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

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**.

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.