**Appendix**
**to the Order of Kazakhtelecom JSC**
**dated __ ____________ 2023**
**No. ________**

# Policy of ensuring security of remote access to the resources of Kazakhtelecom JSC's networks and information systems

Almaty, 2023

## Contents

## 1 Terms, abbreviations and definitions

**IS UDS** - information system “Unified Directory Service”. A centralized software and hardware complex of the Company created on the basis of Microsoft Active Directory software;

**IS** - information security. The state of protection of information resources and systems, which ensures their confidentiality, integrity, authenticity and availability, 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.);

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

**IT** - information technology. Processes, methods of searching, collecting, storing, processing, providing, distributing information and ways of implementing such processes and methods;

**Local access** or connection means the process of gaining access to the Company's networks and IS locally, in places and at facilities owned and controlled by the Company (buildings, offices, branches, representative offices, other separate SS, including those located in another area);

**RD** - the Company's regulatory documents (policies, standards, orders, regulations, guidelines, instructions, etc.);

**Company** - Kazakhtelecom Joint Stock Company;

**Software** - software;

**Policy** - this Policyof ensuring security of remote access to the resources of Kazakhtelecom JSC's networks and information systems 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;

**Computer equipment(CE)** means computer equipment (stationary computers or workstations, portable computers or notebooks, etc.);

**SS** - structural subdivision of the Company;

**Third party, third person** - an individual or legal entity, contractor, supplier, partner, counterparty, contractual partner, etc., interacting with the Company on the basis of contractual agreements and not being a full-time employee of the Company;

**Remote access** means the process of gaining access to the Company's networks and IS from other (third-party) networks, including the Internet, which are not permanently physically or logically connected to the Company's networks and are not under the Company's control.

## 2 Purpose and scope of the Policy

1. This Policy defines a set of rules, requirements and acceptable methods for the procedures of provision, use, control and IS provision of remote access from third-party (external) networks to the Company's network and IS resources.

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

3. The rules and requirements of the Policy are intended to minimize the Company's potential danger (risks) from damage that may be caused by unauthorized use of the Company's resources.

4. The Remote Access Policy covers all resources of the Company's networks and IS that are used for remote access. The Company's network and IS resources include data, information, software, hardware, maintenance and telecommunications. The Policy applies to all persons who use remote access to the Company's network and IS resources in their activities, including all employees and representatives of third parties using these resources.

5. The Policy applies to all types of technical implementations of remote access using any types and kinds of IT systems used to connect to the resources of the Company's networks and IS.

6. The Policy is intended to be distributed within the Company and provided to all Managers, Employees of the Company and other interested parties - participants of the Company's business processes.

## 3 General provisions and requirements of the Policy

7. 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.

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

9. 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 internal or external audits);

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.

10. 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.

11. Remote access is a privilege that shall be subject to additional controls reflecting the additional risks it poses to the Company's network and IS resources to which access is granted.

12.The principles of remote access set forth in the provisions of this Policy shall apply to all types and forms of connections, including through xDSL, xPON, etc. technologies, to the Company's networks and resources from locations and facilities not owned or under the physical control of the Company: buildings, hotels, third-party offices, branch offices (located physically separate from the Company's premises), home offices, representative offices, other separate SS, including those located in another location, etc.;

13.Remote access has the same meaning and status as local access to the Company's network and IS resources and is subject to the same requirements of the applicable RD as local access.

14.Provision of remote access to the Company's IR and IS cannot be full (in terms of rights, level of access to IR/IS, etc.) and unlimited in time.

15.By default, remote access is disabled for any user in the Society.

16.Remote access should be granted to users only when objectively necessary.

17.Remote access shall not be granted to an employee of the Company without the approval and consent of his/her immediate supervisor (substitute).

18.Remote access for third parties shall be provided only on the basis of valid contracts and/or agreements.

