СЕРТИФИКАЦИОННАЯ ПРОГРАММА
QAZAQ GREEN CERTIFICATE

QAZAQ GREEN CERTIFICATION
PROGRAMM

QAZAQ GREEN

BACKUP POLICY

DATA BACKUP AND RECOVERY

Astana

2023

1. Terms and abbreviations

Organization - Qazaq Green Association of RES;

Regulations – Regulations for carrying out information backup and recovery;

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

Corporate computer network - a network of interconnected and coherently functioning software and hardware components designed for data exchange tasks and operated within the Organization;

Local Area Network (LAN)- A group of personal computers or peripherals interconnected by a high-speed data link in a location of one or many nearby buildings;

Unauthorized access to information (UAI) - access to information that violates the rules of access differentiation using standard means provided by means of computer equipment or automated systems;

Backup - is a measure to ensure uninterrupted operation of software and information systems, which consists in creating copies on installation disaster recovery media of data, information processed and stored in information resources with the possibility of recovery and further use;

Internet Network - a system of networks providing access to international information resources;

Reference copying - is a copy of the software on installation emergency recovery media located in information resources with the possibility of further installation and use during recovery operations;

PC - personal computer;

SW - software;

IS - information system "Trading Platform for Commodity and Raw Materials Exchanges of Kazakhstan" 2.0.

2. General provisions

These Regulations define the requirements for the organization of backup measures for software and information resources of the Organization's corporate computer network, as well as establish the responsibilities of PC users, information technology staff, Information Security Specialist and other employees whose competence includes carrying out these measures.

3. Copying program and information resources

1. In order to ensure the possibility of prompt recovery of information and its processing in case of information systems malfunction, copying of reference

software and backup of information resources are used.

2. All software used in IS shall have reference (distribution) copies.

3. The following registers shall be compiled by the information technology staff:

1) a register of reference copies of the software operated in the Organization, in accordance with **Annex 1** to these Regulations;

2) a register of information resources of the Organization's corporate computer network subject to backup, according to **Appendix 2** to these Regulations.

3) The registers shall be coordinated with the Information Security Specialist.

4) Machine data carriers containing a backup copy shall be assigned a confidentiality label according to the highest label of the information contained therein.

4. The Information Security Specialist shall control the maintenance of the register of software master copies and the register of information resources subject to backup.

5. The System Administrator shall control the backup, including the validity of backup copies

6. Backup procedures shall be started in the evening (after 21:00) or at night, in some cases on non-working days.

7. Backup of virtual machines - servers is performed daily in automated mode (according to the schedule) on working days.

8The current copy and at least two previous copies shall be kept.

9.To create full backups, a special Backup server is used as standard; if there is not enough space on this server, an external mobile hard disk drive should be used.

10.For security purposes, media with copies should be stored in a sealed iron, fireproof safe at the system administrator.

11.Access to data carriers with reference copies of software and backup copies of information resources shall be granted only to employees whose competence includes this type of work.

12. Removal of data carriers with reference copies of software and backups outside the building leased by the Organization shall be coordinated with the Information Security Specialist and recorded in the control log. In this case the columns of the log "Start time" "End time", "Downtime", "Remediation method" shall be left blank.

4. Backup procedure

13. Automated systems are backed up based on the following:

- composition and volume of data to be backed up, frequency of backups;
- maximum storage period of backup copies - **1 month;**
- storage of the following 2 archives;

14. The backup system shall ensure performance sufficient to save information within the specified timeframe and with the specified frequency. The backup methodology is described in **Appendix No. 3.**

15. In case of detected attempts of unauthorized access to the backed-up information, as well as other information security violations that occurred during the backup process, an internal investigation is performed by the system administrator to take measures to close vulnerable connections.

5. Checking the data to be backed up

16. Data validation is the process of confirming that the values entered into data objects conform to the constraints in the dataset schemas as well as the rules established for the application. Validating data before sending updates to the underlying database is a practice that reduces the likelihood of errors as well as the expected number of processing cycles between the application and the database.

Equipment involved in backups

Name of equipment	**Functional purpose**
Servers with VMware ESXI software	Physical server (host)
Virtual machines	Database and application servers (virtual machines)

Software involved in backups

Name of software	Functional purpose
Database Servers: postgressql 12 (dva, standard), 14 (clearing, capsytender) mysql 8.029(lpg) Web Servers: Tomcat (apache tomcat version 9.0.16 (centos)) httpd (Server version: Apache/2.4.37 (centos)) nginx (nginx version: nginx/1.18.0 (Ubuntu)) Keycloak (version 4.8.3)	Database management system

JDK (version 12.0.1)	
Centos 8- "CentOS Linux 8 (Core)" (dva,lpg,bd) Ubuntu - "Ubuntu 20.04.5 LTS" (standard)	Operating system

