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 the ADDVOLT Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

1. Scope

The ADDVOLT Vulnerability Management Policy applies to individuals who are responsible for the management of any asset.

2. References, Definitions and Terminologies

None.

3. Objectives

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimise their "attack surface". This policy describes the baseline to guarantee the application of the vulnerability management process in all ADDVOLT support assets.

4. General Guidelines

- Patch Management
  - The ADDVOLT IT team maintains overall responsibility for patch management implementation, operations, and procedures.
  - All Information Resources must be scanned on a regular basis to identify missing updates.
  - All missing software updates must be evaluated according to the risk they pose to ADDVOLT
  - Missing software updates that pose an unacceptable risk to ADDVOLT Information Resources must be implemented within a time period that is commensurate with the risk as determined by the ADDVOLT Change Management Policy.
  - Software updates and configuration changes applied to Information Resources must be tested prior to widespread implementation and must be implemented in accordance with the ADDVOLT Change Management Policy.
  - Verification of successful software update deployment will be conducted within a reasonable time period, and it should be monitored with adequate tools.

- Vulnerability Scanning
  - Vulnerability scans of the internal and external network must be conducted at least quarterly or after any significant change to the network.
  - Failed vulnerability scan results rated at Critical or High will be remediated and re-scanned until all Critical and High risks are resolved.
  - Any evidence of a compromised or exploited Information Resource found during vulnerability scanning must be reported to the ADDVOLT Information Security Officer and IT support.
  - Upon identification of new vulnerability issues, configuration standards will be updated accordingly.