INDEX

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Revision	All	C.Santos	12/08/2024	R.Soares	18/11/2024

Summary

This Policy defines the conditions for the use of electronic message exchange services, within the scope of ADDVOLT's activity. The policy also defines the appropriate conditions for sending messages, to protect the information conveyed and prevent damage to ADDVOLT's image. It is essential to consider that any electronic message sent from an ADDVOLT domain, containing a signature with reference to the ADDVOLT, or any other that represents ADDVOLT, its collaborators or systems as authors, will be or may be considered by the public generally as an official statement or position of ADDVOLT.

This document explains the practices we should adopt to keep information protected when it is sent by email or messaging service.

1. Scope

The email service provided by ADDVOLT to employees is an essential tool for internal and external communication. The inappropriate use of this tool, however, can result in negative consequences for the institution - particularly due to the undue exposure of information and consequent loss of confidentiality.
This policy applies to all message exchange services that can be used by employees of ADDVOLT. Strict compliance is required of all employees.

2. References, Definitions and Terminologies

None.

3. General Rules

- It is acceptable for employees of ADDVOLT to use ADDVOLT's e-mail system for personal purposes, provided that such use is properly moderate, does not violate the company's code of conduct and respects the rules established in the Internal Regulation and in this policy.
- It is prohibited to send chain letters using an email from ADDVOLT.
- Mass email sending, i.e., to a large distribution list, should only be done by ADDVOLT employees who need this type of extended communication (administration, human resources, corporate communication, etc.).
- The content of the messages covered by this policy is also protected by ADDVOLT's information protection policies, promoting its integrity, confidentiality and availability. Users should always keep this aspect in mind, in particular, when sending information abroad.
- Reinforcing the previous point, automatic forwarding of information to the outside should never be done. Institutional email content should be kept on official servers or on personal systems where it is viewed, but never transferred to other external systems.
- It is strictly forbidden for any employee to send e-mails other than through the authorized e-mail systems.
- The creation of e-mails impersonating a third party is a serious violation of this security policy and may give rise to disciplinary and legal procedures.
- Employees should never open documents, files or URLs (links) that they receive in attachments to an e-mail whose origin is unknown or suspicious, or that there is a suspicion that the content may be harmful to the proper functioning of the computer system. These emails should be deleted immediately, and the “Deleted Items” folder should be emptied later. All spam emails, chain letters, and alike should be immediately deleted (including from the deleted items folder) and should never be resent. The employee must also immediately report to the IT Department

any suspicion that an e-mail received may cause a security breach in ADDVOLT's systems, as well as any suspicion of password theft or identity theft.

- The employee must notify the IT Services Department, in the event of receiving frequent spam or chain letters.

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 ADDVOLT resources in their possession.