Responsible Vulnerability Disclosure Policy

We take the security of our systems seriously and we welcome feedback from security researchers in order to improve the security of our products and services.

We require that all researchers take into account the respect for the law. Vulnerability scanning could not serve as a pretext for attacking a system or any other target. Several actions must be avoided. For example:

- Using social engineering
- Compromising the system and persistently maintaining access to it
- Changing the data accessed by exploiting the vulnerability
- Using malware
- Using the vulnerability in any way beyond proving its existence. To demonstrate that the vulnerability exists, the reporter could use non-intrusive methods. For example, listing a system directory
- Using brute force to gain access to systems
- Sharing vulnerability with third parties
- Performing DoS or DDoS attacks

Keep information about any vulnerabilities you've discovered confidential between yourself and Salto Systems until we resolve the issue.

Send an email to securityalert@saltosystems.com if you have identified any issue that potentially can affect the security of our products or services.

We invite ethical hackers to discover vulnerabilities through our Bug Bounty Program on Intigriti.

We strive to acknowledge receipt of your vulnerability report within 7 business days and to complete the triage process within 14 business days. Throughout the process, we will keep you updated on our progress and the completion of any remediation efforts through our bug bounty program.

If additional information is needed, we may reach out to you for clarification. The remediation of reported vulnerabilities is prioritized based on factors such as impact, severity, and exploit complexity. Given these considerations, some reports may require additional time for triage or resolution. You are welcome to check in on the status; however, we kindly request that you do so no more than once every 14 days to allow our teams to focus on remediation activities.

In addition, for some of our products, we're inviting ethical hackers to find vulnerabilities through our Bug Bounty Program on Intigriti.

Get rewarded for making us stronger! Sign up here.

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

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

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".

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