RULES
ORGANIZING AUTHENTICATION PROCEDURES FOR IT DEPARTMENT EMPLOYEES

Astana
2023

1. Terms and abbreviations

The following basic concepts and terms are used in these Rules:

System administrator - a person who provides system administration and technical support services for an IS.

In order to identify, authenticate and comply with the principle of personal responsibility for one's actions, the IS system administrator shall assign personal unique names (account) with passwords to the user.

Organizational and technical support of the processes of using, changing and terminating user passwords is assigned to the IS system administrator.

Information resources - electronic systematized information (database) contained in information systems united by appropriate software;

Password compromise is the leaking or disclosure of a password;

IS user - a subject accessing the IS to obtain the electronic information resources he/she needs, which require authorization;

Organization - RES Association "Qazaq Green" Ltd.

2. General Provisions

In order to identify, authenticate and comply with the principle of personal responsibility for their actions, the system administrator and IS users shall be assigned personal unique names (account) with passwords.

Control over the actions of users, IS system administrator and employees when working with passwords is assigned to the information security specialist responsible for IS maintenance.

Upon hiring a new system administrator, the information security specialist shall familiarize the system administrator with the regulatory documentation related to the functioning and information security of the IS and transfer passwords for IS administration (by transferring information on logins and passwords in a sealed envelope). Upon receipt of the above information, the system administrator shall immediately change the passwords in accordance with these Rules and then transfer the new passwords to the information security specialist. The information on new logins and passwords shall be formalized by the information security specialist in a closed envelope. The facts of transfer of passwords of the corporate network users shall be recorded in a specially kept log according to Appendix 1 to these Rules. The facts of issuance and change of user passwords in accordance with the IS roles shall be recorded in the electronic log of issuance of IS passwords. The electronic log of password issuance shall contain the following fields: serial number; by whom the password was issued, the operation performed, date and time of the operation.

Deletion of accounts of users dismissed, transferred to another structural subdivision, branch, regional center shall be performed by the system administrator immediately upon receipt of a written notification from the personnel department of

the Organization.

Within **3** hours after dismissal, transfer of an employee to another structural subdivision, branch, regional center, the HR department of the Organization must notify the system administrator of the order.

Authentication of some users may be provided using special protective hardware and software recommended for use by information security and centrally procured by the Organization from the developers (suppliers) of the said tools.

3. Regulatory References

The following documents were used for the legal background and reasons for the development of this document :

1. Law of the Republic of Kazakhstan "On Informatization" dated November 24, 2015 No. 418-V ZRC;
2. Law of the Republic of Kazakhstan "On Technical Regulation" dated November 9, 2004;
3. ST RK ISO/IEC 27001-2015 "Methods and means of ensuring security. Information security management system. Requirements".

4. Rules for forming a personal password

Personal passwords shall be selected by users and the IS system administrator independently, taking into account the following requirements:

The password must meet the following requirements:

- password length must be at least 8 characters;
- password characters must include upper and lower case letters, numbers or special characters;
- the password must not include easily computable combinations of symbols (first names, surnames, the name of the automated workstation, etc.), as well as common abbreviations (computer, LAN, USER, etc.), and birthdays;
- it is forbidden to use a "blank" password as a password;
- when changing the password, the new value must differ from the previous one in at least 3 positions;
- the user is not authorized to share his/her personal password with anyone else.
- it is forbidden to select passwords that have already been used before;
- it is forbidden to use the same password for business and non-business

purposes;

- the user may not disclose his/her personal passwords
- it is forbidden to use only login (user name) without password when authorizing a user;
- it is recommended to use random character passwords.

For some employees, multiple unique names (accounts) are allowed in case of business necessity.

Before obtaining a temporary password, the user is recommended to sign a non-disclosure of personal password (Appendix 2).

To obtain a temporary password, the user must provide an identity document or an official ID card.

The user must memorize his password himself and must not save or share it with others in any form.

Passwords may not be given to users by open e-mail messages or transmitted by open e-mail messages from a third party.

The user must sign the password issuance and acceptance log when receiving the password.

5. Password entry (access)

Password entry is case-sensitive (upper-lower) and takes into account the current keyboard layout (EN-RU, etc.).

When entering passwords, it is necessary to exclude the possibility of its recognition by unauthorized persons or password compromise by technical means.

When entering passwords, the validity of the login and password is checked. If the password is entered incorrectly, the system will not be logged in.

6. How to change passwords

When logging in for the first time, the user must change the temporary password. When selecting a password, the following password formation requirements should be followed:

– password must contain at least 8 characters;

– the password must contain uppercase and uppercase alphabetic characters, as well as numbers and/or special characters (#, $, @, etc.);

– password must not include easily computable character sequences such as common abbreviations (e.g. admin, system, user, sys, god) or personal or other publicly available information (e.g. dates, names, titles);

– the password must not include groups of characters whose sequence on the keyboard can be easily calculated (e.g. 1234, qWerty, qwerty123, 321369);

– when changing the password, the new value must differ from the previous one in at least 4 positions.

