## INDEX

## REVISION AND APPROVAL HISTORY

| Revision No. | Description | Page(s) | Made by | Date | Approved by | Date |
|---|---|---|---|---|---|---|
| 1 | General Review | All | C.Santos | 18/09/2024 | Ricardo Soares | 11/21/2024 |
| | | | | | | |
| | | | | | | |

## Summary

The correct reuse and disposal of data storage media that contain or may contain classified information is of great importance to ensure that this information does not leave ADDVOLT's control.

This policy aims to establish guidelines for the reuse and disposal of data carriers where classified information is or may have been stored.

## 1. Scope

This policy applies to the disposal of information storage media, such as those listed below, although not exclusively:
- Hard disks and backup tapes, regardless of their technology
- Hard disks of personal computers, servers and other equipment, regardless of their technology
- Paper records
- External disks or pen drives, regardless of their technology
- Mobile phones

## 2. References, Definitions and Terminologies

None.

## 3. General Rules

The following good practices should be followed:

1. Digital media
   a. Low-level initialization/formatting of storage devices (hard disks, tapes, pens, memories, etc…) to ensure that they can no longer be recovered or, in cases where this is not possible, to physically damage the storage media, ensuring that they cannot be recovered.
   b. In cases where physical access to the storage medium is not possible, use the most appropriate tools for the type of medium in question. For example, in the case of information stored in cloud systems, apply the specific tools or procedures defined by the service provider.

2. Paper media
   a. Documents containing confidential information must be physically destroyed in a machine designed for this purpose before being sent for recycling or treated as waste.

3. In case of doubt, the ISMS Manager or IT Manager should be consulted.

## 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 ISMS 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.