RULES
DIFFERENTIATION OF ACCESS RIGHTS TO ELECTRONIC RESOURCES

Astana
2023

1. Terms and abbreviations

Organization - Qazaq Green Association of RES;

Rules - Rules for differentiating access rights to electronic resources;

Information Security Specialist - an employee of the Organization responsible for ensuring the protection of information resources and ensuring information security of the Organization;

System Administrator (hereinafter - SA) - an employee who performs the functions of administration of servers and application active equipment of the corporate information network, and (or) is responsible for administration:

- of the Organization's information systems;
- database servers of the maintained IS.

Human Resources Specialist- A human resources officer or a person performing his/her duties and/or functions.

2. General Provisions

1. These Rules regulate access to information, software and hardware resources, organizational and technical support of the process of registration of personal computer users and IS system administrators, deletion of accounts in the Organization.
2. Organizational and technical support of the process of access to information, software and hardware resources of users is assigned to the system administrator.

3. User registration rules

3. When a new staff member is hired, the Organization's Human Resources Specialist, in accordance with the staff member's job responsibilities, submits a request to the Information Security Specialist, in the form of a memo, for the necessary access to information resources to perform his or her duties.
4. After a new employee is hired, a specialist of the HR department in accordance with the rules of personnel records management sends an application to the information security specialist on the need to prepare the employee's workplace, on the basis of which the user is registered (user account is created) with access to the information resources of the Organization.
5. For some employees, multiple accounts are allowed in case of business necessity.
6. The password must meet the requirements of the Organization's Rule for the Organization's authentication procedure.
7. Name requirements in the network environment (hostname):

1) The name in the network environment is determined based on the department name and employee name separated by an underscore character.

2) Information about the user (surname, first name) in Russian identifying the user in the network environment shall be entered in the "Computer description" column.

8. Once registered on the network, the user is provided with the Organization's approved information security policies and guidelines for review.

9. The user is obliged to be guided by the Organization's rules and instructions on information security.

10. The CA provides users with access to resources in accordance with the approved Rules of Information Systems Operation.

11. The CA shall maintain an electronic user log containing the following boxes:

1) last name, first name, middle name;
2) subdivision;
3) Position;
4) address, phone number;
5) e-mail address;
6) Internet availability;
7) the name of the personal computer in the network environment (hostname);
8) access to network disks;
9) access levels.

12. Upon termination of an employee of the Organization, the CA is required to lock the user's online account before marking the bypass list, and delete it after three years.

13. When transferring a user, the CA shall make the appropriate changes to the user profile and user logbook.

4. basic rights, duties and responsibilities

14. Responsibilities for granting and revoking access to Resources are assigned to the Organization's system administrator in accordance with departmental regulations and staff job descriptions.

15. Responsibilities for monitoring compliance with the Rules shall be assigned to the Organization's Information Security Specialist.

16. Users are allowed to work with the resources only after familiarizing themselves with the provisions of the Rules and passing the briefing conducted by the Information Security Specialist against their signature in the appropriate log (**Appendix 1**, hereinafter referred to as the User Briefing Log).

17. Compliance with the requirements of the Rules is mandatory for all users allowed to work with the resources.

18. In addition to these Rules, the admission of specialists from external organizations to carry out work on the Organization's premises shall be governed by the relevant regulatory document of the Organization.

19. The activity of users when working with resources can be logged and periodically checked for compliance with the established rules of work by any means not contrary to the legislation of the Republic of Kazakhstan.

5. Resource accounting

20. All information resources of the Organization shall be accounted for and systematized in an appropriate Register.

21. The Roster shall be maintained by the Organization's system administrator.

22. An up-to-date Register shall be available to all users at any given time.

23. Information on a new resource (changes in an existing resource) must be communicated by the unit owning the resource to the Organization's Information Security Specialist within two working days of its appearance in the form of a memo signed by the system administrator (**Annex 2**).

24. Amendments to the Register shall be made within one working day from the date of receipt of the relevant memo.

6. Providing access to resources

25. One of the following conditions must be met for a user to be granted access to a resource:

- access is necessary for the user to perform his/her job duties in accordance with his/her job description;
- access is required for a user to perform the duties of another user on behalf (in the form of a memo) of the system administrator;
- access is required for a user to perform the duties of another user as directed (in the form of an order or instruction) by the Organization's management;
- access is required for the user to perform work as directed (in the form of an order or instruction) by the Organization's management;
- access is required for the user to perform work in the course of implementation of contracts, agreements concluded by the Organization (for employees of "third-party" organizations).

26. To provide access to the resources, the Organization's system administrator (person replacing him/her) shall prepare an application for granting access (hereinafter referred to as the Application, **Annex 3**), guided by the Register.

27. The Organization's system administrator checks within one working day whether the user has a reason to access the resource according to the Application. If access to the resource according to the Application cannot be granted for any reason, the Application shall be returned to the head of the unit that initiated the Application with a detailed description of the reason.