List of backup types and their descriptions
Backup

Backup name	**Brief description of the implementation**	**Frequency of performance**	**Where the information is stored from**	**Where the information is saved**	**Backup retention period**
Database copying	Copying via Crontab	Backup once every 24 hours	Database server	Backup server	full copies - 6 months.
Copying only configuration files from virtual machines	Crontab scheduled copying	Backup once a day	All virtual machines	Backup server	7 days No space to store more archives
Database copying	Crontab scheduled copying	Backup once a day	All virtual machines – database hosts	Backup server	7 days No space to store more archives

17. Verification of redundant data of information of automated systems, including databases, shall be performed as follows: Backup copies are taken from the main server to the test server, the system (database and application) is completely lifted and then tested.

The database copy is transferred from the main server to the Backup server via a secure VPN channel with traffic encryption, after which it is also transferred to the test server via a secure VPN channel.

"Archive Status Log" (incidents).

Verification of the reserved data is carried out semi-annually at the end of June and December during non-holiday weekends. The results of the checks shall be recorded in the "Log of checks, reserved data" according to **Annex 4**

18. If corrupted backed-up data is detected, the system administrator makes an entry in the archive (incident) status log. After that, a mandatory hash check of the sum of three subsequent archives is performed; if there are no corruptions during these checks, the standard archive check procedure is restored.

6. The order of placement of server equipment.

19. Database replication between the primary and backup servers is performed daily after hours in automatic mode, software - as changes are made.

20. The level of physical and environmental protection in the standby

facility shall be the same as the level of security in the main building where the IS is located.

21. In order to maintain redundancy facilities in working condition, the system administrator shall regularly, once a quarter, check the software and technical means of redundancy, redundant equipment.

22. According to the results of the checks, an act of completed work is drawn up and a record is made in the log of testing of backup equipment and backup means, which is described in Appendix 4 hereto.

23. Testing of backup means and backup equipment is performed by the system administrator.

24. In case of negative test results it is necessary to inform the head of the organization about the necessity to replace the backup means or to carry out repair works.

25. In order to minimize erroneous actions on the part of the specialists responsible for the backup, an instruction for the backup and restoration of IS information has been developed.

26. The system administrator is responsible for the development, updating, fulfillment of the requirements of the instruction on system data backup/restoration.

27. Organizationally, technical support specialists shall be guided by these Regulations.

7. Storage and accounting of electronic backup media

28. For security purposes, backup media shall be stored in the manager's iron safe, outside the room where the information system is located.
29. Backup information shall be provided with a guaranteed level of physical and environmental protection in accordance with the security level in the main building.
30. Current and duplicate copies shall be stored.
31. Only responsible employees, information security specialist and system administrator have access to the media with the information system distribution and backup copies of information resources.
32. The information stored on the media must be deleted in a way that guarantees its irretrievable destruction.
33. In case of media failure, it should be disposed of in a manner that guarantees irrevocable destruction of the information stored on it in the presence of a responsible person and the head of the OIT.
34. The destruction of the backup media shall be recorded in a write-off act.

35. The relocation of backups must be previously agreed upon with the head of OIT, the fact of relocation is recorded in the control log of electronic media with backup copies of information resources.
36. The fact of moving backup media outside the premises of the organization must be previously agreed upon with the OIT unit and registered in the journal of bringing in/removing backups.
37. Prohibited:

– make manual changes to the created archives of backed-up information of the systems;

– transfer backup copies of information to unauthorized persons;

– store backups in an unsecured location.

8. Control of backup results

38. Backup procedures for software (not databases or virtual machines) shall be performed by users of these programs by 5 p.m. on the business day following the due date for these procedures.

39. If an error is detected, the person responsible for monitoring results shall notify the system administrator by 6 p.m. of the current business day.

40. During the period of time when the backup system is in an emergency state, daily backups of information to be backed up shall be made using file servers having free disk arrays to provide backup functions.

41. Change testing is performed as needed and is caused by changes in service settings or installation of updates. Changes in configuration settings can be caused by recommendations of service developers (security improvements). Updates are installed on a regular basis as updates become available (for example: for Windows Server 2022 at least once a month).

9. Backup media rotation

42.The backup system shall ensure the possibility of periodic replacement (unloading) of backup media without loss of information on them, as well as ensure restoration of current information of automated systems in case of failure of any of the backup devices.

43. All procedures for loading, unloading media from the backup system are performed by the system administrator.

44.Confidential information from media that are no longer used in the backup system shall be destroyed with physical damage to the media that does not allow its theoretical use as a data storage device. (example - drilling out the HDD case, physical destruction of SSD) with photos of the damage attached to the write-off certificate.

45.To protect against malicious code, the Organization uses ESET Endpoint Security 6.3.2016.1 antivirus software, Windows firewalls in high security mode.

