Security Domains

Security Awareness: Salto Systems conducts regular awareness campaigns across the organisation to prevent and mitigate users' risks.

Physical Security: Salto Systems protects its facilities using appropriate access control systems to restrict access to authorised personnel. In addition, secure areas such as data centers have additional protection measures against environmental threats.

Security Incidents: Salto Systems maintains incident response plans including personal data breach management.

Access Control: Salto Systems implements appropriate access control to ensure access to the applications and systems in general is restricted according to least privilege and need to know principles. All personnel access Salto System's systems with a unique identifier (user ID). In case personnel leave the company, their access rights are revoked.

Network Security: Salto Systems employs encrypted and authenticated connections for connecting to platforms and systems in general by using security capabilities such as firewalls, VPN and authentication mechanisms.

Secure workstations: Salto Systems implements appropriate protection over end user's devices such as advanced antimalware protection, hard disk encryption and appropriate patch levels.

Privacy and Security by design: Salto Systems applies privacy and security by design principles when adopting a new system or enhancing an existing one. This also includes a secure SDLC when it comes to developing software or products.

Vulnerability Management: Salto Systems conducts security reviews on periodic basics and remediate the identified vulnerabilities in order to maintain platforms secure.

Resiliency: Salto Systems adopts backup and disaster recovery plans for adverse situations.

Assurance: Salto Systems conducts regular reviews to ensure compliance with the security policies and standards.

Disclaimer:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, Salto assumes no responsibility for any errors or typos that the downloadable version may contain.

Part of the content of this document may have been generated or assisted by artificial intelligence tools. This document may also include automatic or manual translations provided exclusively for informational purposes, which may contain errors or inaccuracies. Salto does not guarantee the accuracy, quality, or reliability of such content or translations, including those generated by AI.

The User is responsible for verifying the information contained in this document and, in case of doubt, must refer to the original English version, which shall prevail in the event of any discrepancy. Other language versions are provided for informational purposes only.

Although Salto makes reasonable efforts to review the content of its downloadable documents, they may contain errors or omissions. Salto assumes no liability arising from the User's use, interpretation, or decisions made based on the information contained in this document, which is used at the User's sole responsibility.

For more detailed information on the use of artificial intelligence, translations, and applicable limitations of liability, please refer to the "Terms of Use of our Website".

Copyright ©2026 SALTO Systems S.L. All rights reserved

As Salto reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.

Copyright ©2026 SALTO Systems S.L. All rights reserved