

Vulnerability Disclosure Policy

Responsible reporting, investigation and remediation of security vulnerabilities

Version	Effective date	Document owner	Contact
1.0	September 2026	SALUS Controls PLC Security Team	security@saluscontrols.com

1. Introduction	2
2. Scope.....	2
3. Reporting a Vulnerability.....	3
4. Information to Include	3
5. Response Process.....	4
6. Risk-Based Remediation.....	4
7. Coordinated Vulnerability Disclosure	4
8. Security Update Support.....	5
9. Out of Scope.....	5
10. Responsible Security Research	5
11. Contact.....	6
12. Policy Updates.....	6
13. Acknowledgement	6

1. Introduction

SALUS Controls PLC is committed to protecting the security of its products, services, and customers. We welcome responsible reports from customers, security researchers, partners, developers, and other members of the security community who identify potential security vulnerabilities affecting SALUS Controls PLC products or services.

Our goal is to investigate potential vulnerability reports promptly, communicate appropriately with the reporting party throughout the process, and provide proportionate remediation or mitigation to protect users.

Report potential security vulnerabilities privately to security@saluscontrols.com. SALUS Controls PLC will acknowledge receipt within three business days and, in all cases, no later than seven calendar days. This acknowledgment only confirms receipt of the information and does not imply that the reported issue has been confirmed as a vulnerability.



2. Scope

This policy applies to security vulnerabilities affecting:

- SALUS Controls PLC products
- Firmware and software
- Mobile applications
- Cloud services
- Publicly accessible web applications and websites

For product installation, configuration, warranty, or other non-security enquiries, please contact our Customer Support team through the standard support channels.

We accept security reports concerning SALUS products regardless of lifecycle status. For products within their published security support period, vulnerabilities and security updates are handled in accordance with applicable legal obligations. For products outside that period, SALUS Controls PLC will still assess reports and may provide mitigations, migration advice or other guidance according to risk, technical feasibility and applicable obligations.

3. Reporting a Vulnerability

If you believe you have identified a security vulnerability, please report it privately by emailing security@saluscontrols.com. Please report suspected vulnerabilities using this [template](#).

Reports may be submitted anonymously. The absence of a name or two-way contact method will not prevent receipt or initial assessment, but it may limit our ability to request additional information, provide status updates or offer public recognition.

We accept an initial report sent by ordinary email or another channel. If exploit code, credentials, personal data, customer configurations or other sensitive information need to be exchanged, SALUS Controls PLC will offer an available secure method for continued communication. A reporting party's inability or decision not to use encryption will not, by itself, cause the report to be rejected.

4. Information to Include

To help us investigate your report efficiently, please include, where possible:

- Product name and model
- Firmware or software version
- Description of the vulnerability
- Steps required to reproduce the issue
- Expected and actual behaviour
- Potential security impact
- Screenshots, logs, or proof-of-concept, if available
- Your preferred contact details for follow-up

Please avoid including sensitive personal information unless it is necessary to demonstrate the vulnerability.

Please also indicate, where known, whether the issue is public, is being actively exploited, has affected users, or has been reported to another supplier, vendor or coordinator. You do not need to provide every requested item for us to accept and register a report.

During coordinated disclosure, access to non-public vulnerability information is restricted on a need-to-know basis. SALUS Controls PLC may share necessary information with product teams, suppliers, coordinators, affected parties or competent authorities for validation, remediation, user protection and compliance with legal obligations, subject to appropriate confidentiality and data-protection controls.

Personal data submitted with a vulnerability report is processed in accordance with the applicable SALUS Controls PLC privacy notice. Please refer to the privacy-notice URL:

<https://saluscontrols.com/gb/website-privacy-cookies/>.

5. Response Process

After receiving your report, SALUS Controls PLC will:

- Acknowledge receipt within three business days and, in all cases, no later than seven calendar days; where possible, include a unique case identifier and preliminary status information.
- Perform an initial assessment within seven working days
- Validate the reported vulnerability
- Assess its severity and potential impact
- Develop a remediation plan or security update where appropriate
- Keep you informed throughout the investigation and remediation process
- While a case remains active, provide a substantive status update at least once every 30 calendar days and communicate sooner when the confirmed scope, risk, remediation approach or disclosure date changes materially.
- If additional information is required, we may contact you during our investigation.

6. Risk-Based Remediation

Confirmed vulnerabilities are prioritized according to technical severity, exploitability, affected products, potential impact, user exposure, evidence of active exploitation, available mitigations and safe deployment needs. A numerical score may inform the assessment but does not alone determine remediation priority.

SALUS Controls PLC establishes a case-specific remediation target and communicates material changes to the reporting party. Where immediate remediation is not possible, appropriate mitigation or risk-reduction guidance may be provided before a permanent fix is available.