10. Control over compliance with the Regulations

46. The information security specialist shall control compliance with these Regulations in accordance with the information security audit, the plan of which shall be approved by the Head of the Organization.

47. For violation of the norms stipulated by this Regulation, disciplinary sanctions may be applied to the Organization's employees upon recommendation of the information security specialist.

11. Mailing list

Mandatory familiarization of all staff members of the Organization against signature (hereinafter - Sheet of familiarization).

Annex 1
to the Regulations on Backup
Information backup and recovery

Register of reference copies of software operated in the RES Association "Qazaq Green" Ltd

Name software	Responsible for software operation (full name, phone number)	Storage location of the reference copy (building address, room number)	Responsible for keeping the reference copy (full name, telephone number)	How to use the master copy (by whom, in what cases)
IS Carbon Units Registry Qazaq Green Certificate Registry				

Annex 2
to the Regulations on Backup
Information backup and recovery

Register of information resources of the corporate computer network Qazaq Green RES Association, subject to backup copying

Name information resource information resource	Location of the information resource	Schedule copying	Full name, telephone number of the person responsible for copying	Need to duplicate copy	Backup copy storage location (building address, room number)	Place of storage of the duplicate backup copy (building address, room number)	Full name, telephone number of the person responsible for storing the copies
IS Carbon Units Registry Qazaq Green Certificate Registry	Abaya 26 Data Center of Kazaktelecom JSC	Daily		Yes	г. Astana, 26 Abaya St. Data Center of Kazaktelecom JSC	г. Astana, Kabanbai Batyr Ave. 62 NLS LLP	

Annex 3
to the Regulations on Backup
Information backup and recovery

Backup methodology

1. To organize the backup system, the built-in archiving software (hereinafter - software) and the created .sh format files are used, using the capabilities of the "Task Scheduler" function. Taking into account the channel bandwidths and the volume of backed up data, it seems optimal to install independent backup servers. In order to optimize the backup system deployment costs, the backup copy is recorded on a hard disk.

2. With the help of this software such actions as setting modes and scheduling data backup, monitoring the status of task execution, and launching data recovery procedures are performed.

3. To reduce the aggregate load on the information system, all information backup operations should be performed at night. There are three sets of backups:

- monthly set. The information is recorded as of the first day of the current month. The storage period is one month. Stored on the backup server.
- weekly copy. Recorded on Wednesday night and Saturday night. Retention period - Saturday copy - until the following Wednesday, Tuesday copy - until Saturday. Stored on the server.
- daily copy. Recorded every day except weekends. The retention period is one week. Written to the Backup server, if there is no space on a removable hard disk. The hard disk is taken outside the office or to the opposite part of the office on a separate schedule.

4. The Organization distinguishes between two fundamentally different sources of information to be reserved:

1) Information stored directly in the file system - MS Windows – FAT32, NTFS, REFS.

2) Databases of the Applied Information System -LINUX EXT2, EXT3, EXT4, XFS.

5. To back up information stored directly in file systems, the firmware is used to generate backup tasks for information stored in MS Windows file system directories. At the same time, the period of information storage and the backup periodicity are specified.

6. To backup the information stored in the databases of the Applied Information System, the configuration tools of the Applied Information System and archivers are

used as an intermediate automation link. As a result of the work of the intermediate automation link, a catalog with a backup copy of the data of the Applied Information System is formed. By means of the firmware the tasks for backup copying of this catalog are formed. The information storage period and the frequency of backup copying are specified.

Backups should be stored in a remote location, at a secure distance sufficient to avoid any damage due to an emergency in the main building.

Annex 4
to the Regulations on Backup
Information backup and recovery

Backup log

Brief data on database backup		Retention period of database copies, days	
Project Name:	IS Trading Platform for Commodity and Raw Materials Exchanges of Kazakhstan 2.0		
Storage period of database copies on server HDD	1 год		
Database copies storage time on tape	Not stored		
Backup start time	01:00		

	Date			
IP- address server	time	incident	reason	notes

Database recovery log

Date of performance	IP- address server	Type of recovery	Database backup date	Reason	Notes	Performer

Backup log for the central node

Brief data on database backup		Retention period of database copies, days
Project Name:	IS Trading Platform for Commodity and Raw	

	Materials Exchanges of Kazakhstan 2.0	
Combat DB server IP address:	172.16.11.30	
DB backup server IP address:	45.86.81.78	
DB copy archive server IP address:	89.218.68.69	
IP address of the FTP server:		
Database copies storage period on the tape	Not stored	
Backup start time	01:00	

Backup date	Availability of database copies										Note
	On the database server file system		Backup database server		Tape media		Archive server		FTP-server		
21.06.2023			Yes		No		Yes				

FAMILIARIZATION SHEET

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