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	13/08/2024

Summary

In cable networks, information security depends largely on the control of physical means.
In wireless networks, information security depends on how we define the access rules and monitor their application.
The level of security offered by the infrastructure must be homogeneous, without points of vulnerability, guaranteeing in any case a minimum level equivalent to that of a wireless network protected with WPA.

The objective of this policy is to define appropriate practices for controlling connections to ADDVOLT 's physical network.

1. Scope

This policy applies to all computers, servers, smartphones, tablets and other processing and / or communication devices that belong to or interact with ADDVOLT systems or services. It must be complied with by all employees, direct and indirect, who use computer equipment to which the policy applies.
This policy applies to ADDVOLT´s employees, including external consultants, interns, temporary and others, or anyone that is assigned access to the physical network of ADDVOLT.

2. References, Definitions and Terminologies

None.

3. General Rules for Network Security

3.1 Physical Network

- In situations where applicable, closed cabinets should be used to limit access to network points;
- Network sockets that are not necessary must be disconnected in the switching devices (switches);
- Limiting measures must be applied to the network sockets used by devices, such as VLANs that restrict access to resources other than those necessary;
- In general cases, when possible, access to the physical network must be subject to validation through 802.1X, based on pre-authentication in Active Directory;

3.2 Wireless Network

- All electronic devices connecting to one or more wireless networks of the Organization shall:
    - Comply with the standards specified in the Wireless Communication Standard;
    - Be installed, supported, and maintained by the ORGANIZATION's IT Services Department, or alternatively authorized by the same department;
    - Use approved authentication protocols for each network to which they will connect;
    - Use validated and approved encryption protocols;
    - Maintain a hardware address (MAC address) that can be registered and tracked;
    - Do not interfere with wireless access implementations maintained by other organizations.
- Wireless network access point requirements:
    - They must comply with the applicable specific wireless communications standards;
    - They must have the security updates made available by their producers installed;
    - They should require authentication for network access, integrating with the rest of the network infrastructure to restrict access depending on each user's permissions.

- Requirements of wireless infrastructure:
    - There should be separate networks for visits (Guest) and for workers, all of which are always subject to access control;
    - Devices connected to Guest networks should not have access to any assets with classified information;
    - The connection to the Organization's work groups must be subject to validation through active directory authentication;
    - Passwords for access to wireless networks must comply with the ADDVOLT Password Policy.
- Tables of offices and rooms with confidential and / or secret information must be deleted when not needed;
- The keys used to access offices or rooms with confidential or secret information must be handed over to the person responsible for them.

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.