PSIRT & Coordinated Vulnerability Disclosure (CVD) Policy of Maschinenfabrik Berthold HERMLE AG

1. Purpose and objective

HERMLE AG is committed to ensuring a high level of cyber resilience, IT security and product safety throughout the entire life cycle of its machining centres, automation systems and software solutions.
This policy describes the structured approach to dealing with reported security vulnerabilities and supports the requirements of the EU **Cyber Resilience Act (CRA)**.

We welcome collaboration with customers, partners, independent security researchers and institutions in order to identify potential risks at an early stage and resolve them in a sustainable manner.

2. Scope

This policy applies to the following products from HERMLE AG:

- Machining centres and automation systems
- Control-related software, embedded systems and digital services
- Web services and IT systems
- Products and software throughout the entire product life cycle

This does not apply to products for which the support period has expired, products from third-party manufacturers, or systems that fall outside the scope of HERMLE AG's control and responsibility.

3. Principles governing the reporting of a security vulnerability

HERMLE AG adheres to the principle of Responsible / Coordinated Vulnerability Disclosure (CVD):

- Confidentiality of all reported vulnerabilities
- Prompt feedback to the whistleblower
- Objective, transparent communication during analysis and resolution
- Coordinated publication following consultation
- Details will only be published once a fix is available
- No legal action will be taken against whistleblowers who comply with this policy

Public disclosure without prior consultation is not in line with our principles.

4. Roles & responsibilities (PSIRT)

Product-related security vulnerabilities are handled by the Product Security Incident Response Team (PSIRT) of HERMLE AG.

Responsibilities of PSIRT:

- Centralised receipt and assessment of reports
- Risk and impact analysis
- Coordination of internal specialist departments
- Definition and implementation of corrective measures
- Communication with reporting parties, customers and, where applicable, CERTs
- Publication of security advisories

5. Contact details for reporting security vulnerabilities

Please report any product vulnerabilities to:

Email: psirt@hermle.de

Alternatively, you can report the issue via our partner CERT@VDE.
Encrypted communication (e.g. PGP) is provided via CERT@VDE.
Anonymous reports can also be sent to CERT@VDE.

For reports concerning HERMLE AG's web applications and IT systems, please contact our IT security team at: security@hermle.de

Recommended report content

Please provide the following information:

- Affected product / component (machine number, software version(s), HERMLE article number, order number, manufacturer)
- A detailed description of the vulnerability and the steps required to reproduce it. If known, the conditions that must be satisfied for the vulnerability to be exploited
- Proof of Concept, such as a concept script, screenshot or similar (optional)
- If known, the potential consequences (e.g. loss of availability, breach of integrity, compromise of safety)
- If available, documents relating to the security vulnerability (CVE, announcements, release notes, etc.)
- Preferred method of communication for enquiries and updates if required

Only reports written in English or German can be considered.

6. Process flow

When a report has been received, the following will take place:

1. Confirmation of receipt within 3 working days, with the allocation of a unique tracking number
2. Objective and technical assessment of the risk
3. Definition of appropriate measures (e.g. updates, patches, workarounds)
4. Coordinated information for the relevant bodies
5. Coordinated publication if required

Whilst the report is being processed, the PSIRT will keep the reporter regularly informed of the processing status. Unless otherwise agreed, status updates will be provided at least every 14 calendar days

We agree on a reasonable embargo period (usually 90 days), which may be extended on a case-by-case basis depending on the complexity and criticality of the issue.

7. Legal protection for whistleblowers

HERMLE AG undertakes not to take any legal action against whistleblowers acting in good faith, provided that:

- the principles of this policy are observed
- the report is made responsibly and in good faith
- no systems are tampered with or compromised
- no data is published or misused
- no tools or information are passed on to third parties for the purpose of exploitation

8. Remark

Upon request, HERMLE AG will acknowledge the whistleblower's contribution as part of the coordinated publication.

9. Publication of security advisories

HERMLE AG publishes relevant safety information via our coordination partner CERT@VDE

If you have any questions regarding the advisories, please contact our customer service team. Faults

10. Continuous improvement, questions

This policy is reviewed and updated on a regular basis. Any questions regarding this policy can be sent to psirt@hermle.de. Please feel free to contact us with any suggestions on how to improve this policy.

Date: Juli 2026

Maschinenfabrik Berthold HERMLE AG