Index

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	Document Creation	All	C.Santos	30/07/2024	B.Azevedo	12/08/2024

Summary

The Password Management Policy is a document that fits the tactical level of the document structure of the ADDVOLT, reflecting security concerns and considerations regarding the ADDVOLT management systems and passwords.

This document explains the password management requirements of ADDVOLT in order to achieve the following objectives:

- Guide in the correct choice of passwords;
- Define password creation rules;
- Define password change and recovery methods;
- Guarantee its use to protect the integrity, confidentiality and availability of the ADDVOLT Information and infrastructures.

1. Scope

Password management is a key point for the Information Security, ensuring the safeguarding of information and the interests of the ADDVOLT, with the main objective of preventing improper access to the information of the ADDVOLT.
In this sense, this document applies to all employees and stakeholders of the ADDVOLT Security Operations Center, regardless of their role, hierarchical position and contractual relationship who are owners of information assets or have access to networks and systems belonging to ADDVOLT.

2. References, Definitions and Terminologies

Password – A password is a string of characters used to verify the identity of a user during the authentication process.
Double Authentication (Two-factor authentication) – is an identity and access management security method that requires two forms of identification to access resources and data.
Password Management System – a system that facilitates a simple, secure way to store, define and manage passwords and access when required.

3. General Rules for Passwords

All employees, and interested parties, regardless 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 effective access to ADDVOLT networks and systems, all authorized users, as a means of authentication, must enter their individual password and these passwords must comply with a set of rules.

3.1. Password Selection

Use of passwords that are not predictable or easily accessible not only guarantees the privacy of employees, and interested parties, but also prevents any attack on ADDVOLT's Information Security.

In this sense, all users must have strong passwords associated, that is, passwords that are designed in such a way that it is unlikely to be detected or stolen, and password management systems must evaluate and force their robustness.

An appropriate choice of passwords must be based on the following assumptions:

- Within the limits of reasonability, the password must be robust, complex and difficult to break, to guess, or to be discovered by third parties.
- The password must be unique and understood only by the user who generates it.
- The password is confidential and non-transferable, being the total responsibility of employees and interested parties that it remains so, without revealing it to anyone.
- The password must not be registered on paper or any other medium (e.g. post-it, notebooks, documents on the computer) easily accessible by third parties;
- Whenever it is necessary to store the password somewhere, authenticated password management systems with a double authentication factor and with the ability to encrypt stored passwords must be used;
- The 'remember password' function present on some systems (e.g. browsers) should not be used;
- Employees and stakeholders should not use passwords that they currently use in personal applications or outside the scope of the ADDVOLT or reuse passwords used in the past.

On the other hand, there are overly simple and insufficient passwords from a security perspective and that, for this reason, should be avoided, such as:

- “password”, “password1”, “Pa $$ w0rd”;
- “Qwerty”, “zxcvbnm”, “asdfgh”, “12345678” or other letter strings on the keyboard;
- Months of the year, weekdays or any dates;
- Family names, family names or initials of names;
- Simple words or phrases (e.g. google, login, welcome);
- License plates for cars, phone numbers or similar;
- Use of identical characters in a row (e.g. aaaa1111);
- Use of identical characters in different versions of the password (e.g. aaaa1111 / baaa2111);
- Use of control or non-printable characters.

A bad choice or misuse of passwords can jeopardize security and impact the confidentiality, integrity, availability of ADDVOLT networks and systems, as well as the privacy of information used or stored in them.

3.2. Password Creation Rules

Based on the assumptions presented in previous section, the choice of passwords must also comply with the minimum requirements, and ADDVOLT networks and systems must be parameterized to prevent the creation of passwords that do not comply with them.

When the rules defined in the following point are not possible to implement, the user should apply the maximum complexity possible.

3.2.1. Common User

User accounts include all access by employees or external parties to ADDVOLT networks and systems, password formulation of these users must comply with the following requirements:

- Minimum length of ten (10) characters;
- Complexity (at least 3 of the following categories should apply):
    - Capital letters of the alphabet (i.e. AA-ZZ);
    - Lowercase letters of the alphabet (i.e. aa-zz);
    - Number characters (i.e. 0-9);
    - Special characters (i.e.!, #, $,%, &).

3.3. Password Change

Password changes must happen periodically, either due to regulatory or operational requirements or because of the need to increase the protection of a given network or system. Accordingly, the following rules must be effective:

- Standard passwords, i.e. assigned, automatically by the systems, must be changed immediately before any action is taken by the user;
- Networks and systems must ensure that the new password complies with the requirements defined above or, if not, present an error message informing about non-compliance with the requirements.
- All users must be forced to change their passwords taking into account the defined maximum lifetime.
- Whenever there are indications of a vulnerability in networks or systems, the password must be changed immediately.
- Whenever technological attacks (e.g. phishing) occur or the occurrence of an Information Security incident that may have compromised user accounts is identified.

3.4. Password Recovery

After inactivity of the account or forgetting the current password, the user is left without access to the network or the system, having to request the recovery of the password.

This recovery can be performed by the employee or external party if the network or system allows it or by the IT Team by assigning a new password, considering the password recovery procedure.

Whenever the network or system allows password recovery, the password change mechanism must be used and following the confirmation instructions of the network or system itself and the assumptions and criteria defined for choosing a new password.

Otherwise, the employee or External party should contact the IT Team through the communication mechanisms made available so that it proceeds to generate a new password and the consequent sending, which must be promptly changed by the employee or interested party to whom it was sent.

4. Monitoring & 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.