## INDEX

REVISION AND APPROVAL HISTORY ..... 1
Summary ..... 1
1. Scope ..... 1
2. References, Definitions and Terminologies ..... 2
3. Objectives ..... 2
4. General Rules ..... 2

## REVISION AND APPROVAL HISTORY

| Revision No. | Description | Page(s) | Made by | Date | Approved by | Date |
|---|---|---|---|---|---|---|
| 1 | General Review | All | C.Santos | 12/08/202 | R.Soares | 20/11/2024 |
| | | | | | | |
| | | | | | | |

## Summary

This policy aims to establish requirements for the protection of encrypted content and encryption keys under the control of ADDVOLT employees.

## 1. Scope

Encryption is an essential tool for protecting information. Based on cryptographic resources, not only can the confidentiality of information be promoted, but it can also validate its integrity. To be effective, however, the use of cryptography must be judicious, not only in selecting algorithms and figures used, but also in key management.

This policy applies to all contexts listed below, as well as to all employees who may be involved in any of the contexts.

## 2. References, Definitions and Terminologies

None.

## 3. Objectives

This document explains how to manage the life cycle of the cryptography key and defines the rules of use of encryption to protect the information.

## 4. General Rules

The encryption policy must be applied cumulatively of, at different levels, according to the following rules:

- Storage
  - Storage devices that contain confidential information and are transported outside the ADDVOLT in the context of everyday use, must have their content protected by encryption. In particular, the contents of portable computer hard drives should be protected, using the resources provided by each operating system. The number to be used should be AES with a 256-bit key, or another considered equivalent.
- Transfer
  - The information resulting from sessions on remote systems must be protected by a service based on a communication protocol using TLS, or another specific one of customers or suppliers when the application scenario requires it.
  - In other cases, the transfer of information should, whenever possible, be protected by TLS or equivalent mechanisms. Included in this scope is the information transferred using protocols HTTPS, SMTPs, POP3, IMAP, or others, in their scope of use. In the case of SSL, systems that implement version 3.0 or higher must be used. If TLS is applied, the version used must be 1.2, or higher.
  - The ADDVOLT must request, from a credible entity, the generation and signature of institutional digital certificates. These certificates must comply with the technically recommended requirements and be used on all servers that deal with critical information, to protect the confidentiality, integrity and reliability of the information transmitted, in addition to protecting users from situations of usurpation of institutional identity.

- Authentication and Integrity Validation
  - Encryption should be used in situations where it allows validating the authenticity of resources or users. Whenever possible, it should be applied to validate software authenticity, before its installation.
- Key management
  - Keys used in encryption mechanisms, in particular private keys used in public key cryptography, should always be kept securely. Specifically:
    - They must never be stored in email or other mechanisms where they may be exposed to third parties.
    - When applied to servers to protect services, they should also be protected by secure encryption whenever possible.
    - They should never, in general, be kept in digital format without cryptographic protection.