formal process of regular verification of the rules of access to/from the IR shall be maintained that meets the following requirements:

1) IR access rules should be reviewed at regular intervals (at least semi-annually) and after any changes to the IR;

2) IR access rules shall be checked and reassigned when their functional tasks change;

55. Controls over the implementation of IR access management procedures shall include:

1) control over addition, deletion and modification of ports, protocols, ip addresses;

2) immediate blocking of access rights when changing the functional tasks of the IR;

3) inclusion of third parties to interact with the Company's IR only for the period of work (agreement);

4) familiarization with authentication rules and procedures for all users having access to restricted data;

5) use of authentication mechanisms when accessing any database containing restricted data, including access by applications, administrators and any other users;

6) allowing queries and direct access to databases only for database administrators;

7) blocking access to/from the IR in case the monitoring (review, analysis, audit) of security event logs reveals IR actions that are classified by the operator (administrator) as IS violation events.

56. Control and periodic review of the rules of access to/from the IS shall be carried out in the course of IS audit in accordance with the established procedures.

8 Roles and Responsibilities

57. Control over fulfillment of the requirements and rules shall be entrusted to the Company's IS structural division.

58. Responsibility for the relevance of this Policy, as well as its amendments shall be assigned to the IS structural division of the Company.

59. Responsibility for ensuring proper fulfillment of the requirements and rules of the Policy shall be assigned to all interested structural subdivisions of the Company within their authorities and in accordance with the provisions established by this Policy and the documents developed on its basis.

60. Heads of structural subdivisions shall be responsible for timely communication of the Policy requirements to the employees of their subdivisions and/or representatives of third parties as far as they are concerned and for fulfillment of the Policy requirements by the employees of their subdivisions and/or representatives of third parties.

61. The IS structural unit of the Company shall be responsible for proper organization and implementation of general control over compliance with the requirements and rules of this Policy, as well as for administrative and supervisory functions of organizational and methodical management of network security processes.

62. Business owners of the IR are responsible for coordinating access to/from the IR.

63. Implementation of the provisions of this Policy and procedures related to operational (maintenance) support of the processes of managing access to/from the IR and support of the IR users shall be assigned to the Company's structural subdivisions that provide technical support and maintenance of the operational activities of the users and the Company's technical systems and facilities that ensure the operation of the IR.

64. All users are responsible for their actions when working with the Company's IR and handling the Company's protected IR, as well as for fulfillment of requirements and rules established by this Policy and internal documents developed on its basis.

65. In case of detection of violations of the requirements of this Policy by an IR user (IR administrator), which have caused or may have caused serious damage to the Company's business activities, the management of the SS shall notify the IS SS of the incident on a mandatory basis and an internal investigation shall be initiated and conducted with the involvement of interested SSs and in accordance with the approved IS Incident Investigation Procedure.

66. Violation of the provisions of the Policy, including any intentional action taken to breach, block or otherwise circumvent established IS controls, may result in disciplinary action in accordance with labor laws, also administrative or criminal penalties in accordance with applicable laws.

67. The decision on application and selection of liability measures shall be made by the Company's management based on the results of an internal investigation, depending on the

expediency of application of the measures in question, as well as on information about the willfulness of the violation.