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	21/11/2024

Summary

The purpose of this policy is to clearly define the conditions for installing software on ADDVOLT devices or used by its employees, aiming to minimize the risks and consequences identified above.

1. Scope

Allowing employees to install software on company equipment represents exposure to undesirable risks. Conflicts between applications and software libraries that can result in system malfunctions or vulnerabilities, introduction of malware through the installation of infected software, legal infractions caused using unlicensed software and programs that can be used to affect the security of institutional infrastructure are all examples of risks associated with non-judicious software installation. The possibility of exposure or loss of information integrity resulting from these risks, then, requires the definition of a strict policy of installing software on the company's systems or others used to connect to the former.

This policy applies to all computers, servers, smartphones, tablets, and other processing and / or communication devices that belong to or interact with ADDVOLT systems. It must be complied with by all employees, direct and indirect, who use computer equipment to which the policy applies.

2. References, Definitions and Terminologies

None.

3. Objectives

This document explains how to manage the installation of software in ADDVOLT devices.

4. General Rules

- The software can be installed on the devices they use for their professional activity at the institution, if it meets all the following requirements:
  - Be directly necessary for the performance of professional functions, considering in this group the development tools, libraries, components or similar.
  - Do not violate licensing conditions or incur other illegal situations.
  - Do not engage in any activity that could harm working conditions or the actions of ADDVOLT employees or customers.
  - Do not interfere with aspects of ADDVOLT's infrastructure; in particular, your security or the security of your information.
  - Do not establish direct or indirect connections with external services or systems.
  - Be from a reliable source and, preferably, digitally signed by the producer. In cases where this is not possible, as in certain cases of installation by source code, the integrity of the code must be verified by means such as the analysis of your "fingerprint".
  - In the case of libraries, tools, and software development components where such verification is not possible, the person responsible for the Software Production Unit or the IT Services Department should be consulted.
- In other cases, prior notice must be sent to the IT Services Department, which may, in justified cases, not authorize this installation, proposing alternatives.
- When the installation requires the elevation of privileges before the operating system, this can be done by any user who has been assigned a local account with administration privileges, who must use it exclusively in this circumstance.