INDEX

REVISION AND APPROVAL HISTORY

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

Summary

The Organization's activity requires storing and processing information, internal and customer, in various computer systems. Implementing policies promoting the security of this information, such as the Server Security Policy, requires that changes be applied to each system with varying periodicity. It is, therefore, necessary to properly manage a situation where the non-implementation of preventive and corrective measures is unacceptable, but the introduction of changes may also mean a risk.

1. Scope

This policy should apply to all servers that store confidential information or support critical systems, and in all cases where the change in the execution environment to be applied to a particular server may entail some risk to the system or to the information contained therein; in particular, loss of availability of the services published by the system, or loss of confidentiality or integrity of the information.

2. References, Definitions and Terminologies

None.

3. Objectives

The objective of the Change Management Policy, then, is to minimize the risk introduced by the introduction into information systems that contain classified information or support critical services, maximizing the protection of its content and promoting its availability.

4. General Guidelines

- Any changes within the scope of this policy must be implemented by an IT Support department member and previously authorized by the head of the same department.
- Where possible, the change should be validated in advance in a quality control environment before being passed on to productivity systems.
- Changes should be applied at times when the impact on the operation is minimal.
- When applying the change to systems in a productive way, the possibility of going back on the operation should always be safeguarded, resuming the initial scenario, with the least possible impact on the operation and without risk to the stored information.
- In the implementation of the previous point, it is to:
  - In the case of virtualized systems, pre-stop services may allow change of relevant information, create a copy of the system and apply the change.
  - There are no non-virtualized systems operating with classified information in the organization's infrastructure. However, a change in a virtualization support system can lead to the loss of information and service availability. Thus, in these cases, an alternative infrastructure should be prepared in advance, where minimum services can be made available in the event of any resulting failure of the amendment introduced.
- After the change is applied, all services should be reactivated, and the correct operation of the system verified. Only after the operationality and final integrity of the system have been properly validated can the previously made copy be deleted.