# 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 | 11/21/2024 | Ricardo Soares |
| | | | | | | |
| | | | | | | |

## Summary

The purpose of this policy is to establish rules for the communication of information classified as "confidential".

## 1.  Scope

This policy applies to all ADDVOLT employees who receive or send information classified as "confidential".

## 2.  References, Definitions and Terminologies

None.

## 3.  Objectives

Information transfer classified as confidential, from outside and to outside, must be adequately protected to promote its security. This policy essentially addresses the components of integrity and confidentiality, preventing that in the event of improper access to information, it can be manipulated or accessed.

| | |
|---|---|
| Doc. Type | POLICY |
| Doc. Number | ISMS.15.01 |
| Department | ISMS |
| Creation Date | 2024-03-29 |

**ADDVOLT®**

Information Transfer Policy

## 4. General Guidelines

All information classified as "confidential" and that needs to be transferred must be previously protected by strong encryption. When possible, encryption can be applied at the transport channel level, if there is a guarantee of this means for effective protection from shipment to delivery and storage at the recipient (for example, VPN or pen drive with native cryptographic support and considered secure).

Whenever the conditions described above are not met, the general information protection method should be applied:

- File encryption with a password, preferably using the means offered by the operating system or utilities approved by the ADDVOLT IT Department. SharePoint is the approved method for file sharing. Access must be controlled and limited in time or revoked when not necessary.
- In cases where it is necessary to transfer multiple files, a single archive file may be created, applying the general method described above.
- All passwords to be used must comply with ADDVOLT's policies for that scope.
- Direct file sharing through Teams is not allowed with accounts external to the organization. SharePoint links must be used instead.

Receiving information from customers or suppliers may be an exception to the general terms, as it may be subject to the respective policy of the customer or supplier concerned. In these cases, you should:

- Check if the Customer or supplier has an adequate information transfer policy
  - o If the customer or supplier has a protected information transfer policy:
    - ▪ Use the client's methodology.
    - ▪ Confirm receipt of the information with the Client.

If the customer or supplier does NOT have a protected information transfer policy:

- Inform the customer or supplier about ADDVOLT's general method of transferring information, assisting in its application.
- If the customer or supplier refuses to use the indicated methodology, inform him that ADDVOLT will not be responsible for the consequences that may arise from a transfer made inappropriately.

Whenever encrypted data is exchanged to/from outside Europe, ensure compliance with requirements applicable at the other transfer location. For the first analysis can be consulted the https://www.gp-digital.org/world-map-of-encryption/