Appendix
to the Order of Kazakhtelecom JSC
dated __ _____ 2023
No. _____

Policy of managing access to information resources of Kazakhtelecom JSC

Almaty, 2023

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 unit, department, service, realizing the authority to own, use and dispose of the information of the IR in accordance with its functions, tasks and within the limits established by law. IR Business Owner is determined at the stage of creation of the IR;
IS - information security. The state of protection of information resources and systems, when their confidentiality, integrity, authenticity and availability are ensured, which is achieved by a whole complex of organizational and technical measures aimed at data protection;
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.);
IR Register is a list of information resources in electronic form. The owner of the IR Register is the SS IT.
IS - information system. A system designed to store, process, search, disseminate, transfer and provide information using appropriate organizational resources (human, technical, financial, etc.);
RD means the Company's regulatory documents (policies, standards, orders, regulations, guidelines, instructions, etc.);
Company - Kazakhtelecom Joint Stock Company;
Policy - this Policy of access management to information resources of Kazakhtelecom JSC approved by the Company;
User - an employee of the Company or a representative of a third party working with the Company's IS and using its IR in accordance with the established rights and rules of access to information;
SS - structural subdivision of the Company;
SS IT - a structural subdivision of the Company responsible for IT, maintenance and operation of the Company's IR and IS;
Third party, third person - an individual or legal entity, contractor, supplier, partner, counterparty, contracting party, etc., interacting with the Company on the basis of contractual agreements and not being a full-time employee of the Company;
Access subject - a person or process whose actions are regulated by the rules of access differentiation. An access subject may mean both users and administrators of the Company's IR, as well as service accounts required for the Company's IR functioning.

2 Purpose and scope of the Policy

1. This Policy defines the general principles of providing and managing access to the Company's IR.

2. The Policy is a regulatory document and is intended for mandatory use in the Company.

3. The provisions of this Policy are aimed at:

1) creation of a unified approach in ensuring IS when providing and managing access to the Company's IR 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 procedure and requirements, the implementation of which is mandatory to ensure the efficiency of the Company's activities, preservation of its reputation and fulfillment by the Company of its obligations to counterparties;

5) delimitation of powers and determination of responsibility for IS provision and management of access to the Company's IR.

4. The provisions of this Policy are intended to reduce potential danger (risks) for the Company from damage that may be caused as a result of 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 granting and managing access to the Company's IR, the procedure for controlling compliance with the provisions of the Policy and responsibility for non-compliance therewith.

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 SS IS.

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 private IS policies of the Company and documents developed on their basis.

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

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

15. All 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 SS IS shall be developed for each IR of the Company and kept up to date.

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

18. Creation and maintenance of the Company's IS Register shall be assigned to the IT SS in accordance with the established procedure.

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

20. Information on the new 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 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.

21. Amendments to the IR register shall be made by the SS IT authorized to maintain the IR register within two working days from the date of appearance in the form of a memo or in another official and accepted form in the Company, agreed and signed by the head of the SS - business owner of the IR.

22. The IR shall be used in accordance with the operating instructions for software and hardware, and other internal RD.

23. It is prohibited to deliberately disable the IR, block access to it and any other actions preventing normal operation 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 IR, detection of a failure in the operation of the IR, etc. to the IS.

25. Provision of access to the IR shall be made by forming and implementing roles to ensure that the access rights (powers, privileges) of the users and administrators of the IR correspond to their functional responsibilities. The aggregate of such roles constitutes a matrix of access to the IR, which is formed in electronic form or on paper. For each IR, the

Company shall develop, implement and use an appropriate access matrix, which shall be coordinated with the SS IS.

26. “Role” management shall be the main mechanism for managing access rights (powers, privileges) of users and administrators of IR in the Company.

27. Roles shall be formed taking into account the principle of minimum authority. The level of authority of an access subject shall comply with the principle of minimum sufficiency for solving the functional tasks and/or job responsibilities assigned to the access subject (user).

28. No role shall allow a user to perform critical operations (deletion of data, change of privileges, etc.) individually.

29. Critical workflows shall be protected from erroneous and unauthorized actions by administrators. Routine administration, diagnostic and recovery procedures should be performed through special roles in the IR without direct access to data. In critical systems, by decision of the business owner of the IS, the role of the IS administrator of the IS may be introduced, whose functions include confirmation of the rights and authorizations of users entered in the system by its IS administrator.

