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	20/11/2024

Summary

The Access Control Policy is a document that dictates the necessary requirements for ADDVOLT to ensure access by employees, or authorized interested parties, and to prevent unauthorized access to ADDVOLT information.

This document intends to explain the security requirements for ADDVOLT's access management, to obtain the following objectives:

- Limit access to ADDVOLT's information and information processing resources to the minimum required;
- Ensure access for employees or authorized interested parties;
- Prevent unauthorized access to information or information systems;
- Make employees and interested parties responsible for protecting their authentication information in the systems.

1. Scope

Access management is a focal point for the Privacy and Information Security of ADDVOLT, as each employee or interested party should only have access to the information that they are specifically authorized to use in the course of their work duties.

2. References, Definitions and Terminologies

None.

3. General Rules for Access Control

3.1 General Guidelines

This document serves as a reference to guarantee the logical access of authorized users and prevent unauthorized access through ADDVOLT networks and systems to information, having as its main purpose its Information Security.

Premise through which the main objectives of Access Management are achieved:

- Ensure that only authorized access to information networks and systems is performed;
- Prevent unauthorized access to services available on the network and in information systems; and
- Prevent compromise or theft of information.
- In this sense, guidelines should be defined and followed in order to:
- Identify and register users of networks and information systems;
- Restrict and manage privileged access granted to users;
- Periodically review the existing users, their permissions and the privileges assigned;
- Manage access credentials assigned to users;
- Identify the services and information to be made available to employees, and interested parties according to their work functions;
- Identify access controls to be implemented in networks and information systems; and
- Train and instruct employees, and stakeholders on the topic.

3.2 Access Management Principles

ADDVOLT provides all employees and interested parties with the necessary access to the networks and information systems necessary to carry out their work functions based on the following principles:

- Identity
  - Users of networks and systems must be unique and individual and must be protected by the employee or interested party to which they were assigned.
  - According to Information Classification rules defined in the ISMS, generic or group users, except for rare exceptions, should never have access to information classified as Confidential and Restricted.
- Privileged Accounts
  - The assignment of privileged accounts (e.g. administrator, super-user, root) must be restricted to the minimum necessary and they must be controlled and not assigned by default.
  - The authorization to assign and use these accounts must be explicitly approved.
- Minimum Access Principle
  - The attribution of accesses should always be based on the Principle of Minimum Accesses in order to ensure that employees and interested parties only have the accesses necessary for their work functions.
- Audit

- Networks and information systems must keep a record of user access management, considering login attempts and actions taken by them.
- This record should be reviewed periodically and must be protected to any changes.

3.3 Systems and Networks Access Management

To guarantee the correct and effective access management, the following requirements must be considered:

- A standard nomenclature must be defined to identify each user uniquely;
- All users of ADDVOLT networks and systems must be registered with information regarding their user profile;
- There must be rules regarding the use and management of users' passwords.
- Passwords for users with privileged access (e.g. system administrators) must be subject to stricter rules following ISMS.03.01 - Password Management policy;
- The assignment of privileges to users must be carried out under a formal authorization process and based on minimum privileges for the performance of functions in accordance with the role;
- The authorisation process must ensure that periodic reviews of users' access rights are carried out;
- User accounts must be deactivated immediately after termination or suspension of contractual agreements, or any legal link established with ADDVOLT

3.4 Systems and Networks Identification and Authentication

To ensure the ability to identify a user on networks or systems or the ability to prove that a user is really who he says he is, the following requirements must be considered:

- Ensure the use of organizational identifiers in order to identify users;
- Ensure that only one identifier is created after approval and that it cannot be reused by another employee or interested party;
- An access credential must be assigned to an user individually, guaranteeing improper access are not made instead of its receiver (e.g. SMS access code with limited validity, Authenticator Application) and guarantee the auditability of the access made;
- Define authentication mechanisms that are strong enough to guarantee the security of information on networks and systems;
- Authentication process must use secure sessions and protocols (e.g. HTTPS, TLS);

- Protect and encrypt the authentication content from unauthorized modifications or disclosures;
- Ensure the authenticity of authentication certificates (e.g. CA/Browser Forum);
- Whenever possible, implement two factor authentication mechanisms.

3.5 Systems and Networks Access Controls

To ensure the security of the information processed/stored by ADDVOLT's networks and systems, the following requirements must be considered:

- Security mechanisms at the level of the operating system must be used to restrict or prevent unauthorised access to computers;
- The password management system for accessing networks and systems must be interactive and guarantee their quality;
- The use of applications that overlap and can circumvent the security mechanisms of networks and systems is totally prohibited;
- Time controls for connections should be considered in the case of sensitive systems, mainly when located in high-risk locations;
- Access for application support users and external parties, must be in accordance with the contract signed between the parties

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 the ADDVOLT resources in their possession.