Coordinated Vulnerability Disclosure Policy

1. Purpose

This Coordinated Vulnerability Disclosure (CVD) Policy provides a clear process for customers, distributors, security researchers and other parties to report suspected cybersecurity vulnerabilities affecting our products and associated services.

For the purposes of this policy, a cybersecurity vulnerability is a weakness, susceptibility or flaw in a product, software, firmware or associated digital service that could be exploited by a cyber threat and compromise its security. Examples may include weaknesses that could allow unauthorised access, disclosure or modification of data, disruption of normal operation, or other unintended or unauthorised behaviour.

We encourage responsible reporting so that potential vulnerabilities can be investigated and, where necessary, appropriate corrective or mitigating action can be taken.

2. Scope

This policy applies to cybersecurity vulnerabilities affecting products and services supplied or operated by Trumeter, including, where applicable:

- industrial control and automation products;
- connected hardware and embedded devices;
- firmware and software;
- industrial IoT products and interfaces;
- associated configuration and management software;
- industrial cloud services; and
- software components supplied as part of our products or services.

This policy is intended for genuine cybersecurity vulnerability reports. General technical support, product faults, service requests and commercial enquiries should continue to be submitted through our normal customer support channels.

3. Reporting a vulnerability

If you believe you have identified a cybersecurity vulnerability affecting one of our products or services, please report it to: security@trumeter.com. Where possible, please provide:

- your name and contact details;
- the affected product or service;
- product model or part number;
- firmware or software version;
- a description of the suspected vulnerability;
- the steps required to reproduce the issue;
- details of the potential security impact;
- relevant logs, screenshots or diagnostic information; and
- any proof-of-concept information that may assist our investigation.

Please provide as much information as possible to help us to understand and reproduce the issue.

4. What you can expect from us

When we receive a vulnerability report, we will:

1. acknowledge receipt of the report;
2. review the information provided;
3. assess whether the reported issue represents a cybersecurity vulnerability;
4. investigate the affected product or service;
5. assess the potential impact and risk;
6. develop corrective or mitigating measures where appropriate; and
7. communicate relevant information to affected parties where necessary.

Where possible, we will maintain communication with the person who reported the vulnerability during our investigation. The time required to investigate and remediate a vulnerability will depend on its complexity, severity, affected products and the availability of appropriate corrective measures.

5. Coordinated Disclosure

We ask reporters to allow us a reasonable timeframe to investigate and address a suspected vulnerability before publicly disclosing technical information that could increase the risk to customers or users.
Where public disclosure is appropriate, we encourage reporters to coordinate the timing and content of disclosure with us.
We may publish security advisories or other information where this is necessary to inform customers about an affected product, associated risks, available updates, mitigating measures or actions customers should take.

6. Responsible Security Research

We ask anyone investigating our products or services to act responsibly and in good faith. In particular, please:

- avoid accessing, modifying or deleting data belonging to other parties;
- avoid actions that could disrupt operational systems or services;
- avoid actions that could create a risk to health, safety, the environment or industrial processes;
- minimise access to confidential, personal or commercially sensitive information;
- do not use a vulnerability for extortion, financial gain or other malicious purposes; and
- report identified vulnerabilities to us promptly.

Because many of our products are used in industrial and operational technology environments, testing should not be performed on live operational systems where doing so could affect equipment, processes, safety or availability. Where practical, testing should be performed in an isolated or appropriately controlled environment.

7. Vulnerabilities Affecting Third-Party Components

Our products may incorporate hardware, software, open-source software or other components supplied or maintained by third parties.
Where a reported vulnerability relates to a third-party component, we may coordinate with the relevant supplier, maintainer or other affected parties as part of the investigation and remediation process.
We ask reporters not to contact multiple affected parties independently where doing so could result in premature disclosure or increase security risk without first discussing an appropriate coordinated approach with us.

8. Regulatory Reporting

We assess reported vulnerabilities and cybersecurity incidents against applicable legal and regulatory requirements. Where a vulnerability or incident meets applicable regulatory reporting criteria, we will make the necessary notifications to the appropriate authorities in accordance with the relevant requirements and reporting timescales. This includes, where applicable, reporting obligations under Regulation (EU) 2024/2847 (Cyber Resilience Act).

9. Security Updates and Advisories

Where appropriate, we will provide:

- firmware or software security updates;
- patches;
- configuration changes;
- temporary mitigating measures;
- product security advisories; or
- other instructions intended to reduce cybersecurity risk.

Customers should ensure that they maintain appropriate contact details with us or their authorised distributor and review relevant product security communications.

10. Confidentiality

Information provided to us in connection with a vulnerability report will be handled appropriately and shared internally or with relevant third parties only where necessary to investigate, remediate, coordinate or meet legal and regulatory obligations. We will take reasonable steps to protect the identity and contact information of vulnerability reporters where requested and legally permissible.

11. Recognition

Where appropriate and with the reporter's agreement, we may acknowledge individuals or organisations that responsibly report significant vulnerabilities.

12. Contact

Cybersecurity vulnerabilities should be reported to: security@trumeter.com
For normal technical support, product faults or service requests that do not involve a suspected cybersecurity vulnerability, please use our standard customer support channels.

13. Policy Review

This policy will be reviewed periodically and updated where necessary to reflect changes to our products, services, applicable cybersecurity requirements and vulnerability disclosure practices.

Gil Copitch
Chief Executive Officer

4th September 2026