7. Coordinated Vulnerability Disclosure

SALUS Controls PLC works with the reporting party and, where needed, suppliers, coordinators and other affected parties to establish a case-specific disclosure date. The timing may be revised according to severity, active exploitation, user risk, remediation and deployment progress, supply-chain dependencies and applicable legal or regulatory duties. Material changes to the target date will be communicated to relevant parties.

SALUS Controls PLC may accelerate user notification or public disclosure when a vulnerability is already public, is being actively exploited, presents an urgent user risk, is likely to leak, or when notification is required by law. Where a complete fix is not yet available, SALUS may provide temporary mitigation or risk-reduction guidance without unnecessarily enabling exploitation.

Information about remediated vulnerabilities will be published in accessible human-readable security advisories. Advisories will identify the vulnerability and affected products, publication and revision dates, potential impact and severity, available remediation or mitigation, required user actions and contact information. Third-party component advisories may refer to authoritative upstream information where this enables users to determine whether SALUS products are affected.

Vulnerability information will also be made available in a widely recognized machine-readable format unless a justification for not doing so is documented and approved. Publication may be

delayed or omitted only where the applicable conditions have been assessed, documented and approved.

Where required by applicable law or necessary to protect users, SALUS Controls PLC will inform affected users and provide available mitigation or corrective guidance through appropriate accessible channels.

8. Security Update Support

SALUS Controls PLC provides security updates throughout the support period established for each applicable product. The support period is determined in accordance with applicable legal requirements, considering the expected period of use of the product, its nature and reasonable user expectations.

The support period will be at least five years unless the product is reasonably expected to be in use for a shorter period and may be longer where justified by the expected product lifetime. The applicable support-period end date will be communicated through the relevant product information.

9. Out of Scope

All potential security reports are registered and receive an initial assessment. Issues that are purely functional, commercial or support-related may be routed to the appropriate support channel. If an issue cannot initially be reproduced, SALUS Controls PLC may request additional information and may reassess the report when new evidence becomes available.

Theoretical issues, physical-access scenarios, denial-of-service conditions, social-engineering scenarios and third-party dependencies are assessed according to their realistic security impact, exploitability and the product's intended and reasonably foreseeable use.

Vulnerabilities in third-party components integrated into, supplied with or relied upon by a SALUS product remain subject to SALUS product-impact assessment.

10. Responsible Security Research

SALUS Controls PLC supports responsible security research conducted in good faith. We ask researchers to:

- Act responsibly and ethically
- Avoid disrupting products, services, or customer operations
- Avoid accessing, modifying, or deleting customer data
- Report vulnerabilities privately through the process described in this policy
- Allow SALUS Controls PLC reasonable time to investigate and remediate the issue before public disclosure
- Comply with all applicable laws and regulations while conducting security research

When a reporting party acts in good faith, complies with this policy, avoids harm and reports promptly, SALUS Controls PLC does not intend to initiate legal action solely because of security research conducted in accordance with this policy. This statement does not authorize access to third-party systems or data, bind a third party or authority, or remove the reporting party's obligation to comply with applicable law and obtain required permission.

11. Contact

For all security-related reports or questions regarding this policy, please contact:

SALUS Controls PLC Security Team

Email: security@saluscontrols.com

12. Policy Updates

This policy is reviewed at least annually and following material changes to applicable legal requirements, reporting channels, product scope or vulnerability-handling processes. The current version, publication date, last-updated date and policy owner are displayed with the published policy.

13. Acknowledgement

With the reporting party's consent, SALUS Controls PLC may acknowledge the name, alias or organisation of a reporting party that submits a valid vulnerability report and supports coordinated disclosure. Reports may be submitted anonymously, and declining recognition does not affect acceptance, prioritisation or remediation decisions.

This policy does not establish a bug bounty or guarantee financial or other rewards.

SALUS Controls PLC - Suspected Vulnerability Report Form

Use this form to report a suspected security vulnerability affecting a SALUS product, application, cloud service or website.

Please complete as much information as you can. You do not need to complete every field for us to accept your report.

You may submit a report anonymously. However, if you do not provide contact details, we may be unable to request additional information or provide updates about your report.

Once completed, please send this form to **security@saluscontrols.com**.

Please do not include passwords, authentication tokens, private keys or unnecessary personal/customer data.

Fields marked "Required" are required only where reasonably available. If you do not have all information, you may still submit the report.

