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

Password protection policy of Kazakhtelecom JSC

Almaty, 2023

Contents

1. **Terms, Abbreviations and Definitions ……..……...3**
2. **Purpose and scope of the Policy. ……..4**
3. **General provisions and requirements of the Policy. ……. 4**
4. **Password generation rules ……7**
5. **Password entry rules ……....8**
6. **Password change procedure ……9**
7. **Roles and responsibilities ……...10**

1 Terms, Abbreviations and Definitions

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;
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 set of organizational and technical measures aimed at data protection;
IR - information resource (asset). For the purposes of this Policy, it shall mean 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 IS (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 technology. Processes, methods of searching, collecting, storing, processing, providing, disseminating information and ways of implementing such processes and methods;
RD - the Company's regulatory documentation (policies, standards, orders, regulations, guidelines, instructions, etc.);
UC - unauthorized access. Access to information or IS resources carried out with violations of the established rules and/or access rules;
Company - Kazakhtelecom JSC;
Software - software;
Policy - this Password Protection Policyof 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;
Computer equipment(CE) means computer equipment (stationary computers or workstations, portable computers or notebooks, etc.);
SS- structural subdivision of the Company;
SS TS - a structural subdivision of the Company or a subdivision (or organization) engaged to perform these functions, which performs technical support of users and UHS in the Company;
Third party, third person - an individual or legal entity, contractor, supplier, partner, counterparty, contractor, etc., interacting with the Company on the basis of contractual agreements and not being a full-time employee of the Company;
KeePass - cross-platform free password storage software;
SNMP - Simple Network Management Protocol;
sudo (literally “substitute user and do”) - a program for system administration of UNIX-systems, which allows delegating certain privileged resources to users and keeping a record of their work.

2 Purpose and scope of the Policy

1. The Policy regulates organizational and technical support of the processes of creating, using, changing, terminating passwords for user accounts and administrators of the Company's IS, as well as control of actions when working with passwords.

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

3. Passwords are the most important aspect of IS, the primary method of protection of access to the Company's IS, provide delimitation of user rights and protection of user accounts. An incorrectly chosen password increases the potential risk of intrusion into the Company's IS.

4. Compliance with this Policy minimizes the likelihood of a breach of the Company's IS regime by misuse of passwords.

5. All Company employees and third party representatives having access to the Company's IS resources shall be responsible for correct selection and storage of passwords in accordance with the requirements of the Policy and shall be liable for failure to comply with these requirements.

6. The Policy applies to anyone who has access or is responsible for providing access to any of the Company's IS, including all sites, and all components of the Company's IT infrastructure.

7. 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

8. 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, international standards on IS ISO/IEC 27000, COBIT, ITIL, current state and immediate prospects of development of information structure of the Company, capabilities of modern organizational and technical methods of information protection.

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

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

1) changes in regulatory and 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.

11. 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.

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

13. The Policy is based on a structural approach to password protection, whereby the following conditions shall be ensured:

1) a password is a means of protecting information, CE, software, servers, applications, active data transmission equipment and information of confidential nature from intrusion and is a numeric and symbolic sequence consisting of a certain number of characters and symbols;

2) a password must be kept secret and is effective as a means of protection only when used correctly;

3) passwords shall be stored electronically only in a secure form.

14. The user's ID and password in the IS are account records (data), on the basis of which the user is granted access rights to technical means and the IS, the user's actions in the IS are logged and the confidentiality of information processed (created, transmitted and stored) by the user is ensured.

15. The user is obliged to remember his/her identifier and password.

16. Passwords can be personal (personal, individual) and group (common, collective).

17. A personal password shall belong to only one user and shall be used to differentiate access in multi-user ISs, as well as access to resources of individual use.

18. Personal passwords for access to IS resources shall be set for the first time, as a rule, by IS administrators. After the first login to the IS and thereafter, passwords shall be selected, created and used by IS users independently, taking into account the requirements of the Policy.

19. A group password shall belong to several users who are united into a respective group based on some features and rules and shall be used in multi-user ISs for access to shared resources and/or in ISs with a single technically possible password if it is required to provide access to the IS for several users.

20. The processes for creating and using group passwords shall be harmonized and strictly controlled by the IS. The creation of group passwords in IS shall be performed by IS administrators with appropriate privileges and in compliance with the requirements of the Policy.

