
CVD Policy

Coordinated Vulnerability Disclosure Policy
of SensoTech GmbH

Version 1.0 · As of September 2026

Contents

Contents.....	2
1. Purpose	3
2. Scope.....	3
3. Reporting Security Vulnerabilities.....	3
4. Information to Include in a Report.....	3
5. Response Times.....	4
6. Safe Harbor	4
7. Coordinated Disclosure.....	4
8. Closing a Vulnerability Report.....	5
9. Vulnerability Assessment.....	5
10. Handling Confirmed Vulnerabilities.....	5
11. Recognition of Security Researchers	5
12. Data Protection	5
13. Point of Contact	5

1. Purpose

SensoTech GmbH is committed to developing, providing and maintaining its products and services securely.

This Coordinated Vulnerability Disclosure Policy (CVD Policy) describes the process for reporting, assessing, addressing and disclosing security vulnerabilities in products, software, firmware and digital services provided by SensoTech GmbH.

The policy supports the vulnerability management requirements of the Cyber Resilience Act (EU) 2024/2847 and promotes responsible cooperation with security researchers, customers, integrators and partners.

2. Scope

This policy applies to:

- LiquiSonic® measurement systems
- LiquiSonic® controllers
- LiquiSonic® sensors
- Mobile applications
- Software tools and configuration programs provided by SensoTech
- Future digital products with network or data communication capabilities

The following are outside the scope of this policy:

- General product defects unrelated to security
- Service and support requests
- Complaints or warranty claims

Note:

This policy does not authorize security testing of systems or infrastructure belonging to customers or other third parties. Testing may be carried out only on your own systems or with the express permission of the respective owner.

3. Reporting Security Vulnerabilities

Security researchers, customers and partners are asked to report potential vulnerabilities responsibly.

Contact

Email: security@sensotech.com

Subject: Security Vulnerability Report

4. Information to Include in a Report

A vulnerability report should include, where possible:

- Name of the affected product
- Software or firmware version
- Description of the vulnerability and the conditions required to exploit it
- Impact on availability, integrity or confidentiality
- Steps to reproduce the issue
- Proof of concept, if available
- Screenshots or log files
- Time and circumstances of discovery
- Contact details of the person submitting the report

Anonymous reports are also accepted.

5. Response Times

SensoTech aims to meet the following response times:

Activity	Target timeframe
Acknowledgment of receipt for vulnerability reports	Within 5 working days
Initial substantive assessment	Within 10 working days
Regular status updates	At least monthly
Publication of a security advisory	Risk-based, once suitable protective or remedial measures are available

The actual time required to handle a report may vary depending on its complexity, the availability of countermeasures and the tests required.

These response times relate solely to communication with the person submitting the report. Statutory reporting deadlines, in particular those under Article 14 of the CRA, remain unaffected.

6. Safe Harbor

SensoTech welcomes responsible security research.

Provided the research is conducted in accordance with this policy and does not involve intentional harm or apparent criminal intent, SensoTech will generally not initiate legal action of its own in relation to that security research.

This commitment applies provided the reporting person:

- Acts in good faith;
- Tests only their own systems or systems for which the respective owner has expressly authorized testing;
- Investigates and exploits a vulnerability only to the extent necessary to verify it;
- Does not impair the availability of systems;
- Does not carry out DoS/DDoS, brute-force or social engineering attacks;
- Does not alter or delete data and accesses data only to the extent necessary for verification;
- Does not disclose personal, confidential or otherwise protected data or pass it on to third parties;
- Respects the privacy and rights of third parties;
- Does not adversely affect live customer systems; and
- Allows SensoTech reasonable time to investigate and remedy the vulnerability.

This commitment applies only within the limits of applicable law.

Confidentiality:

Vulnerability reports are generally treated as confidential. The identity and contact details of the person submitting the report will not be published without their consent, unless required by law.

7. Coordinated Disclosure

SensoTech follows the principle of coordinated disclosure.

Before publishing information about a vulnerability, the reporting person is encouraged to:

- Allow SensoTech sufficient time to analyze it;
- Agree on a publication date together with SensoTech; and
- Refrain from publishing technical details while doing so could put customers at risk.

The aim is to publish information only when suitable risk-mitigation measures are available.

The timing and scope of publication are determined on a risk-based basis. In particular, SensoTech considers the availability of countermeasures, the risk of further exploitation and the protection of affected customers. Statutory notification and reporting obligations remain unaffected.

8. Closing a Vulnerability Report

A CVD case may be closed, in particular, if:

- The report is found to be unfounded or the issue cannot be reproduced;
- The vulnerability has been remedied or adequately mitigated and the necessary information has been provided;
- The reported product is found not to be affected; or
- Further investigation is not possible because the necessary information is unavailable despite reasonable efforts.

Where contact details are available, SensoTech will inform the reporting person when the case is closed.

9. Vulnerability Assessment

Each report is assessed in particular against the following criteria:

- Whether SensoTech products and product versions are actually affected
- Impact on availability, authenticity, integrity and confidentiality
- Practical exploitability under realistic operating conditions
- Potential impact on customers and their processes
- Indications of previous or ongoing exploitation
- Availability of mitigation or remediation measures

10. Handling Confirmed Vulnerabilities

If a vulnerability is confirmed, SensoTech may take the following measures:

- Software or firmware updates
- Security advisories
- Configuration changes
- Recommendations for customers
- Product changes
- Coordination with manufacturers or maintainers of affected third-party components

Prioritization is based on risk in accordance with SensoTech's internal vulnerability management process.

11. Recognition of Security Researchers

SensoTech thanks those who help improve the security of its products.

With the reporting person's consent, they may be acknowledged publicly.

12. Data Protection

Personal data is processed only to the extent necessary to handle and coordinate the vulnerability report, communicate with the reporting person and comply with legal obligations.

Processing is carried out in accordance with applicable data protection laws.

13. Point of Contact

SensoTech GmbH

Steinfeldstraße 1

39179 Magdeburg-Barleben

Email: security@sensotech.com



SensoTech GmbH

Steinfeldstraße 1
39179 Magdeburg-Barleben
Germany
+49 39203 281 100
info@sensotech.com
www.sensotech.com

SensoTech Inc.

69 Montgomery Street, Unit 13218
Jersey City, NJ 07303
USA
+1 973 832 4575
sales-usa@sensotech.com
www.sensotech.com

SensoTech (Shanghai) Co., Ltd.

Room 609, Bldg.1, No.778, Jinji Road.
Pilot Free Trade Zone, 201206 Shanghai
China
+86 21 6485 5861
sales-china@sensotech.com
www.sensotechchina.com