Suspected Vulnerability Report

1. Reporter Information

Field	Response
Name or alias (Optional)	
Organisation (Optional)	
Email/Contact method (Required unless reporting anonymously)	
Preferred language (Optional)	
Reporting anonymously?	☐ Yes ☐ No

2. Affected Product or Component

Field	Response
Product or service name (Required)	
Model (If applicable)	
Hardware version (If known)	
Firmware / Software / Application version (If known)	
Country/ Region	
Other relevant configuration information	

3. Description of the Suspected Vulnerability

Field	Response
Short title (Required)	
Please describe the security issue you identified (Required)	
When did you first notice the issue?	
What did you expect to happen?	
What actually happened?	
Can you reproduce the issue?	☐ Yes ☐ No ☐ Sometimes ☐ Unknown
If possible, describe the steps needed to reproduce it:	
What security impact do you think the issue could have?	
Attachments included? You may provide relevant screenshots, logs, videos or proof-of-concept information.	☐ Yes ☐ No

Additional technical information (optional – for security researchers)

Field	Response
Vulnerability type (Authentication bypass, injection, memory corruption, etc.), if known	
CWE/ CVE, if known	
Technical cause / details	
Test environment / configuration	
Proof of concept	

4. Attack Scenario

The attack scenario is different from the reproduction procedure. Describe how a realistic attacker could exploit the issue.

Field	Response
If known, please describe how someone could exploit this vulnerability	
Attacker access	☐ Remote network ☐ Adjacent network ☐ Local network ☐ Local device ☐ Physical access ☐ Unknown
User interaction required	☐ Yes ☐ No ☐ Unknown
Special permissions/ account required	☐ Yes ☐ No ☐ Unknown If Yes, please describe the permissions / account required:

5. Impact Assessment (Optional)

Complete this section if you can assess the potential impact.

Impact area	Reporter assessment
Confidentiality	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Integrity	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Availability	☐ None ☐ Low ☒ Medium ☐ High ☐ Unknown
Safety	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Privacy	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Supply-chain or broader ecosystem impact	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Suggested severity, if available (Optional)	☐ Low ☐ Medium ☐ High ☐ Critical ☐ Unknown
CVSS vector, if available (Optional)	

6. Exploitation and Disclosure Status

Field	Response
Is the vulnerability already public?	☐ No ☐ Yes ☐ Unknown If yes, please provide URL and date:
Is a proof of concept public?	☐ No ☐ Yes ☐ Unknown If yes, please provide URL and date:
Is active exploitation known or suspected?	☐ No ☐ Yes ☐ Unknown If yes, please provide details:
Has another vendor, supplier, CERT or coordinator been contacted?	☐ No ☐ Yes ☐ Unknown If yes, please provide party, case ID and date:
Do you plan to discuss or publish the issue after remediation?	☐ No ☐ Yes ☐ Unknown If yes, please provide details:
Preferred coordinated disclosure date, if any	

Coordinated disclosure note:

Please keep non-public vulnerability information confidential until an agreed disclosure date. If the risk changes, active exploitation is observed, or public disclosure becomes likely, please contact security@saluscontrols.com promptly so the disclosure plan can be reassessed.

7. Suggested Remediation or Mitigation (Optional)

- Suggested root-cause fix, if known: _____
- Suggested temporary mitigation or workaround, if known: _____
- Relevant industry practice, defensive rule or reference: _____

8. Acknowledgement Preference

Choice	Response
May we publicly acknowledge you if an advisory is published?	☐ Yes ☐ No
Display name, alias or organisation	
Preferred profile or reference link, if accepted by policy	

9. Attachments and Additional Information

Please list any files included with your report. Do not include passwords, authentication tokens, private keys or unnecessary personal/customer data.

Field	Response
Are files attached to this report?	☐ Yes ☐ No
Type of files attached	☐ Screenshots ☐ Logs ☐ Video ☐ Proof of concept ☐ Packet capture ☐ Other
Description of attached files	
Additional information relevant to the report	
Confidentiality or handling requirements	

If you include logs, screenshots, videos, packet captures or proof-of-concept material, please remove unnecessary personal data, customer data, passwords, authentication tokens, private keys or other sensitive information before submitting the report.

10. Good-Faith Confirmation

By submitting this report, the reporting party confirms, to the best of their knowledge, that:

- ☐ The report is accurate and was obtained through good-faith security research.
- ☐ Testing was limited to systems, devices, accounts and data the reporting party owns or was authorised to test.
- ☐ Unnecessary access to, retention of or disclosure of non-public data was avoided.
- ☐ The reporting party will coordinate disclosure in accordance with the published policy, subject to applicable law and any urgent change in user risk.
- ☐ I confirm that I have not intentionally included passwords, authentication tokens, private keys or unnecessary personal/customer data.

Submission date: _____

Reporter name or alias, if provided: _____

How to submit this report

Please email the completed form to: **security@saluscontrols.com**

You may also report a suspected vulnerability directly by email without using this form. Use of this form is recommended because it helps SALUS Controls PLC collect the information needed to assess the report efficiently.