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	Ricardo Soares	11/21/2024

Summary

The purpose of this policy is to define rules and requirements for connecting to ADDVOLT's networks, or to a client network from any external system. These rules and requirements were defined in a way not only to avoid situations of irregular access but also to minimize the potential exposure to damage eventually resulting from the use or unauthorized access to your resources. The types of damage considered include, in addition to the traditional ones related to integrity, availability and confidentiality in general, damage to the public image, resulting from legal infractions or the spread of malicious activity to other internal or external systems.

1. Scope

This policy applies to remote access connections used to access information on ADDVOLT's or to the Client's servers. This policy covers all forms of remote access used to connect to ADDVOLT's or Client's networks, including VPN.

2. References, Definitions and Terminologies

None.

3. Objectives

Remote access to ADDVOLT's network and systems is essential for activity performance and maintaining the productivity of the company. However, in many cases, this remote access comes from networks or systems that are not subject to security restrictions, or even possibly already compromised, representing a real risk to the infrastructure and information of ADDVOLT and its Customers. Predicting, identifying, and mitigating these risks is a fundamental task.

4. General Guidelines

- All remote accesses to ADDVOLT information or systems must be made exclusively through a secure channel, using its institutional VPN system and authorized client applications. Authorized application for inbound and outbound is TeamViewer. No additional application shall be used without authorization from IT team.
- Cases where the institutional VPN cannot be used, the IT Department should determine the alternative means.
- In all cases where remote access is subject to the introduction of passwords, these must comply with the password policy.
- When using an ADDVOLT computer to remotely connect to ADDVOLT corporate network, the user must ensure that the equipment is not connected to any other network at the same time, except for personal networks that are under total control or under total control from a trusted supplier.
- All equipment that is connected to ADDVOLT systems, using remote access technologies, must use updated antivirus software that complies with the antivirus policy.
- All connections, including those made by external elements to ADDVOLT, must comply with the requirements established in this and other applicable policies.
- For additional information on ADDVOLT's remote access connection options, including obtaining credentials for remote access, the IT Department should be contacted.
- Each remote access will be subject to limitations on access to internal resources, applied depending on the user who authenticates with the VPN system.
- Remote accesses can be recorded and monitored by the IT Department when we suspect that can have some information security threat.