21. The password for a user account with administrative privileges obtained through various means, such as group membership or programs such as sudo, shall be unique from other account passwords for that user.

22. All administrative (system) account passwords, as well as application and active hardware passwords, must be stored in an encrypted database with restricted access.

23. You may not:

1) sharing your password with anyone;

2) use the same personal account by different users;

3) use the same password to access different IS;

4) using the same password for other systems (e.g. home Internet, free e-mail, forums, etc.);

5) transmitting passwords using third parties, unencrypted e-mail, or other open means over the Internet;

6) storing passwords in public form on any type of storage media, including those written down on paper and in an easily accessible place;

7) openly storing passwords in program texts or files and recording them on any type of storage media.

24. Passwords may be transferred in the following cases:

1) Transfer of passwords from an employee to the SS manager in case of industrial necessity in case of temporary absence of the employee;

2) Transfer of passwords from an employee to the SS manager in case of termination of his/her authority (dismissal, etc.) and impossibility to cancel the account with mandatory subsequent password change;

3) transfer of passwords between employees in case of using group accounts or common work e-mail addresses to perform job duties;

4) transfer of passwords for storage to the SS Unit Manager in accordance with clause 25 of the Policy.

25. Hard copy passwords may be stored only in the personal safe (or in a personal sealed, lockable cabinet) or in the safe (or in a sealed, lockable cabinet) of the SS manager in a sealed envelope. When operational necessity arises in the event of an employee's temporary absence or in the event of termination of the employee's authority (layoff, etc.), the SS manager shall be permitted to open the password envelope.

26. It is allowed to store user passwords on the Company's IT systems in files that are not accessible to other users (i.e. exclusively on local disks, not on network disks and not in shared folders). In such cases, it is necessary to store passwords in encrypted form (e.g. using KeePass program, encrypted archive, etc.).

27. Passwords of IS administrators (system administrators, network administrators, application system administrators, information security administrators, etc.) shall be stored in accordance with clause 25 of the Policy. Immediately after changing the passwords, the IS administrator shall submit their new values (together with the names of the respective accounts) in a sealed envelope to the head of the SS for safekeeping.

28. If it is necessary (emergency situations, force majeure, etc.) to use the IS administrator's password in his/her absence, the envelope with the password shall be given by the head of the SS to the employee working with the IS against signature. In such a case, the IS administrator who was absent earlier shall change his password immediately upon his return to the workplace.

29. In the event that a user is required by anyone to provide his/her password, the user shall refer to this Policy, notify his/her immediate supervisor, and/or refer the requestor to the IS SS for clarification on the matter.

30. The user must take all steps to ensure that the password belonging to the user is not compromised.

31. The user is personally responsible for keeping his/her password confidential.

32. Any facts of compromise shall be reported to the immediate supervisor of the SS and the IS SS by any method available and accepted in the Company.

33. When creating a new account in the relevant IS and/or performing procedures for its replacement, restoration, unlocking, etc., it is required to generate and assign a

temporary password to the user account by means of the IS itself and/or by the IS administrator. Further actions are described in clause 18 of this Policy.

34. Temporary passwords shall be assigned to a user only after the user has been identified.

35. Temporary passwords should not be guessable or repeatable from user to user.

36. When using the SNMP protocol, a different connection string (Community Name) value than the standard “public”, “private”, “system” and different from the password used to log in to the system must be used.

37. On the part of the IS SS, as part of IS audits, activities shall be performed to test various passwords for tamper resistance and selection. If during such activities a password is matched or compromised, the corresponding account shall be locked and the user and the IS administrator shall be notified (reprimanded) and instructed to perform procedures to change the password and unlock the account.

38. All user, administrator, and system passwords shall comply with the requirements of the Policy.

4 Password generation rules

39. Passwords shall be generated in accordance with the requirements of the Policy provisions as part of various procedures (methods, regulations, instructions, rules, etc.) for maintenance (operation, administration, operational management, etc.) of the Company's IS.

