RULES
ANTIVIRUS CONTROL ORGANIZATION

Astana
2023

1. Terms and abbreviations

Organization - Qazaq Green Association of RES;

Rules - Rules for the organization of antivirus control.

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

Antivirus is special software that provides protection against viruses and other malicious programs;

A computer virus is a specially written program (i.e., some set of executable code) that can "attribute" itself to other programs ("infect" them) create its own copies and embed them in files, system areas of the computer, etc., as well as perform various undesirable actions on the computer;

Malware is any software designed to gain unauthorized access to information and/or to cause other harm (damage) to the Organization and/or the PC user;

User - a person participating in the operation of the Organization's corporate computer network and using the Organization's information resources.

PC - personal computer.

2. General Rules

1. These Rules define the requirements for the organization of anti-virus protection of information resources of the corporate computer network of the Organization from the destructive impact of computer viruses and malicious software; establishes the responsibility of the Organization's employees - users of personal computers connected to information resources of the corporate computer network of the Organization, Information Security Specialist.

2. Workability, efficiency of antivirus protection, fulfillment of requirements to its organization is ensured by the system administrator.

3. Installing and updating antivirus tools

3. Antivirus programs are essential for:

1) protecting information resources from virus infection;

2) detecting and recovering files infected with viruses;

3) maintaining up-to-date status of servers, various services, running tasks and systems.

4. Only licensed antivirus tools purchased independently are allowed for use in the Organization.

5. Any information received and transmitted via telecommunication channels, as well as information on removable media, is subject to mandatory

antivirus control.

6. Anti-virus programs are installed by the system administrator on all personal computers and servers of the Organization's corporate computer network.

7. Antivirus configuration should ensure that:

1) automatic launch of the antivirus monitoring at every computer restart (forservers - at restart);

2) at certain times of the day, a full antivirus scan (scan) of the local disks installed on your computer;

3) update antivirus databases at certain times of the day;

4) Treatment of virus-infected files or deletion if treatment is not possible.

5) check web pages for malicious code.

6) Check e-mail attachments and files received from public networks for viruses.

4. Procedure for antivirus control

8. Installation (modification) of system and application software of computers and local area network should be performed only in the presence of the system administrator.

9. The software to be installed (modified) on the computer must be checked for the absence of computer viruses. Immediately after installing (modifying) the computer software, an anti-virus scan must be performed.

10. Installation, setup, configuration of parameters, administration of anti-virus control tools on computers (LAN servers) is performed by the system administrator, in accordance with the manuals for the use of specific anti-virus tools.

11. Any information (text files of any format, data files, executable files) received and transmitted via telecommunication channels, as well as information from removable media (magnetic disks, CD-ROMs, flash drives, etc.) received from third parties and organizations is subject to mandatory antivirus control.

12. Control of information on removable media is performed immediately before its use

13. Particular attention should be paid to removable media (flash cards, CDs) belonging to persons temporarily allowed to work on PCs in the Organization (intern students, temporary substitutes, etc.). The work of these persons should be carried out under the direct supervision of the Organization's employees, especially if the work takes place using the resources of the local area network.

14. The user is not allowed on his personal computer:

1) change the settings and configuration of antivirus applications;

2) remove or add any antivirus programs;

3) work with removable media without first checking them with an antivirus

program installed on the personal computer;

4) to run unknown applications sent by e-mail.

15.The user is obligated to:

1) Every day at the beginning of work, when booting up the computer, make sure that there is a resident (located in the computer's RAM) antivirus monitor (on the right side of the taskbar there should be an icon with the logo of the antivirus protection program and the name of this program popping up above it), and in case of its absence, notify the system administrator.

2) independently start an unscheduled antivirus scan of the local drives of his/her personal computer upon receiving a notification from the IT service about the presence of a virus in the corporate computer network of the Organization, as well as in case of suspicion of a computer virus (atypical operation of programs, appearance of graphic and sound effects, data distortion, file disappearance, frequent appearance of system error messages, etc.);

3) If a new virus is detected that cannot be cured by the anti-virus tools used, immediately notify the system administrator.

16. The system administrator is obligated to:

1) install antivirus programs on personal computers and servers and instruct users on the settings made;

2) monitor servers and the corporate network for viruses;

3) send all users a warning about viruses entering the corporate network and instructions on anti-virus protection measures;

17.The system administrator responsible for antivirus protection shall:

1) ensure automatic monitoring of daily updates of antivirus databases;

3) analyze the work of the anti-virus gateway at least once a week;

4) prepare schedules and order of operation of modules of the antivirus program;

5) monitor the status of anti-virus protection in the corporate network of the Organization, as well as compliance with the requirements of this Rule by users;

6) immediately notify the information security specialist of the fact of detecting a virus infection in the corporate network, the suspected source of the infected file (message), the nature of the information contained in the file (message) and the anti-virus measures being taken.

18. Every day at the beginning of work when the computer is booted (for LAN servers - at restart) in automatic mode, antivirus control of PC boot files shall be performed.

19. Any information (text files of any format, data files, executable files) received and transmitted via telecommunication channels, as well as information on removable (alienable) media shall be subject to mandatory anti-virus control. Unzipping and control of incoming information should be carried out immediately after its reception or on condition of initial loading of the operating system into the

RAM of the computer from a "clean" (not infected with viruses) and write-protected system disk - on any other computer. It is possible to use another method of antivirus control of incoming information, providing a similar level of control efficiency. Control of outgoing information should be performed immediately before archiving and sending (recording on removable media).

20. Files placed in the electronic archive shall be subject to mandatory anti-virus control.

21. The system administrator is obliged to provide repositories with antivirus databases at least once a week to update antivirus databases in the organization.

22. If files infected with computer viruses are detected during an anti-virus scan, the system administrator shall:

-suspend work;

-disconnect the infected PC from the local network;

-immediately report the fact that virus-infected files have been detected;

-in conjunction with the owner of the infected files, analyze the necessity of their further use;

-provide treatment or destruction of infected files;

-in case of detection of a new virus that cannot be cured by the anti-virus tools used, send the file infected with the virus to the site of the anti-virus manufacturer; upon detection of virus-infected files, make a memo in which it is necessary to indicate the presumed source (sender, owner, etc.) of the infected file, the type of the infected file, the nature of the information contained in the file, the type of the virus and the anti-virus measures taken.

16. The responsibility for the organization of anti-virus control in the Organization, in accordance with the requirements of this Rule, shall be assigned tothe system administrator.

17. The system administrator is responsible for conducting anti-virus control activities in departments and complying with the requirements of the Rule.

5. Monitoring compliance Regulations

18. Compliance with this Rule shall be monitored by the Information Security Specialist.

19. For violation of the norms of this Rule, disciplinary measures may be applied to the Organization's employees upon recommendation of the Information Security Specialist.

6. Mailing list

All employees of the Organization shall be acquainted with these Rules against signature (hereinafter referred to as the Familiarization Sheet).

FAMILIARIZATION SHEET

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