Cybersecurity Vulnerability Reporting Policy

V1.00

Purpose. This policy defines how our Invertek Drives receives, analyses, handles, and discloses security vulnerabilities in our products. The process follows a four-stage approach aligned with principles from ISO/IEC 29147 and 30111 and mirrors widely adopted practices in industry.

Reporting

How to report an incident:

- Email our Product Security Incident Response Team (PSIRT)
- **Email Address:** IDL.cybersecurity@shi-g.com
- If possible, please encrypt with our PSIRT PGP key published on our key on a Cybersecurity page
- Web form (recommended for attachments)
- **Address:** Offa's Dyke Business Park, Welshpool, Powys, SY21 8JF, United Kingdom

What to include:

- Affected product including model code and serial number where appropriate
- Firmware Version
- environment/configuration
- reproduction steps
- impact and plausible attacker path
- proof of concept (if available)
- any mitigations you suggest
- your preferred credit name (or state if you prefer anonymity)

Acknowledgement & communications:

- We aim to **acknowledge within two (2) business days** and provide **periodic updates** (at least every 14 days) until closure
- Anonymous reports are accepted; however, we may be unable to provide status updates

Invertek Drives Limited
Offa's Dyke Business Park, Welshpool, Powys, UK, SY21 8JF
Tel: +44 (0)1938 556868 | **Fax:** +44 (0)1938 556869 | **Email:** sales@invertekdrives.com
Registered in England No. 3504834 VAT Number GB 712854929

Research conduct:

- Please avoid privacy violations, service degradation, or accessing more data than is necessary to demonstrate the issue

Safe harbour:

- Acting in good faith and in accordance with this policy means we will not pursue legal action related to your security research and reporting.

Analysis

Validation & triage:

- PSIRT will attempt to **reproduce** the issue, determine **root cause**, and **assess risk** using an industry scoring system such as CVSS
- We may contact you for additional details or artifacts during analysis

Severity & impact:

- We will evaluate exploitability, affected versions, and potential impact on confidentiality, integrity, and availability

Handling (Remediation)

Fix & mitigation strategy:

- For confirmed vulnerabilities, we prioritize **remediations** based on severity and potential customer impact
- where fixes are not immediately feasible (e.g., in end of life products), we will publish **mitigations** or **upgrade guidance**

Coordination:

- We coordinate internally across engineering and support to verify and test patches or configuration guidance before public release, following CVD principles

Customer readiness:

- To reduce risk, we may time patch availability and communication so customers can plan deployment

Invertek Drives Limited

Offa's Dyke Business Park, Welshpool, Powys, UK, SY21 8JF

Tel: +44 (0)1938 556868 | **Fax:** +44 (0)1938 556869 | **Email:** sales@invertekdrives.com

Registered in England No. 3504834 VAT Number GB 712854929

Disclosure

Advisory publication:

- When a fix or meaningful mitigations are ready, we will publish a **Security Advisory** detailing affected versions, impact, remediation steps, and **acknowledgements** (if you opt in)

Timing:

- We favour **coordinated disclosure**—publishing after remediation or by mutual agreement on a timeline. If necessary to minimize risk, we may **delay advisory publication briefly** to allow patch rollout

Where advisories live:

- We will maintain a **Security Advisories** page and provide subscription options

Recognition:

- With your consent, we will credit reporters (e.g., on a "Hall of Thanks" page)

Supporting Policies & Notes

Scope and out of scope examples:

- In scope: Our owned/operated products, and software platforms that we actively support
- Out of scope: Social engineering, physical attacks, denial of service testing, spam, reports without actionable detail, and issues in end of life offers where only mitigations may be possible

Security.txt & PGP:

- We will publish a **.well-known/security.txt** file with our contact, PGP key, policy link, and acknowledgment page to make reporting easier for researchers and automation

Standards alignment:

- Our workflow aligns to **ISO/IEC 29147** (vulnerability disclosure) and **ISO/IEC 30111** (vulnerability handling)

Invertek Drives Limited
Offa's Dyke Business Park, Welshpool, Powys, UK, SY21 8JF
Tel: +44 (0)1938 556868 | **Fax:** +44 (0)1938 556869 | **Email:** sales@invertekdrives.com
Registered in England No. 3504834 VAT Number GB 712854929

Incident Reporting

Reporting of any incidents of actively exploited vulnerabilities contained within our products will be reported to the CSIRT and ENISA through Invertek Drives' Authorised European Representative:

Invertek Drives Iberica S.L.U
C/ Fondo
25 Nave 14
P.I.Can Coll -08185 Lliçà de Vall-
Barcelona

Reporting Steps:

- 24 Hours: Early warning report after becoming aware of an incident or vulnerability
- 72 Hours: Detailed follow-up notification
- 14 Days (Vulnerability): Final report after a corrective measure (patch/fix) is available
- 1 Month (Incident): Final report for severe incidents
- User Notification: Manufacturers must also inform users "in a timely manner" about vulnerabilities and provide mitigation measures

Invertek Drives Limited
Offa's Dyke Business Park, Welshpool, Powys, UK, SY21 8JF
Tel: +44 (0)1938 556868 | **Fax:** +44 (0)1938 556869 | **Email:** sales@invertekdrives.com
Registered in England No. 3504834 VAT Number GB 712854929