Coordinated Vulnerability Disclosure Policy (CVD)

LANTECH Informationstechnik GmbH

63930 Klingenberg am Main / Germany

Version: 1.0
Effective date: 08.09.2026
Last updated: xx.09.2026

1. Purpose

LANTECH Informationstechnik GmbH (“LANTECH”) is committed to the security of its products and to protecting its customers, users, and partners.

This Coordinated Vulnerability Disclosure (CVD) Policy establishes a structured process for security researchers, customers, partners, and other parties to report potential security vulnerabilities affecting LANTECH products.

LANTECH encourages responsible and coordinated disclosure so that reported vulnerabilities can be investigated, assessed, and remediated before detailed information is disclosed publicly.

2. Scope

This policy applies to security vulnerabilities identified in products with digital elements manufactured by LANTECH, including, where applicable:

- hardware products;
- embedded software and firmware;
- product operating systems;
- web-based management interfaces;
- web based applications;
- software tools and applications;
- software supplied with LANTECH products;

Products that have reached the end of their applicable support period may have limited or no security update support. LANTECH will nevertheless assess reports concerning such products and determine appropriate actions based on the associated cybersecurity risk. The meaning of products include hardware and software products.

3. Reporting a Vulnerability

Potential security vulnerabilities should be reported to LANTECH through the following security contact:

Global Security Contact: cra@lantech-group.eu
Security Website: https://www.lantech.eu/cra

Security Files:
https://lantechcom.docsecbox.com/folder-share/QOiVZH8rm081aqvv

Please use the subject line:

Security Vulnerability Report – [Product Name]

To enable LANTECH to investigate the issue efficiently, please provide as much of the following information as possible:

- affected product name and model/version;
- hardware revision, if applicable;
- firmware or software version;
- detailed description of the vulnerability;
- steps required to reproduce the issue;
- potential security impact;
- proof-of-concept information, screenshots, logs, or other relevant evidence;
- known exploitation conditions;
- suggested mitigation or remediation, if available;
- your preferred contact details;
- whether you wish to be publicly acknowledged.

Please do not include sensitive personal information unless it is necessary for the investigation.

4. What You Can Expect from LANTECH

After receiving a vulnerability report, LANTECH will make reasonable efforts to:

1. acknowledge receipt of the report;
2. review the information and determine whether the reported issue can be reproduced;
3. assess the potential cybersecurity impact and severity;
4. communicate with the reporter where additional information is required;
5. develop appropriate remediation or mitigation measures where necessary;
6. make security updates available in accordance with the applicable product support policy;
7. coordinate disclosure of the vulnerability where appropriate; and
8. publish relevant security information or a security advisory when appropriate.

The time required to resolve a vulnerability depends on its complexity, severity, affected products, availability of remediation measures, and the need to coordinate with third-party component suppliers.

5. Coordinated Disclosure

LANTECH asks reporters to allow reasonable time for investigation and remediation before publicly disclosing detailed information about a reported vulnerability.

During the investigation, reporters are requested to:

- keep vulnerability details confidential until coordinated disclosure has taken place;
- avoid publishing exploit code or technical information that could facilitate malicious exploitation before a remediation or mitigation is available;
- avoid accessing, modifying, deleting, or exfiltrating data belonging to other parties;
- avoid actions that could disrupt production systems or services;
- avoid denial-of-service testing against operational systems unless expressly authorized; and
- cooperate with LANTECH in determining an appropriate disclosure timeline.

LANTECH will seek to coordinate disclosure with the reporter and, where relevant, affected suppliers, component manufacturers, maintainers, CSIRTs, or other competent authorities.

6. Vulnerability Assessment and Remediation

Reported vulnerabilities will be evaluated according to their technical characteristics and cybersecurity risk.

Where appropriate, Lantech may use recognized vulnerability assessment methods, including the Common Vulnerability Scoring System (CVSS), to support severity classification.

Depending on the assessment, remediation may include:

- firmware or software updates;
- configuration changes;
- compensating security controls;
- temporary mitigations;
- product documentation updates;
- security advisories; or
- other appropriate corrective measures.

Where a vulnerability affects a third-party component incorporated into a LANTECH product, LANTECH may coordinate with the relevant component manufacturer, supplier, or maintainer.

7. Security Updates and Advisories

Where security updates are provided, Lantech will make appropriate information available to affected users so that they can identify the affected product and take the necessary remediation or mitigation measures.

Security advisories may include, as appropriate:

- affected product models;
- affected firmware or software versions;
- vulnerability description;
- security impact;
- severity assessment;
- CVE identifier, where applicable;
- fixed versions;
- available mitigations or workarounds; and
- instructions for obtaining and installing the security update.

In justified cases, detailed vulnerability information may be withheld temporarily where immediate publication could increase cybersecurity risk before affected users have had a reasonable opportunity to apply the relevant remediation.

8. Responsible Security Research

LANTECH welcomes good-faith security research intended to improve the cybersecurity of its products.

Researchers should conduct their activities responsibly and in accordance with applicable laws and this policy.

Security testing should be limited to systems and products that the researcher owns or for which the researcher has obtained appropriate authorization.

Researchers must not intentionally:

- compromise the privacy or safety of other users;
- access data beyond what is necessary to demonstrate a vulnerability;
- modify or delete third-party data;
- introduce malware;
- disrupt services or operational networks;
- conduct social-engineering attacks against LANTECH employees, customers, or partners; or
- use discovered vulnerabilities for unlawful purposes.

9. Recognition

Where appropriate and with the reporter's consent, LANTECH may acknowledge individuals or organizations that responsibly report valid security vulnerabilities.

Any public acknowledgement will be coordinated with the reporter before publication.

10. Regulatory Reporting

Where required by applicable cybersecurity legislation, LANTECH may report vulnerabilities, incidents, or related information to competent authorities, Computer Security Incident Response Teams (CSIRTs), ENISA, or other designated authorities.

Such regulatory reporting obligations are separate from the coordinated vulnerability disclosure process described in this policy.

11. Contact

Questions regarding this policy or reports of potential vulnerabilities should be directed to:

LANTECH Informationstechnik GmbH
Philipp-Kachel-Str. 42a
63911 Klingenberg / Germany

Global Security Contact: cra@lantech-group.eu
Global Security Website: https://www.lantech.eu/cra

For vulnerability reports, please include sufficient technical information to allow LANTECH to reproduce and assess the reported issue.

12. Policy Updates

LANTECH may update this Coordinated Vulnerability Disclosure Policy periodically to reflect changes in its products, security processes, applicable standards, or legal and regulatory requirements.

The current version of this policy will be made available through LANTECH's security website.