19.The process of obtaining, changing or canceling remote access for a user shall be official and organized in accordance with this document, in accordance with the remote access management procedure (methodology, instructions, rules, etc.), which shall be developed on the basis of the provisions of this Policy, other RD and IS Policies of the Company, IS legislation of the Republic of Kazakhstan, RD of the regulator (regulatory and supervisory authorities) and international IS standards.

20.The remote access management procedure for the Company's employees (methodology, instructions, rules, etc.) shall ensure registration of the following information:

1) data on the person to whom access is granted (full name, position, division, etc.);

2) the purpose of providing remote access;

3) a list with the names of IS or IR to which remote access is organized;

4) the date of granting access and justification for granting access.

21.Remote access users must be registered in the IS UDS and have valid personal credentials (records) - login and password. It is possible to use other authentication methods, such as multi-factor methods, hardware keys, certificates, etc.

22.Account role management within the framework of providing users with remote access should be based on the available functionality of the IS UDS, in which, based on the relevant developed procedures (methods, instructions, rules, etc.), should also be performed distribution of user credentials to certain groups, to which further should be applied privilege and security management policies in the systems of technical support of remote access (security gateways).

23.All actions performed in the IS UDS as part of remote access management (granting, modifying, canceling, etc.) shall be coordinated with the IS SS.

24.The use of local user credentials in remote access technical support systems is not allowed. Exceptions may be made only in certain non-standard cases, cases of lack of technical implementation/opportunity and/or cases with network-to-network connections.

25.For exceptional cases a different, but not contradicting the requirements and rules of the Policy, procedure of remote access organization, officially agreed upon and controlled by the IS SS, may be established.

26.The period of validity of remote access for the Company's employees shall be determined by the period of time necessary and sufficient for the employee to perform tasks in accordance with his/her functional and job responsibilities.

27.The period of validity of remote access for representatives of third parties shall be determined by the terms of contractual agreements, but shall not exceed one calendar year from the date of provision of remote access under existing contractual agreements. In case of long contractual obligations, more than one calendar year, it is necessary to ensure that the formal procedure for renewal of remote access for a new established reporting period is performed in advance in accordance with the requirements of the Policy.

28.The validity of the remote access must be checked and monitored for relevance and/or expiry on a regular basis, from the moment of its granting, by the user himself, his direct supervisor or other person responsible for such a process, of the relevant SS concerned. In the case of third party representatives, the obligation to fulfill these requirements shall be the responsibility of the supervising and responsible person of the SS concerned within the framework of the contractual agreements in force.

29.In order to extend the term of validity of the remote access, the user and/or the manager of the concerned SS shall ensure that a formal process is initiated in advance, at least 10 working days prior to the expiration of the access, in accordance with the remote access management procedure (methodology, instructions, rules, etc.) for the extension of the remote access.

30.In the absence of the user and/or manager interested in initiating the process for renewal of remote access, in order to comply with the appropriate level of IS, the remote access shall be blocked automatically, without any prior notification.

31.In case there is no need for further use of the remote access by the user, the head of such SS shall notify the IT SS and the IS SS by an appropriate memo within 2 working days.

32.The remote access procedure shall be terminated upon notification to the IS by the EX unit (in case of transfer, dismissal, long vacation, etc.).

33.Users are prohibited to use remote access to access the Internet through the Company's networks for entertainment, commercial, personal or other interests that are not the interests of the Company.

34.Performing any illegal actions through the Company's networks by any remote access user is strictly prohibited. The User shall be fully responsible for the consequences of unauthorized (illegal) use of the remote access provided to him/her.

35.It is prohibited to use remote access without officially going through the procedure (methods, instructions, etc.) for obtaining remote access.

