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

Event registration is essential for the operational management of information systems. It is this registry that implements the primary mechanism to support the monitoring and control of activity, allowing its analysis and audit to identify possible risks and incidents.

1. Scope

This policy applies to all ADDVOLT systems that may carry out activities whose monitoring may be relevant. This group includes physical access control systems, physical servers, operating systems, services, and applications.

2. References, Definitions and Terminologies

None.

3. Objectives

The purpose of this policy is to define a policy and a set of procedures for centralized collection and storage of system events, promoting the reliability of the information collected and allowing its subsequent analysis, in order to identify in advance any risks or signs of activity that it may place, concerning the integrity, availability or confidentiality of information.

4. General Guidelines

ADDVOLT collects activity information from different systems in its infrastructure. This information is used to measure or identify, among others:

- Regular and authorized use of resources.
- The correct functioning of systems.
- Possible illegitimate accesses or attempts to access information or systems.
- The adequate implementation of security control measures.
- The eventual exercise of illicit or illegal activity.
- Compliance with policies and procedures.

The IT Department of ADDVOLT implements a centralized mechanism for collecting activity information in compliance with the following requirements:

- In all monitored systems, a component responsible for sending activity information to the centralized system will be installed, regardless of whether it can continue to store it locally. In cases where this is not possible, external services will obtain this information, then deliver it to the central registration system.
- The central registration system will be executed in a protected system, isolated from other functionalities, and will use a database to store the information.

- Upon receiving a registration request, the central system will always add time information and identification of the origin of the request. This information will be used to identify eventual situations of temporal desynchronisation between what is reported by each system and the one verified, resulting from malfunction or system manipulation.
- All stored records will also be associated with a digital signature, allowing the identification of possible situations of fraudulent manipulation of activity records.
- The registration system will also include a query interface, where filters can be applied to analyse the registered information.

The IT department is responsible for the regular analysis of the recorded information, taking appropriate response measures in case of identification of irregular situations