30. The process of management (creation, implementation, modification, use, etc.) of access matrices and roles shall be carried out in accordance with the developed procedures (rules, instructions, etc.) and shall be implemented in some official and accepted form in the Company, for example, by means of an automated electronic system, etc., based on the requirements of the provisions of this Policy, the legislation of the Republic of Kazakhstan in the field of IS, RD of the regulator (regulatory and supervisory authorities) and international IS standards.

31. The list of those IS to which access rights “by default” are granted (i.e. the minimum set of IS required for the work of a particular unit/employee), as well as the “default” access rights themselves shall be defined. Such access rights should be minimal.

32. Access may not be granted to an employee of the Company without the approval and consent of his/her immediate supervisor, or in the case of third parties - the responsible person of the Company (subdivision - supervisor), a signed non-disclosure agreement (NDA), approval and control by the SS IS.

33. Provision of access to the Company's IR cannot be full and unlimited in time.

34. Users are prohibited to use someone else's authorization to access the Company's IR and/or transfer such authorization to someone else (transferring one's password to another person);

35. Each IR user shall be assigned a unique identifier (user name). Access to all the Company's IR shall be based on user authentication and authorization.

36. Passwords, multi-factor method, physical code carriers, biometric parameters and other carriers, methods may be used as authentication methods.

37. The initial logon password or physical medium must be presented to the user in a manner that precludes the possibility of compromise.

38. Interactive procedures shall be utilized to change the user's password during the process to ensure sufficient passwords are available.

39. The user shall be required to change his or her IR access password on a regular basis, and the functionality of the IR shall allow for this.

40. Direct user access to databases shall not be granted.

41. All password actions shall be performed in strict compliance with the requirements of the Password Protection Policy provisions.

42. Access to the IR is not provided (terminated) in case of lack of industrial necessity, changes in functional and job responsibilities, employee dismissal, contract termination or breach of contracts and/or agreements.

43. Access to the IR may be provided only for legitimate purposes that do not contradict the interests of the Company and the laws of the Republic of Kazakhstan.

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

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

4 Procedure for granting access

46. 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.

47. Applications for granting access to the IR shall comply with the requirements and implementation forms developed and adopted by the Company and shall contain the following minimum information:

1) data on the person (subject) to whom access is granted (full name, position, division);
2) name of the IR in accordance with the register to which access is requested;
3) list of requested access roles (and in case the roles are not defined - access rights);
4) date of granting access and justification for granting access;
5) term of validity for which the access is granted.

48. In order to grant access to a user to 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 is necessary for the user to perform the duties of another user on the instructions (in the form of a memo) of the SS manager;
3) access is necessary for the user to perform the duties of another user upon instruction (in the form of an order or instruction) of the Company's management;
4) access is necessary for the user to perform the work as instructed (in the form of an order or instruction) by the Company's management;
5) access is necessary for the user to perform work in the course of realization of contracts, agreements, contracts concluded by the Company (for representatives of third parties).

49. The person initiating the provision of access shall be obliged to submit a corresponding justification of the need to provide access.

50. The person to whom access is granted (subject of access) shall be familiarized with this Policy and other private IS policies of the Company regulating the use of the IR.

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

1) the initiator, represented by the head (substitute person) of the interested SS, shall duly execute an application for granting access to 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 SS IS, which within one business day checks whether the user has 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 shall be returned to the initiator with a detailed description of the reason for refusal.

4) the responsible SS shall grant access for the established validity period;

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

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

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

53. 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 provisions, conditions for compensation for damages arising from IS violations, as well as failures in the operation of IR and violation of their security caused by third-party interference.

54. Based on the assessment of the IS risk associated with third party access, 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 result of third party activities;

2) carrying out the activities of third parties only in the presence of the Company's responsible employees;

3) maintaining an audit trail on the activities of third parties;

4) recording the session of access to information assets by special software and hardware complexes.

55. The SS IS shall be obliged to conduct periodic monitoring (audit) of compliance with the rules of access provision.

5 Procedure for Changing Access Rights

56. If it is necessary to grant a user additional powers (roles) to access the already used by him/her IS, it is necessary to act in accordance with the provisions of this Policy regulating the procedure for granting access to the IS.

57. If it is necessary to replace (fully or partially) the user's authority (roles) to access the IR already used by the user, one should act in accordance with the provisions of this Policy regulating the procedure for canceling access to the IR.

