	ANTIVIRUS USE POLICY	Document number	MSU.BG.PL.06
		Release date	05.03.2021
		Revision Number	00
		Revision date	--
		Page Number	1/2

1. Aim

The purpose of this policy is to define the anti-virus usage principles for computers used within MŞÜ and for all systems threatened by malware.

2. Scope

All computers used within MŞÜ, all systems threatened by malware, and users using them are within the scope of this policy.

3. Responsible

The Administration is responsible for the creation of this policy. Users who use any computer or systems that are threatened by malware are responsible for its implementation.

4. Application

Definition: While describing the policy items, the term “computer” will be used in general for computers and all systems threatened by malware .

- All computers, servers, etc. of our institution or the users we serve. Anti-virus software must be installed on their system.
- Anti-virus software should be configured to provide real-time protection.
- Antivirus software and virus definitions should be updated automatically.
- Computers without anti virus software installed should not be connected to the network.
- Antivirus should not be disabled, even temporarily, by any personnel without permission.
- Other measures should be taken when antivirus software is disabled.
- Database updates of anti-virus software should be done automatically.
- In case of spread, infected machines should definitely be removed from the corporate network and should not be connected to the network until they are completely cleaned.

- Computers should be scanned with anti-virus software by the person responsible for device usage at specified periods, not exceeding 6 months.

- Portable devices plugged into computers should be scanned by antivirus software each time they are plugged in.

- Unnecessary folders, files or disks to share, read/write permissions should not be given.

Prepared	Controlling	Approver
EFRAİM YILDIZ	CENGİZ ALMAZ	İHSAN TUĞAL

4. Sanction

In case of violation of this policy, the reason for the violation is investigated by obtaining the necessary personnel support by the Administration. Violation is unintentional and personnel training, etc. If it is caused by a deficiency, work is done to close the deficiency that is the source of the problem. The administration is warned in writing via e-mail.

If the violation is understood to be intentional or if the unintentional violations are repeated more than 3 times, action is taken against the personnel in accordance with the civil servants law no. 657 and the additional sanctions specified by the university official letter.

All users are responsible for reporting security breach incidents and violations of this policy to the Administration as soon as possible.

Prepared	Controlling	Approver
EFRAİM YILDIZ	CENGİZ ALMAZ	İHSAN TUĞAL