№ 03.06.25 от 03.06.2025

NAZARBAYEV UNIVERSITY

Policy for the application of anti-virus protection in the autonomous organization of education “Nazarbayev University” and its organizations

Category: Policy

Approval Date: 03.06.2025

Effective Date: 03.06.2025

Level of Access: Open to Public

Classification Number: 7. IT

Approving Authority: Managing Council

Registration Number: 03.06.25

Owner: “Nazarbayev University IT Support” Private Entity

Revision Date: 05.06.2028

Applicability: NU and its organizations

Retired Documents:

Title: Regulations about antivirus protection at the autonomous organization of education “Nazarbayev University”

Date: 25.04.2013

Registration Number: 4.4.1

Approving Authority: Executive Council

Section 1. Objective and application

1.1 These Rules for the Application of Antivirus Protection in the autonomous educational organization "Nazarbayev University" and its affiliated entities (hereinafter – the Rules) regulate the requirements for organizing the protection of virtual and physical servers, as well as corporate devices of the autonomous educational organization "Nazarbayev University" (hereinafter – the University) against malicious software.

1.2 The purpose of these Policy and procedures is to ensure the effective protection of information, as well as hardware and software assets, from malicious software threats.

1.3. The scope and requirements of these Rules apply to all virtual and physical servers and corporate devices of the University, as well as to personal devices of individuals connected to the corporate network of the University and its affiliated entities.

Section 2. Terms / Definitions

2.1. The following terms, definitions and abbreviations shall apply in these Policy:

1) **Server Administrator** - an employee of a structural unit of the University or its affiliated entity responsible for the configuration and maintenance of a physical or virtual server, as well as for ensuring the security of the University's corporate devices;

2) **Anti-virus software** - software or a set of software tools designed to detect, prevent the spread of, and remove malicious software (viruses, trojans, spyware, and other types of malware) from computers and other corporate devices;

3) **Malicious software** - any software developed with the intent to cause harm, gain unauthorized access, disrupt system operations, steal data, or perform other malicious actions on computers, servers, mobile devices, or networks;

4) **Corporate Device** – a computer or other device owned by the University that contains data, including virtual machines deployed on University servers.

5) **Corporate Network** – the University’s private computing network that integrates its information resources, users, devices, and systems to ensure secure data exchange, collaboration, and management of business processes.

6) **Protected Objects** – virtual and physical servers, as well as corporate devices, that are subject to protection against malicious software.

7) **User** – an individual in possession of a corporate device registered on the University’s balance sheet, or an individual whose personal device is connected to the University’s Corporate Network.

8) **Institution** – the private institution “Nazarbayev University IT Support”, responsible for technical support and maintenance of the information systems and users of the University and its affiliated entities.

2.2. Terms used but not defined in these Rules shall be interpreted in accordance with the legislation of the Republic of Kazakhstan and the University’s internal regulatory documents.

Section 3. General provisions

3.1. Setup of security features

3.1.1. Only licensed antivirus software approved by the University's Information Security Service is permitted for use at the University.

3.1.2. Protective tools used for Protected Objects must be procured by the University’s Information Security Service.

3.1.3. Antivirus software must be mandatorily installed on all Protected Objects by the Institution’s employees or Server Administrators.

3.1.4. In case of difficulties with the installation of antivirus software, Administrators may submit a support request through the University's IT Helpdesk portal(https://helpdesk.nu.edu.kz/support/home).

3.1.5. If a User connects a personal device to the Corporate Network, it must have functioning antivirus software of a current version installed.

3.1.6. If a personal device connected to the Corporate Network does not have antivirus software installed, the University’s Information Security Service reserves the right to disconnect such a device from the Corporate Network.

In such cases, the owner of the personal device will be notified via corporate email.

3.1.7. If antivirus software cannot be installed due to technical or other objective reasons, the User must obtain approval for an “exception” from the University’s Information Security Service by providing written justification and ensuring alternative security measures.

3.2. Restrictions, rights and responsibilities of users

3.2.1. Restrictions for University users:

1) it is prohibited to modify or remove antivirus software installed on Protected Objects;

2) it is prohibited to use Corporate Devices without installed antivirus software;

3) the use of removable storage devices without prior scanning by antivirus software is not recommended;

4) it is prohibited to open files (including pirated software copies) received from unknown or untrusted sources/websites or senders.

5) it is prohibited to interfere with the operation of antivirus software while it is performing a malware scan on a Corporate Device.

3.2.2. Users are required to independently initiate an unscheduled antivirus scan on Protected Objects in the event of suspected malware presence (e.g., abnormal program behavior, data corruption, file disappearance, frequent system error messages, or other signs of infection).

3.2.3. If malware is detected that cannot be neutralized by the antivirus software, the User must immediately submit a request to the University's Information Security Service.

3.3. Responsibility for Violations

3.3.1 Users must comply with the requirements of these Rules. In the event of a violation, Users may be held accountable.

3.3.2. Depending on the nature and severity of the violation, the following measures may be applied:

1) warning – in the case of a first-time violation, if it did not lead to significant consequences;

2) access restriction – temporary blocking of a Corporate Device until the violation is resolved.

3.3.3. Compliance with the requirements of these Rules is monitored by the University's Information Security Service.

Section 4. Waiver

4.1. Not applicable.

Section 5. Temporary provisions

5.1. Not applicable.

Section 6. Revision

6.1. This Policy shall be reviewed every year within three years after their approval and revised if necessary.

Section 7. Related documents

7.1. Not applicable.