6 Procedure for revoking access

58. Access rights to the IR are revoked and/or accounts are blocked in the following cases:

1) changes in the functional and/or job responsibilities, staffing schedule, or form of employment of the employee;

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

3) changes in the technological processes of information processing such that the user no longer requires access;

4) violation of the rules for access to the IR by the user;

5) the employee goes on maternity leave (parental leave);

6) prolonged absence, inactivity of the employee lasting more than 45 calendar days;

7) change of position, form of employment, or dismissal from the Company;

8) lack of production necessity;

9) termination of contractual agreements with third parties;

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

59. In case of changes in functional and/or job responsibilities, staffing schedule, form of employment, etc. all existing access rights of the Company employee are cancelled and new access rights are assigned corresponding to his new duties and status in accordance with the requirements of the provisions of the Policy.

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

61. The responsibility for initiating the cancellation of the user's access to the IR is assigned:

1) in the event of expiration of the validity period of the granted access, change of functional and/or job responsibilities, staffing schedule, form of employment, etc. of the Company employee or his dismissal, change of technological processes of information processing in such a way that the employee no longer requires access - to the immediate supervisor, the relevant interested SS;

2) in the event of detection of accesses with violations of validity periods, violations by the user of the rules of access to the IR and/or other requirements of this Policy - to the SS IT or the SS IS during audits.

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

63. The actual implementation of access cancellation to the IR is carried out by the authorized SS IT, after receiving approval from the SS IS.

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

7 Control of Access Rights

65. The SS IS shall periodically check (audit) compliance of access rights to the IR with the access matrix, as well as control over revocation of access rights to dismissed

employees and blocking of access to long-term absent employees, etc., in accordance with the requirements of the Policy.

66. To ensure effective access control, a formal process for regular review of user access rights must be maintained that meets the following requirements:

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

2) access rights of users shall be checked and reassigned when their job responsibilities within the Company change, as well as when they move from one job to another within the Company;

3) verification of the rights of users having special privileges for access to the system should be performed more frequently (but at least once every 6 months);

4) it is necessary to regularly check the adequacy of assigned privileges to avoid any of the users obtaining excessive rights;

5) changes to privileged accounts should be logged.

67. Controls over the implementation of user access management procedures should include:

1) controls over the addition, deletion, and modification of identifiers, authentication data, and other identity objects;

2) authentication of users before changing passwords;

3) immediate blocking of access rights upon termination;

4) blocking of accounts inactive for more than 45 days;

5) enabling accounts used by third parties for remote support (work) only while work is in progress;

6) tracking remote accounts used by third parties during the work;

7) familiarizing all users who have access to restricted information with authentication policies and procedures;

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

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

10) blocking the account for a period of 30 minutes or until the account is unblocked by the administrator;

11) blocking of user accounts when the results of monitoring (viewing, analyzing, auditing) of security event logs reveal user actions that are classified by the operator (administrator) as IS violation events.

68. Control and periodic review of user access rights to the IS shall be performed in the course of IS audit in accordance with the established procedures of the IS Audit Policy.

8 Roles and Responsibilities

69. Control over fulfillment of the requirements and rules, as well as responsibility for the relevance of this Policy (amendments thereto) shall be assigned to the Company's IS structural subdivision.

70. 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.

71. 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.

72. The Company's IS structural subdivision 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 performing administrative and supervisory functions on organizational and methodical management of the processes of access to the IR.

73. The business owners of the IR are responsible for coordinating access to the IR.

74. Implementation of the provisions of this Policy and procedures related to operational (maintenance) support of the processes of managing access to 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.

75. HR structural subdivisions of the Company shall be responsible for mandatory and timely provision of information on changes in the staffing table in respect of dismissed and/or temporarily unemployed, long-term absent employees of the Company to the Company's IS structural subdivision to ensure fulfillment of the requirements of the provisions of this Policy in terms of control and audit of accesses to the Company's IR. The information shall be provided in an official and accepted by the Company form, e.g. by means of an automated electronic system, etc. Provision of information shall be performed:

1) on a regular basis, upon occurrence of the above changes confirmed by agreed dispositive documents (orders, instructions, etc.);

2) on a monthly basis in the form of a summary report with information on all the above changes for the reporting period.

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

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

78. Violation of the provisions of the Policy or the documents developed in support of this Policy, including any intentional action taken to breach, block or otherwise circumvent established IS controls, may result in administrative or criminal penalties in accordance with applicable law, as well as the Company's Personnel Management RD.

79. The decision on the 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 appropriateness of the measures in question, as well as information on the willfulness of the violation.