28. After agreement with the Information Security Specialist, the Application shall be submitted for approval to the Head of the Organization (his/her substitute). In case of approval on the same day, the original of the approved Application shall be

transferred to the Information Security Specialist for permanent storage, and a copy of the Application (with the specified Application number) shall be transferred to the system administrator to perform work on granting access in accordance with the Application.

29. Information on approved Requests shall be recorded in the log of registration and accounting of requests for granting access to resources (hereinafter - the Log of Requests, **Annex 4**), which is maintained electronically by the system administrator.

30. Active Directory authorization is required to access network resources.

31. Access granting is controlled by the system administrator.

32. Users authorized in Active Directory have access to corporate mail, electronic document management system.

33. Access levels are presented in the access matrix.

34.A VPN connection (SSTP, https protocol) is used to connect to the IC, inside the VPN tunnel using https, port 81.

7. Utilization of resources

35. The utilization of resources shall be in accordance with operating instructions for software and hardware.

36. It is prohibited to deliberately disable resources, block access to them and any other actions that interfere with the normal operation of resources.

37. If a resource failure is detected, the user must report the incident to the system administrator and information security specialist.

8. Changing access rights to resources

38. If it is necessary to grant the user additional authority (roles) to access a resource already used by the user, proceed in accordance with Section 6 of the Rules.

39. In case it is necessary to replace (fully or partially) the user's authorization to access a resource already used by him, it is necessary to act in accordance with clause 40 of the Rules.

7. Revoking access to resources

40. Revocation of access to resources occurs in cases of:

- changes in the user's job responsibilities;
- expiration of the Application period;
- changing the technological processes of information processing so that user access is no longer required;
- violation of the rules of access to the resource by the user;
- when an employee goes on maternity leave (parental leave);
- user dismissal;
- as otherwise required by the Organization's management or the Organization's

system administrator.

Access revocation must be initiated within one business day of the occurrence of the relevant event.

41. The responsibility to initiate revocation of a user's access to resources rests with:

- in case of changes in the user's job duties or his/her dismissal, changes in technological processes of information processing in such a way that the user's access is no longer required - to the Organization's system administrator;
- in case of expiration of the Application validity period, violation of the rules of access to the resource by the user - on the Information Security Specialist of the Organization.

42. Information on the initiation of revocation of access (with indication of the reason) shall be communicated in any form in writing by the head of the relevant unit of the Organization to the Information Security Specialist.

43. Access is revoked by the system administrator at the instruction of the Information Security Specialist

44. Information on access revocation shall be entered by the Information Security Specialist within one working day in the Application Registration Log.

8. Monitoring compliance with Regulations

45. The information security specialist checks semi-annually whether the list of registered users corresponds to the staffing schedule and its changes, and submits a report to the first manager as part of internal audit.

46. For violations of the norms stipulated by these Rules, disciplinary sanctions may be imposed on the Organization's employees upon the recommendation of the manager in charge of information security issues, based on the materials of an official investigation.

9. Mailing list

All employees of the Organization shall be familiarized with this document against signature (hereinafter referred to as the familiarization sheet).

Annex 1
to the Rules for the delimitation of access rights
electronic resources
"__"_____ 202_ № ____

Journal

Instructing users on the rules of access to the resources of the RES Association "Qazaq Green" ULE

№ n/a	I got the briefing:			Briefed me:		
	Last Name First Name.	Position held	Caption	Last Name First Name.	Caption	Date

Information security specialist

_____
(FULL NAME)

Annex 2
to the Rules for the Delimitation of Rights access to electronic resources
"__"_____ 202_ № ____

MEMO

In accordance with the Rules for the delimitation of access rights to information resources, approved by the order dated "___"_____.202__. No.___, I request to include (cancel) a new information resource in (from) the register(s).

Name of information (program) resource	Grounds for inclusion of a new resource in the organization's register (date and number of the law or other normative act)	Period of validity (permanently or specify interval)
1	3	6

Administrator System _____

"____"_____202__ _____
signature

APPROVED

_____

"____"_____202_

Annex 3
to the Rules for the delimitation of access rights
electronic resources

"__"_____202_ № ____

Application #_____
Providing access to information, software and hardware resources
of the RES Association "Qazaq Green"

Employee's Last Name and First Name, (tab. no.), position	No. of cubicles, Telephone (in.)	Justification of the need to perform the specified type of work in accordance with the employee's job duties (reference to the section of the job description or other normative document in accordance with clause 4.1. of the Rules)	Resource (according to the List)	Mode of access (**open/close**: read/close; view, enter, corr., print).	Period of validity (permanently or specify date interval)
1	2	3	4	5	6

Administrator System _____
"____"_____202__ _____
signature

Annex 4
to the Rules for the delimitation of access rights
electronic resources
"__"_____ 202_ № ____

Journal
Registration and accounting of requests for access to
information, software and hardware resources of the RES Association "Qazaq Green"

Application No.	Full name, position	Division	Information resource on request	Date of approval of the application	Access period

FAMILIARIZATION SHEET

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