INDEX

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Review	All	C.Santos	12/08/2024	R.Soares	20/11/2024

Summary

This policy defines guidelines to protect ADDVOLT's computer systems (servers, personal computers, and other systems), using antivirus programs.

An effective implementation of this policy will minimize the risk of ADDVOLT losing information.

This document explains the antivirus requirements of ADDVOLT to achieve the following objectives:

- Protect the assets.
- Reduce the severity of a virus attack.

1. Scope

Viruses, worms and other malicious software pose a growing threat to the integrity, privacy and availability of information, making it necessary to establish rules to promote the security of systems and the information stored or processed in them. In this context, the proper use of antivirus systems represents an unavoidable practice of responsible use.

This policy applies to all ADDVOLT systems or those operated by it, and where it is advisable to use antivirus programs - namely servers and personal computers. It must be put into practice by all ADDVOLT employees, or by those who are allowed access to their systems or computer network.

2. References, Definitions and Terminologies

None.

3. General Rules

All employees, and interested parties, regardless of the resources to which they have access, are responsible not only for the appropriate and safe choice of passwords, but also for their protection against possible misuse and or unauthorized use.

- For computers with Windows operating system is mandatory the installation of antivirus software and the antivirus must be active. Using Bitdefender, Microsoft Defender or another defined by IT is recommended.

- For computers with other operating systems (MacOS or Linux), it is recommended the installation of one antivirus software. Namely XProtect for MAC.

- Computers must be running an updated version of antivirus software, capable of protecting the operating system in real time and automatic updates. The antivirus software should start automatically when each machine is turned on.

- ADDVOLT's IT Operational Department can recommend one antivirus software for each operating system. ADDVOLT adopted Microsoft Defender as the AV solution for all platforms (Windows, Mac and Linux).

- Computer users will notice the icon to the right of the taskbar near the system tray (clock), indicating that the antivirus is successfully installed. If this icon is missing, you must restart the antivirus software.

- Any warnings visible on screen from the antivirus software about identified/detected threats from viruses/malware should be reported to the IT Operational Department as soon as possible and the computer disconnected from ADDVOLT network immediately on seeing the warning.

- Update antivirus software operations should not be interrupted.

- Computers must be regularly connected to the internet to update to the latest versions.

- Under no circumstances should an email or suspicious file be opened; in that case, the computer must be disconnected from the network and the IT Department contacted.
- If a system becomes difficult to use due to interference from an antivirus program, the IT department must be notified.

4. Monitoring and Compliance

ADDVOLT reserves the right to periodically audit networks and systems to ensure that they are following the requirements defined in this standard.

Accordingly, the Security team must monitor compliance with this standard through the various methods at its disposal and considering all Information Security requirements, including, but not limited to, management reports, internal and external audits and feedback information officer, information assets or information processing resources of the ADDVOLT.

Under no circumstances is an employee or ADDVOLT interested party authorized to engage in illegal activities under national or international law using ADDVOLT resources in their possession.