INDEX

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Review	All	C.Santos	2024-09-10	Ricardo Soares	11/21/2024

Summary

Mobile devices like smartphones and tablets are important tools for daily activity, leisure or professional support. However, mobile devices also pose a significant risk to systems and information security. Without complying with adequate security procedures, mobile devices can become a channel for unauthorized access to ADDVOLT's infrastructure, allowing breaches of confidentiality and availability, or at the limit, of information integrity.

In the defense of its interests, as well as those of its customers, ADDVOLT has an obligation to protect the information assets it uses during its activity.

1. Scope

This policy applies to all personal devices that have access to the ADDVOLT's networks and that belong to its employees, including external consultants, interns, temporary and others, or who use their own devices that have access to the company's networks, and must be met by its owners.

The purpose of this policy is, in addition to other policies, to define the set of practices and requirements for the safe use of mobile devices within its computer network.

2. References, Definitions and Terminologies

None.

3. General Rules

Technical requirements

- The devices must comply with that defined in the ADDVOLT's Wireless Network Security Policy.
- The devices must use one of the following operating systems: Android 9.0 or later, IOS 12 or later.
- Devices must store all registered passwords in encrypted storage, or do not store them.
- Devices should not be jailbroken or have any software / firmware installed that allows access to functionality not intended for users.
- The devices must not have installed pirated software or other illegal content.
- All installed applications must be obtained from sources officially approved by the owner of the operating system platform.
- Installing code from untrusted sources is prohibited. If in doubt, contact the IT Services Department.
- Devices must be kept up to date with patches provided by the manufacturer. The user must carry out this check at least weekly.

User Requirements

- Users should only upload data to their mobile devices that is essential for the exercise of their function, such as email messages.
- The devices should never have saved access data to resources that are not personal - particularly, from ADDVOLT or its customers. For example, there should never be configurations of VPN access to ADDVOLT or its customers, with permanently stored credentials.
- The access control to the devices must be done by biometric means, or a secure password that complies with the “Password Policy (ISMS.02.01)”, if possible. If it is not

possible to comply with this requirement, the control must be conditioned to a password that is as robust as possible.

- In ADDVOLT's infrastructure, except for devices that may be authorized by the person in charge of the IT Services Department, the devices covered by this policy may only be connected to guest networks (Addvolt-Guest).
- Users should notify the IT Department of all lost or stolen devices, if they contain company data.
- Users should be cautious about the simultaneous use of personal and work email accounts on their devices, taking special care to ensure that company data is only sent via the company's email system. If a user suspects that company data has been sent from a personal email account, either in the body of the text or as an attachment, he must notify the IT Services Department.

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.