40. When creating any password, the following requirements should be followed:

1) password length for users shall be at least eight characters;

2) the password length for administrative (system) accounts shall be at least ten characters long;

3) the password must contain lower and upper case letters (lower and uppercase), decimal digits and/or special characters (@ # $ & * %, etc.);

4) the password must not contain the user account name or any part of it, or include easily computable combinations (phone numbers, first names, last names, birthday dates, names of CE, etc.), as well as common abbreviations (LAN, USER, etc.).

41. Whenever possible, special controls should be utilized when generating passwords to prevent users from selecting bad and “weak” passwords, i.e., passwords that do not meet the requirements of the Policy.

42. Any system or software that meets the requirements of the Policy may be used to generate passwords.

43. IS administrators, whose duties include creating and deleting user accounts, shall not have access to the values of users' personal passwords.

5 Password entry rules

44. The password shall be entered according to the following rules:

1) password entry shall be performed directly by the IS user (password owner);

2) when entering a password, characters must not be displayed on the screen in an explicit form;

3) in order to prevent incorrect password entry, the user must make sure that the selected input language (keyboard layout) is correct, as well as exclude the possibility of unauthorized persons viewing what is typed on the keyboard;
4) IS should be configured in such a way that after 5 unsuccessful password entry attempts the account is blocked for 10 minutes. In case of systematic blocking of the user account (more than 3 times in a row), which may indicate a possible attack, hacking or other IS violations, the account shall be permanently blocked;
5) resumption of the blocked user account shall be carried out on the basis of the user's registered request to the TP SS, after receiving approval from the IS SS;
6) in case of a scheduled or unscheduled password change, the new password must be entered twice.

6 Password change procedure

45. Any passwords must be changed periodically. In the absence of other RD of the Company regulating the frequency of password changes in a specific case and for a specific IS, the password must be changed in accordance with the requirements of the provisions of the Policy.
46. Scheduled password changes are made at least once every 3 months for user accounts and at least once every 6 months for administrative (system) accounts (domain administrator, local administrator, root, etc.).
47. When changing a password, the new value must differ from the previous one in at least 4 positions;
48. The uniqueness of passwords must be ensured during 9 periods of their validity.
49. The target IS to which a user connects with a temporary password, if possible, must be configured in such a way as to require the user to change the temporary password and provide him with this opportunity. In the absence of this functionality in the IS, the conditions must be ensured and the corresponding rights must be granted that allow the user to perform the procedure for changing the temporary password independently.
50. In the event of termination of powers (dismissal, etc.) of an employee who had access to service, system or group accounts, the passwords for these accounts must be changed.
51. Technological access passwords (standard "default" passwords of manufacturing companies intended for access to system resources, servers, software, computer equipment, active data transmission equipment and other components of the Company's IT infrastructure) must be changed or blocked immediately after the completion of installation work by the administrator of this IS.
52. In the event of a compromise of the user's personal password, the password must be immediately replaced. If the password has been lost, then after the user has been identified by the IS administrator (system administrator, application systems administrator, etc.), a temporary password is generated and issued to replace the lost one, which must be changed immediately upon logging into the system.
53. In the event of a compromise of the IS administrator's password (system, network administrator, application systems administrator, information security administrator, etc.), the password must be changed immediately.

7 Roles and responsibilities

54. Control over fulfillment of the requirements and rules of the Policy shall be vested in the IS SS.
55. Responsibility for controlling the implementation and relevance of the Policy, as well as for amending it, shall be vested in the IS SS.
56. Responsibility for ensuring proper fulfillment of the requirements and rules of the Policy shall be assigned to all interested SS within the scope of their authority and in accordance with the provisions established by the Policy and the documents developed on its basis.
57. 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.
58. Responsibility for organizational and methodological support of password generation, use, change and termination processes, control of user actions when working with passwords shall be assigned to IS SS and interested SS of the Company.
59. Technical security of password generation, use, change and termination processes in all Company's SS shall be the responsibility of the Company's IS administrators.
60. All users shall be familiarized with the requirements of the Policy.
61. All users shall be responsible for their actions when using passwords in working with the Company's IS and handling the Company's protected IRs, as well as for compliance with the requirements and rules set forth in the Policy and internal documents developed on its basis.
62. 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 SS and in accordance with the approved IS Incident Investigation Procedure.
63. Violation of the provisions of the Policy or documents developed in support of the Policy, including any intentional action taken to violate, 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.
64. 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.