Vulnerability Disclosure Policy

- July 6, 2026 -

Introduction

Hengstler GmbH, Dynapar and Dover Motion (collectively referred to as "Hengstler-Dynapar") are committed to ensuring the security of our customers by protecting the confidentiality, integrity, and availability of our products and the information they process.
This Vulnerability Disclosure Policy (VDP) provides security researchers with clear guidelines for conducting vulnerability discovery activities directed at Hengstler-Dynapar products and describes our preferences for how discovered vulnerabilities are reported, handled, and disclosed.

The Hengstler-Dynapar Product Security Incident Response Team (PSIRT) is responsible for coordinating the response to product vulnerabilities and security incidents. Hengstler-Dynapar defines a vulnerability as any unintended weakness in a system, product, or service that, when exploited, could affect the confidentiality, integrity, or availability of that system, product, or service. The PSIRT works with customers, suppliers, independent researchers, and government organizations to fulfill its mission.

This policy is aligned with the principles of ISO/IEC 29147 (Vulnerability Disclosure) and ISO/IEC 30111 (Vulnerability Handling Processes) and supports compliance with the EU Cyber Resilience Act (CRA), in particular Annex I, Part II.

We encourage you to contact us to report potential vulnerabilities in our products.

Authorization (Safe Harbor)

If you make a good-faith effort to comply with this policy during your security research, we will:

- consider your research to be authorized,
- work with you to understand and resolve the issue quickly, and
- not recommend or pursue legal action related to your research.

Should legal action be initiated by a third party against you for activities conducted in accordance with this policy, we will make this authorization known.

Good faith requires that you do not abuse data you encounter, do not actively exploit vulnerabilities beyond what is necessary to confirm them, and comply with applicable law.

Guidelines for Researchers

Under this policy, “research” means activities in which you:

- notify us as soon as possible after discovering a real or potential security issue;

- make every effort to avoid privacy violations, degradation of user experience, disruption of production systems, and destruction or manipulation of data;
- only use exploits to the extent necessary to confirm a vulnerability's presence — do not exfiltrate data, establish persistent access, or pivot to other systems;
- give us a reasonable amount of time to resolve the issue before public disclosure;
- do not submit a high volume of low-quality reports.

Once you have established that a vulnerability exists or you encounter any sensitive data (including personally identifiable information, financial information, proprietary information, or trade secrets), you must stop testing, notify us immediately, and not disclose this data to anyone else.

Test methods – Not Authorized

The following test methods are not authorized under this policy:

- Network denial-of-service (DoS / DDoS) tests or any tests that impair access to or damage a system or its data.
- Physical testing (e.g. office access, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing against Hengstler-Dynapar staff, facilities, or partners.

Scope

In Scope

This policy applies to the following systems and services:

This policy applies to the following Hengstler-Dynapar products and systems:

- Industrial hardware products developed and sold by Hengstler-Dynapar, including rotary encoders, counters, printers, relays, and related control or motion-feedback devices.
- Embedded firmware and software running on Hengstler-Dynapar products, including communication stacks, configuration interfaces, and diagnostic or management functions.
- Product communication interfaces such as fieldbus, industrial network, or diagnostic interfaces, where exploitation could affect the confidentiality, integrity, or availability of the product or connected systems.
- Software tools or utilities provided by Hengstler-Dynapar for product configuration, operation, or maintenance.

Vulnerabilities in third-party components are considered in scope only when those components are integrated into Hengstler-Dynapar products and exploitation could impact product security.

Out of Scope

The following are out of scope:

- Products or services not expressly listed above, including unrelated connected services.
- Vulnerabilities in unsupported / end-of-life products.
- Low-risk or purely informational findings with no realistic exploitation path.
- Vulnerabilities in third-party systems outside Hengstler-Dynapar's control; these should be reported to the respective vendor.

The Hengstler-Dynapar PSIRT reserves the right to determine whether a reported issue is within scope and will work with the reporter to gather sufficient information to make an informed decision. Security advisories will not be issued for issues outside PSIRT scope or for issues rated low or informational; such issues may instead be addressed via regular bug-fix releases.
If you are unsure whether a target is in scope, contact us at **PSIRT@hengstler-dynapar.com** before testing.

Reporting a vulnerability

Vulnerabilities can be reported confidentially through the following channels:

- **E-mail (primary channel):** at **ProductSecurity@hengstler-dynapar.com**
- **Web form** in the Security section of the Hengstler-Dynapar OpCos' website — currently under development. Once available, the form will provide an HTTPS-encrypted submission path. Until then, please use e-mail.
- **security.txt** in accordance with RFC 9116, published under `/.well-known/security.txt` on the Hengstler-Dynapar OpCo's websites. The security.txt reflects the contact information defined in this policy and references this document via its *Policy:* field.

Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt within **3 business days**.

PGP-encrypted e-mail is **not yet supported**. For particularly sensitive information, please use the HTTPS web form once available, or contact us at **PSIRT@hengstler-dynapar.com** to arrange a secure channel.

Information submitted under this policy will be used for defensive purposes only — to mitigate or remediate vulnerabilities. We will not share your name or contact information without your express permission. By submitting a vulnerability report, you acknowledge that you have no expectation of payment and that you waive any future pay claims against Hengstler-Dynapar related to your submission.

What we would like to see from you

To help us triage and prioritize submissions effectively, please include — where possible:

- The product name and version, and the affected component or interface.
- The location where the vulnerability was discovered and the potential impact of exploitation.
- A detailed description of the steps needed to reproduce the vulnerability (proof-of-concept scripts or screenshots are very helpful).
- Your assessment of severity and any known mitigations.
- Reports in English, where possible.

Incomplete reports will still be considered.

What you can expect from us

When you share your contact information, we commit to coordinating with you as openly and quickly as possible.

1. **Acknowledgement** of receipt within 3 business days.
2. **Triage and technical** validation of the report.
3. **Risk assessment** considering confidentiality, integrity, availability, and any safety-related impact.
4. **Remediation planning** — software update, firmware update, configuration guidance, or mitigation / workaround.
5. **Coordinated disclosure timing**, agreed with the reporter.

We will be as transparent as reasonably possible about progress, including issues or challenges that may delay resolution, and we will maintain an open dialogue throughout.

Public disclosure follows these principles:

- **Confidentiality before disclosure** — vulnerabilities are not made public initially.
- **Coordination, not confrontation** — disclosure timing is agreed with the reporter.
- **Remediation before publication** — technical details are published only after appropriate mitigations are available, or after a jointly agreed deadline if full remediation is not feasible in the short term.
- **Proportionality** — response times and disclosure timing are based on severity, exploitability, and customer impact.

We aim to notify customers and the public simultaneously.

Public Disclosure and Security Advisories

After remediation of a confirmed vulnerability, Hengstler-Dynapar may - where appropriate - publish:

- a Security Advisory identifying affected products and versions,
- a description of the vulnerability at an appropriate level of abstraction,
- recommended updates or mitigations,
- a CVE identifier, where useful or required.

Confidentiality and Legal Reporting Obligations

Hengstler-Dynapar will:

- treat all reports confidentially,
- use any personal data only for the purpose of handling the report, and
- refrain from legal action against reporters acting in good faith under this policy.

Independently of this policy, Hengstler-Dynapar fulfills its statutory reporting obligations, in particular under the **EU Cyber Resilience Act (CRA)** — including notification of actively exploited vulnerabilities and severe incidents to the competent authorities (e.g. **ENISA** and the relevant **national CSIRT**, such as the German BSI / CERT-Bund). Where findings affect users beyond Hengstler-Dynapar, we may additionally coordinate with bodies such as **CISA** under their coordinated vulnerability disclosure process. Fulfillment of legal obligations may require disclosure of relevant information to competent authorities.

Lifecycle, End-of-Support and Cessation of Operations

Hengstler-Dynapar manages vulnerability handling across the full supported lifecycle of each product. End-of-support dates are communicated in advance through the channels used to reach users (vendor security page, customer portal, and direct notice to known B2B customers).

For the duration of the support period, security updates remain available for retrieval for at least ten years after issuance, in line with EU Cyber Resilience Act requirements.

In the event that Hengstler-Dynapar ceases operations for a product, product line, or as a legal entity, and can therefore no longer fulfil its obligations under the EU Cyber Resilience Act, we will:

- notify the relevant market surveillance authorities of the cessation;
- inform affected users through the channels used for security communications, where appropriate; and

- where possible, transfer responsibility for ongoing vulnerability handling and security updates to a successor entity, upstream maintainer, or designated third party, and document the hand-off.

Security advisories, SBOM artifacts, and CSAF documents already published will remain available in their archived form, subject to operational feasibility.

Contact

Hengstler-Dynapar - Product Security (PSIRT) E-mail: PSIRT@hengstler-dynapar.com

Questions or suggestions for improving this policy are welcome at the same address.

Document change history

Version	Date	Description
1.0	July 06 2026	First issuance

Reference:
https://www.cisa.gov/vulnerability-disclosure-policy-template