SENTECH Instruments GmbH

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

Product Security Policy

1. Purpose

SENTECH is committed to developing and maintaining products that meet high standards of quality, reliability and cybersecurity. As our plasma processing and thin-film metrology systems become increasingly connected within laboratory, research and manufacturing environments, cybersecurity is an integral part of product design, development and lifecycle management.
This Product Security Policy outlines SENTECH's approach to protecting the confidentiality, integrity and availability of its products and supporting customers in maintaining secure operating environments.

2. Scope

This policy applies to SENTECH products containing software, firmware or network-enabled functionality, including associated applications and communication interfaces supplied by SENTECH.
The policy covers cybersecurity throughout the supported product lifecycle.

3. Security by Design

Cybersecurity considerations are incorporated throughout the product development process. During system design and implementation, SENTECH seeks to identify and reduce cybersecurity risks using recognised engineering practices.

Product development activities may include:

- Security-focused system design
- Risk assessment and threat analysis
- Secure software development practices
- Security testing and verification
- Validation before software and firmware release
- Ongoing review of identified vulnerabilities

Security requirements are considered alongside product safety, reliability and performance throughout development.

4. Vulnerability Management

SENTECH maintains processes for identifying, assessing and managing cybersecurity vulnerabilities that may affect its products.
Potential vulnerabilities may be identified through:

- Internal testing and validation
- Customer feedback
- Security researchers
- Suppliers and technology partners
- Public vulnerability databases
- Industry cybersecurity notifications

Each reported issue is evaluated to determine its technical validity, potential impact and appropriate remediation.

5. Security Updates and Patch Management

Where cybersecurity vulnerabilities require corrective action, SENTECH evaluates appropriate mitigation measures based on the nature and severity of the issue.

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

Corrective actions may include:

- Software updates
- Firmware updates
- Security patches
- Configuration recommendations
- Temporary mitigation guidance
- Security advisories

Security updates are validated before release to help ensure compatibility with supported product configurations.

SENTECH provides security updates and vulnerability remediation throughout the applicable support period. In accordance with the EU Cyber Resilience Act (CRA), the support period is determined taking into account the expected lifetime and intended use of the product and will generally be at least five years. Where the expected lifetime of a product exceeds five years, an appropriate longer support period may apply.

Customers are encouraged to install recommended updates and maintain supported software versions whenever practical.

6. Incident Response

SENTECH maintains procedures for receiving, investigating and managing reports of cybersecurity vulnerabilities and security incidents.

Reported issues are reviewed by appropriate technical specialists who assess:
The nature of the reported issue

- Potential impact on product security
- Possible customer impact
- Required corrective actions
- Communication requirements

Where appropriate, customers will be informed of relevant security updates or recommended mitigation measures.

7. Responsible Vulnerability Disclosure

SENTECH encourages customers, researchers and partners to report suspected cybersecurity vulnerabilities responsibly.

Reports should be submitted using the SENTECH Cybersecurity Contact Form or through the designated Product Security contact at security@sentech.de

SENTECH supports coordinated vulnerability disclosure and requests that security researchers refrain from public disclosure until a reasonable opportunity has been provided to investigate and address the reported issue.

Further information is available in the SENTECH **Responsible Vulnerability Disclosure Policy.**

8. Customer Responsibilities

Cybersecurity is a shared responsibility between SENTECH and its customers.

SENTECH Instruments GmbH

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

Customers are encouraged to:

- Install security updates provided by SENTECH.
- Operate products using supported software and firmware versions.
- Restrict access to authorised users.
- Protect user credentials and administrative accounts.
- Integrate products into appropriately secured network environments.
- Follow applicable organisational cybersecurity policies and procedures.
- Report suspected cybersecurity issues promptly.

9. Third-Party Components

Where products incorporate third-party software or hardware components, SENTECH monitors relevant cybersecurity information and evaluates the potential impact of newly identified vulnerabilities on supported products.

Where necessary, appropriate mitigation measures or updates will be implemented.

10. Product Lifecycle Support

Cybersecurity is considered throughout the supported lifecycle of SENTECH products.
As products evolve, SENTECH reviews relevant cybersecurity risks and, where appropriate, provides software maintenance, firmware updates or security guidance to support customers operating supported systems.

Support availability may vary depending on product generation, software version and lifecycle status.

11. Compliance

SENTECH continuously reviews its cybersecurity processes in line with applicable legislation, recognised industry practices and customer requirements.
This includes ongoing consideration of relevant standards, regulatory obligations and product security requirements applicable to connected industrial equipment.

12. Contact

Questions regarding product cybersecurity or the reporting of suspected vulnerabilities may be submitted through the SENTECH Cybersecurity Contact Form or by contacting the designated Product Security contact at security@sentech.de.

Technical support enquiries, service requests and application-related questions should continue to be directed through the standard SENTECH support channels.

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