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 Acceptable Use Policy is a document that reflects the rules for acceptable use of information that must be known to all employees and interested parties when using ADDVOLT assets.

1. Scope

The way in which information is used constitutes a focal point for ADDVOLT Information Security, regulating the actions that employees, or interested parties can carry out on ADDVOLT information. Since all employees and stakeholders are responsible for making good judgments in conscience related to the good use of information.
In this sense, this document applies to all employees and stakeholders, regardless of their role, hierarchical position and contractual relationship who have access to ADDVOLT information.

2. References, Definitions and Terminologies

None.

3. General Rules for Acceptable Use

3.1. Limitations

In order to guarantee and maintain an appropriate level of protection for your information assets, ADDVOLT is committed to:

- Identify assets and maintain an updated inventory with the identification of the people designated as their owners;
- Establish the duties of the owners, covering the protection and maintenance of controls on the assets and information of the ADDVOLT;
- Instituting the rules for an acceptable use of ADDVOLT information and assets materialised in different specific rules and regulations;
- Establish an information classification system that should be used to define security levels;
- Define the expected protection categories for each of ADDVOLT assets and information, in order to establish classification and management procedures for them.
- All safety guidelines applicable to the systems must be detailed in terms of configurations, specific developments or other measures in order to ensure that they are implemented by all areas responsible for the management of ADDVOLT systems through standards and regulations appropriate to the matters referred to.
- In all systems whose technical nature does not allow the fulfilment of a certain configuration, this fact must be recorded in order to recognize and implement compensatory controls that aim to mitigate the identified risks. In more complex situations, the level of related risk and the cost / benefit ratio of implementing additional controls should be reassessed.

3.2. Information Access

The authorization of physical and logical access to any type of information is the responsibility of the respective owner of the information asset concerned and is conditioned by the need to use it to perform the operational functions within the ADDVOLT.

Employees and stakeholders are responsible for making good judgments related to the reasonableness of individual behaviours. Additionally, at all times, they must follow the requirements defined at Information Security Management System documents, and in case of doubt, Security team must be contacted.

Access to any type of information asset is prohibited without prior consent of information owner. This authorisation may be implied by the assigned rating level (e.g. public), but it is formally mandatory at the most restricted levels of criticality. Access to any type of information by external entities to ADDVOLT is only allowed through the existence of a contractual relationship that justifies it, or a formal authorisation from the information owner. Whenever ADDVOLT makes new services

that include any type of remote access to information residing in its systems available to other entities with whom it relates, control procedures and mechanisms must be defined to ensure its security.

In order to guarantee the non-repudiation of activities with impact on information security, measures must be implemented that are technically and economically feasible to allow an effective identification of the activities in question and their authors, namely, the maintenance of the necessary information, event records, in accordance with applicable law and relevant internal rules.

3.3. Widespread Usage

ADDVOLT information stored in electronic devices owned or contracted by ADDVOLT by employees remains the property of ADDVOLT.

The owner of the information is responsible for circumscribing the controls that guarantee the use and availability of the information as a corporate resource in accordance with the rules and regulations instituted.

Employees access the information according to the respective confidentiality classification conferred and the prior consent of the owner of it, being responsible for complying with the controls established and using the information only for the purposes for which they are authorized.

The situations of theft, loss or usurpation of the ADDVOLT proprietary information must be immediately reported.

All employees must not talk about classified information in public spaces, either in person or by telephone.

3.4. Inappropriate Usage

The following activities are generally prohibited. However, employees, or interested parties may be exempt from them in the course of their work activities.

Under no circumstances is an employee, or interested party authorized to perform any activity that is illegal while using ADDVOLT resources.

ADDVOLT reserves the right to prohibit, at any time, activities that damage its reputation and good name and to monitor, access and use the activities carried out as evidenced in litigation, audits or investigations. It is also prohibited to carry out any activity that includes transmission, distribution or storage of material that violates any applicable Law and regulation, including, but not limited to:

- Material protected with copyright, trademark and property rights without authorization and in an inappropriate manner
- Material that is obscene, defamatory or that constituted a legal threat;
- Material that involves slander, invasion of privacy or harassment.

3.5. Systems & Networks

At the level of ADDVOLT systems and network, the following activities are forbidden:

- Violate the rights of any person or company protected by copyright, trade secret, patents or other intellectual property in accordance with the law and similar regulations, including copying multimedia material or installing or distributing unlicensed software for use by ADDVOLT;
- Provide information about employees, or stakeholders outside ADDVOLT;
- Reveal passwords of ADDVOLT user accounts;
- Make fraudulent offers of ADDVOLT services;
- Violating the security of systems and network, including accessing data to which employee, or interested party is not a recipient, accessing a server through an unauthorized user account, network sniffing or scanning, flooding server with pings, falsify packages, compromise availability or transmit viruses or malicious code;
- Bypass user or security authentication on any system or network.

3.6. Email & Communications

Regarding the ADDVOLT's email and communications, the following activities are forbidden:

- Sending unsolicited e-mail messages to people who have not requested it (e.g., spam, advertising);
- Use without authorization or falsify information in electronic mail headers;
- Use e-mails from internet, intranet or extranet service providers on behalf of, or to disclose, any ADDVOLT service;
- Send messages that are the same or whose subject has nothing to do with ADDVOLT to a large group of users;
- Issuing opinions or communicating information via ADDVOLT's email without notice that they are the responsibility of ADDVOLT, unless he is carrying out his duties;
- Open email attachments received from unknown senders, as they may contain viruses or malicious code.

3.7. Social Networks & Instant Messaging

Social networks and instant messaging tools should only be used when approved and with a commercial and marketing basis.

ADDVOLT allows the use of social networks and instant messaging tools for personal use as long as it is not carried out in an abusive manner and under certain conditions. Accordingly, the following activities are prohibited:

- Use social networks or instant messaging tools from a consumer perspective or other external resources to conduct ADDVOLT related topics;
- Use social networks or instant messaging tools to transmit confidential, proprietary, personal or potentially embarrassing information about ADDVOLT or its employees or stakeholders.

3.8. Data Protection

Employees and interested parties must recognize the fundamental principles of data protection, in particular considering the General Data Protection Regulation:

- Personal data must be treated fairly and legally;
- Personal data must be processed for limited purposes;
- Personal data must be adequate, relevant and not excessive;
- Personal data must be accurate and up to date;
- Personal data must not be stored any longer than necessary;
- Personal data must be processed in accordance with the rights of the data subjects;
- Personal data must be protected;
- Personal data must not be transferred without prior authorization and guarantee of protection.

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 Policy and other policies and documents of ISMS.

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.