36.Remote access to the resources of the Company's networks and IS shall be organized only through secure network connections using VPN technologies accepted for use in the Company, on the basis of the Company's corporate technical means and IS systems and in compliance with the following basic requirements:

1) availability of a unique identifier for each user;

2) use of strong passphrases and/or public key infrastructure with tamper-resistant passphrases;

3) identification and authentication of users using appropriate secure protocols;

4) encryption of the data transmission medium with resilient algorithms;

5) keeping records (logging) of successful and unsuccessful authorization attempts during the connection process;

6) using secure data transfer protocols such as IPsec and SSL;

7) application of the remote access session validity time limitation of the "node-network" type within 12 - 24 hours from the moment of its establishment. Upon expiration of the set time limit, automatic termination and/or re-initialization of the remote access connection should be performed. For remote access of the "network node" type, the time criteria shall be set according to individual requirements when agreeing on the connection parameters between the process participants;

8) access from wireless networks of users who have not been identified and authenticated shall be provided only to guest segments and/or the Internet.

37.In order to ensure the proper level of remote access security and minimize IS risks, users are prohibited to use third-party software and/or cloud services (GoToMyPC, LogMeIn, Teamviewer, etc.) other than those permitted for use in the Company to organize remote access.

38.Users using a remote access connection of the "network node" type shall be sure and guarantee that their CE is not simultaneously connected to any other network that is not the Company's network. In case of remote access connections of the "network-to-network" type, in order to supplement, but not exclude, the provisions of this Policy, the rules and requirements determined by the provisions of contracts and/or agreements may be applied, which shall regulate various technological parameters and aspects of the connection, for example, the list of CE used, the possibilities and limits of using the network infrastructure of the interacting parties, types of encryption, etc.

39.When accessing the resources of the Company's networks and IS, users are fully responsible for preventing access to any information and data of the Company by persons (including family members, relatives, acquaintances, etc.) who do not have appropriate legal authorizations and privileges from the Company. This rule shall be observed as long as remote access connections to the Society's networks are active.

40.Users are prohibited from disclosing or sharing their credentials (login and password) in any form (verbal, written, e-mail, etc.) or to anyone, including family members.

41.Personal CE used for remote access must comply with the same RD requirements as those for CE owned by the Company.

42.All CE used for remote access must have the latest versions of licensed and Company-approved software (VPN, anti-virus, local firewalls and operating systems, etc.) installed. If the CE contains unlicensed software and/or outdated versions of software and operating systems that do not meet the requirements of the Company's corporate standards, it is mandatory to eliminate these discrepancies before using remote access.

43.The use of any unregulated and/or limited information resources by the remote access user shall be officially encouraged in advance by the direct supervisor of the SS concerned and agreed upon by the IS SS.

44.Any user software, system or facility that may interfere with or work to bypass the Company's remote access routing and security technical facilities and systems shall be disabled for the duration of the remote access session.

45.When using remote access it is strictly prohibited to copy, replicate, store and distribute data containing commercial, confidential and other secrets of the Company, including personal data of the Company's employees.

## 4 Roles and Responsibilities

46.Control over the implementation of the requirements and rules of the Policy shall be vested in the IS SS.

47.Responsibility for monitoring the implementation and relevance of this Policy, as well as its amendments, shall be vested in the IS SS.

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

49.Heads of SS are responsible for timely communication of the Policy requirements to the employees of their subdivisions and/or representatives of third parties as they relate to them and for compliance by the employees of their subdivisions and/or representatives of third parties with the requirements of the Policy.

50.The IS SS shall be responsible for the 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 methodological management of remote access processes.

51.Implementation of the provisions of this Policy and procedures related to operational (maintenance) support of remote access processes and support of remote access users shall be entrusted to the SS that provide technical support and maintenance of operational activities of users and technical systems and facilities of the Company providing remote access.

52.In case of detection of violations of the requirements of this Policy by an IS user, which have caused or may have caused serious damage to the Company's business activities, an internal investigation shall be initiated and conducted with the involvement of interested SPs and in accordance with the approved IS Incident Investigation Procedure.

53.Violation of the provisions of the Policy or 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 laws, as well as the Company's Personnel Management RD.

54.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 expediency of applying the measures in question, as well as information on the willfulness of the violation and the damage caused.