SENTECH Instruments GmbH

Schwarzschildstr. 2
12489 Berlin, Germany
+49 30 6392-5520
info@sentech.de
www.sentech.de

Responsible Vulnerability Disclosure Policy

1. Purpose

SENTECH is committed to the security, reliability and integrity of its products and services. We recognise that independent security researchers, customers and partners play an important role in helping identify potential cybersecurity vulnerabilities.
This Responsible Vulnerability Disclosure Policy explains how to report suspected security vulnerabilities affecting SENTECH products and how we manage such reports.

2. Scope

This policy applies to cybersecurity vulnerabilities that may affect SENTECH products, including but not limited to:

- Product software
- Firmware
- Embedded control systems
- Network-connected components
- Associated desktop applications
- Product communication interfaces

This policy does not apply to:

- General technical support requests
- Product feature requests
- Equipment configuration or process optimisation
- Product documentation corrections
- Third-party products that are not supplied by SENTECH

3. Reporting a Vulnerability

If you believe you have identified a security vulnerability affecting a SENTECH product, please report it as soon as possible using our Cybersecurity Contact Form or by contacting our Product Security Team at security@sentech.de

To help us investigate efficiently, please include where possible:

- Your name and organisation
- Contact details
- Product name and model
- Software or firmware version
- Serial number (where applicable)
- Description of the vulnerability
- Steps required to reproduce the issue
- Potential impact
- Any proof-of-concept material or supporting documentation
- Log files or screenshots, where appropriate

Reports should contain sufficient information to enable us to reproduce and verify the issue.

4. Our Commitment

Upon receiving a vulnerability report, SENTECH will:

- Acknowledge receipt of the report.
- Assess the information provided.
- Validate whether the reported issue represents a genuine security vulnerability.

SENTECH Instruments GmbH • Geschäftsführer: Dr. Marcel Schulze, Friedrich P. Witek •
Amtsgericht Charlottenburg HRB 33353

SENTECH Instruments GmbH

Schwarzschildstr. 2
12489 Berlin, Germany
+49 30 6392-5520
info@sentech.de
www.sentech.de

- Investigate the potential impact.
- Determine appropriate mitigation measures.
- Develop and validate corrective actions where necessary.
- Communicate with the reporter during the investigation where additional information is required.

Where appropriate, SENTECH may issue software updates, firmware updates, security advisories or other corrective measures.

5. Coordinated Disclosure

We request that reporters do not publicly disclose details of a vulnerability until SENTECH has had a reasonable opportunity to investigate the issue and, where appropriate, develop and release corrective measures.

Coordinated disclosure helps reduce the risk of exploitation before customers can implement mitigations. SENTECH values constructive collaboration with the cybersecurity community and will work in good faith with reporters throughout the disclosure process.

6. Good Faith Research

SENTECH supports responsible security research conducted in good faith.

Researchers are requested to:

- Avoid actions that could negatively affect customers or production systems.
- Avoid accessing, modifying or deleting customer data.
- Avoid interrupting product operation.
- Avoid exploiting vulnerabilities beyond what is reasonably necessary to demonstrate their existence.
- Comply with all applicable laws and regulations.

7. Out of Scope

The following activities are generally considered outside the scope of this policy:

- Social engineering attacks
- Physical attacks against facilities or personnel
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) testing
- Spam or phishing campaigns
- Vulnerabilities affecting third-party software outside SENTECH's control
- Reports based solely on outdated software versions that are no longer supported
- Automated vulnerability scan reports without evidence of a specific security issue

8. Security Updates

Where vulnerabilities require corrective action, SENTECH will assess the appropriate remediation strategy based on the severity, product lifecycle and potential customer impact.
Corrective actions may include:

- Software updates
- Firmware updates
- Security patches
- Configuration guidance
- Temporary mitigations
- Security advisories

SENTECH Instruments GmbH • Geschäftsführer: Dr. Marcel Schulze, Friedrich P. Witek •
Amtsgericht Charlottenburg HRB 33353

SENTECH Instruments GmbH

Schwarzschildstr. 2
12489 Berlin, Germany
+49 30 6392-5520
info@sentech.de
www.sentech.de

Customers are encouraged to maintain supported software versions and install recommended security updates promptly.

9. Confidentiality

Information provided through the vulnerability reporting process will be treated confidentially and used solely for investigating and resolving reported cybersecurity issues.
Personal information will be processed in accordance with applicable data protection legislation.

10. Legal Notice

This policy does not create any contractual obligations or guarantee that every reported issue will result in a software update or public advisory.
SENTECH reserves the right to determine the severity, priority and remediation approach for reported vulnerabilities based on technical assessment and product lifecycle considerations.

11. Contact

Cybersecurity reports should be submitted using the SENTECH Cybersecurity Contact Form or sent to the designated Product Security contact at security@sentech.de
Please do not use this reporting channel for technical support or service requests. General product support enquiries should be directed through the standard SENTECH support channels.

SENTECH Instruments GmbH • Geschäftsführer: Dr. Marcel Schulze, Friedrich P. Witek •
Amtsgericht Charlottenburg HRB 33353