

Vulnerability Disclosure Policy For Reporters

Reporters MUST adhere to the following guidelines.

In this document, Hengstler GmbH, Dynapar and Dover Motion are collectively referred to as "Hengstler-Dynapar".

1. General

- Reporters MUST comply with all applicable jurisdiction laws in connection with security research activities or other participation in this vulnerability disclosure program.
- Reporters MUST comply with all of Hengstler-Dynapar's terms of use.
- Reporters SHOULD make a good faith effort to notify and work directly with the affected vendor(s) or service providers prior to publicly disclosing vulnerability reports.

2. Scope of Authorized Testing

- Reporters MAY ONLY test Hengstler-Dynapar hardware and software sold to customers with the explicit written permission of that customer ("Authorized Equipment"), to detect a vulnerability for the sole purpose of providing Hengstler-Dynapar information about that vulnerability. "Authorized Equipment" does not include the Hengstler-Dynapar web sites and properties.
- Reporters SHOULD only test against test accounts owned by the Reporter or with explicit written permission from the account holder if they abide by the Terms of Service for that account.
- Reporters MUST avoid any harm to Hengstler-Dynapar's information systems, products, and customers.
- Reporters SHOULD contact Hengstler-Dynapar at psirt@hengstler-dynapar.com if at any point you are uncertain of whether to proceed with testing

3. Coordination with Hengstler-Dynapar

- Reporters SHOULD submit vulnerability reports, including any websites and properties to Hengstler-Dynapar via the Security section of the Hengstler-Dynapar website — currently under development. Once available, the form will provide an HTTPS-encrypted submission path. Until then, please use ProductSecurity@hengstler-dynapar.com.



- Reporters SHOULD submit high-quality reports that contain sufficient descriptive details to permit Hengstler-Dynapar to reproduce the vulnerable behavior accurately.
- Reporters SHOULD NOT report unanalyzed crash dumps or fuzzer output unless accompanied by a sufficiently detailed explanation of how they represent a security vulnerability.
- Reporters MAY include a proof-of-concept exploit if available.
- Reporters MAY request that their contact information be withheld from any affected vendor(s) outside of Hengstler-Dynapar.
- Reporters MAY request not to be named in the acknowledgments of Hengstler-Dynapar's public disclosures.
- Reporters MUST NOT require Hengstler-Dynapar to enter a customer relationship, non-disclosure agreement (NDA) or any other contractual or financial obligation as a condition of receiving or coordinating vulnerability reports.
- Hengstler-Dynapar SHALL confirm receipt of the vulnerability report with the Reporter.
- Hengstler-Dynapar MAY investigate the vulnerability report and inform the reporter through the means defined in the report submission.
- Hengstler-Dynapar MAY contact the vulnerability reporter for more information if Hengstler-Dynapar cannot validate the reported vulnerability.
- Hengstler-Dynapar MAY communicate with the vulnerability reporter on the mitigation status
- Hengstler-Dynapar MAY communicate with the vulnerability reporter when a mitigation has been validated and when it will be released to Hengstler-Dynapar customers.
- Hengstler-Dynapar MAY attribute the vulnerability reporter in any security advisories Hengstler-Dynapar publishes about the vulnerability the reporter discovered. The vulnerability reporter will have the option to opt-out of being attributed, at reporter's discretion

4. Coordination with vendors

- In the event that the Reporter finds a vulnerability in a Hengstler-Dynapar hardware or software product due to a vulnerability in a generally available product or service, the Reporter MAY report the vulnerability to the affected vendor(s), service provider(s), or third-party vulnerability coordination service(s) to enable the product or service to be fixed

5. Coordination with others

- Reporters SHOULD NOT disclose any details of any Hengstler-Dynapar hardware or software vulnerability or any indicators of vulnerability to any third party

6. Public disclosure

- Reporters MAY disclose to the public the prior existence of vulnerabilities already fixed by Hengstler-Dynapar, including potential details of the vulnerability, indicators of vulnerability, or the nature (but not the specific content) of information rendered available by the vulnerability.
- Reporters choosing to disclose to the public SHOULD do so in prior consultation with Hengstler-Dynapar.
- Reporters MUST NOT disclose any incidental proprietary data revealed during testing.

7. Document change history

Version	Date	Description
1.0	July 06 2026	First issuance.