The owner of the password is personally responsible for keeping the main password secret. It is prohibited to disclose the password to other persons, including employees of the structural subdivision, to write it down, as well as to send it in plain text in electronic messages.

A password should never be stored on a computer system in an unsecured form. The owner should avoid making a record (e.g., on paper, in software files, or on a portable device) of passwords without assurance of their secure storage and approval of the method of storage.

Account blocking is controlled by the system administrator, according to the account log entries.

The user/administrator of the Organization's information system must change the main password at least once a month. The main password can only be created by the user or administrator of the Organization's information system. It is prohibited to generate passwords by computer programs and third parties.

The Administrator transmits his/her authentication credentials for access to the Organization's information systems in hard copy in a sealed envelope to the ISMS Management Representative, who in turn stores them in a locked vault.

An IS user who has lost his/her access details to the system shall officially apply for assistance to the system administrator to set another password on the basis of a letter to the Organization. A user of the corporate network who has lost his/her access details to the IS shall officially apply for assistance to the system administrator to set another password on the basis of a password request (Annex 2). The system administrator, if necessary, may change the password for the user of the corporate network and IS at any time (both when registering in the system and after a certain period of password use).

The system administrator shall check the cyclic use of old passwords and exclude the reuse of passwords. The IS system administrator shall also delete unused user accounts (logins and passwords).

The system administrator defines a password change policy that provides for a password expiration date, the issuance of a warning message about the need to change the password, and blocking access to information resources after the password expiration date of 45 days.

The IS system administrator must be able to change the password at any time. The password of a corporate network user shall be changed by the system administrator.

7. Password management

The password management system shall:

1) maintain a history of previous user passwords, and prevent their reuse;

2) store and transmit passwords in a secure form (encrypted or hashed).

8. Password storage

Password holders are prohibited from:

1) give other users a personal password and register them in the system under their own account and password;

2) record passwords in an electronic notebook, file and other data carriers, except for paper media, with paper media with password records to be kept in a safe.

IS system administrator passwords with account names and the date the passwords were set shall be kept in sealed envelopes in a safe with the immediate supervisor.

The IS system administrator and users shall, within 3 hours after changing their passwords, give their new values together with the names of their respective accounts in a sealed envelope to the heads of the relevant department. Upon receipt of the envelope with the new passwords, the envelope with the old passwords shall be destroyed.

All users working in the IS must undergo secure authentication that identifies them and eliminates the possibility of password selection and data interception during authorization.

In the event of a compromise of the system administrator's IS password, the IS administrator shall:

1) to change your password immediately;

2) notify the information security officer.

If there is a business need for urgent access to personal computer data of a temporarily absent user, it is authorized:

1) the system administrator, on the instruction of the direct information security specialist of the absent employee, to change the password of the temporarily absent user to use the computer. The user is obliged to change the password within twenty-four hours upon returning to work. These operations are recorded in the password issuance log (Appendix 1);

2) when an employee is temporarily absent, the information security specialist, as instructed by the immediate supervisor, should open the envelope with the password and use the computer. When the user goes to work, he/she must change the password within 24 hours. These operations are recorded in the password issuance log (Appendix 1).

All users should be aware of the need to prohibit the inclusion of passwords in an automated enrollment process, such as using stored macro commands or function keys.

Responsibility for the disclosure of the received password and actions performed on the personal computer lies with the person who received the password after such an event. Upon arrival, the temporarily absent user is obliged to change the password at the first login.

The account of a user who has gone on extended leave (more than 60 days)

shall be blocked by the IS system administrator upon receipt of a written notification from the organization's human resources department.

To recover a forgotten password on a PC, you must contact your immediate supervisor for a decision on unlocking the user account.

If the password is compromised, the user must immediately change their password.

9. Responsibilities when organizing password protection

Employees working with the IS shall be familiarized against signature with the requirements of these Rules and warned of responsibility for the use of passwords that do not meet the requirements, as well as for disclosure of password information.

The other users of the system are responsible for storing accounts and passwords.

For disclosure of password information, which represents confidential information, an employee shall be held liable in accordance with the current legislation of the Republic of Kazakhstan.

Annex 1
to the Rules for inventory and
passportization of computer hardware,
telecommunication equipment and
information system software
"__"_____202_ г. № _

Password log

№	Name/signature of system administrator	Name/signature of employee	Operation performed	Date
1				

Annex 2
to the Rules for inventory and
passportization of computer hardware,
telecommunication equipment and
information system software
"__"_____202_ г. № _

APPLICATION
password

Name of structural subdivision

_____

Name of corporate network user, position

_____

Reason for issuing a password:

_____
_____
_____
_____
_____
_____
_____
_____

Date and signature

"____"_____ _____

FAMILIARIZATION SHEET

№	Surname, first name, patronymic	Position	Personal signature	Date
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				