CVD (Coordinated Vulnerability Disclosure)-Policy

1. Introduction and Scope

At **VEGA**, the safety of our products with digital elements is paramount. This policy describes how you can report any potential vulnerabilities in our products and how we will handle your report. We welcome reports from security researchers, customers, partners and the general public.

Scope: This policy applies to the following products and services:

- All VEGA equipment with the following equipment names: “VEGA…”
- PROTRAC series (MINITRAC, PIONTRAC, WEIGHTRAC, FIBERTRAC, SOLITRAC)
- PLICSCOM
- PLICSMOBILE
- VEGA Tools app
- VEGA Inventory System
- VEGA DTM Collection
- VEGA DataViewer

The following are excluded from the scope: VEGA products and services that have been officially declared end-of-life.

2. Contact options for reporting

You can reach our security team via the following channels:

- E-mail: psirt@vega.com
- Phone: +49 7836 50-0

3. Content of a vulnerability report

Please provide the following information so that we can process your report as quickly as possible:

- Name of the affected product*
- Version (e.g. hardware version, software version, tool version)
- Environment (e.g. combination with other VEGA equipment, operating system)
- Description of the vulnerability and possible impact*
- Steps for replication

*Required information

4. Process and ongoing communication

Once we have received your report, we will proceed as follows:

1. Confirmation of receipt within 2 working days and assignment of a unique tracking number.
2. Review and verification of the reported vulnerability.
3. Status updates every 20 days.
4. Fixing the vulnerability and publication in accordance with the sections on *disclosure strategy and embargo*, and *publication*.

5. Secure and anonymous communication

Vulnerability information is sensitive. Should you wish to encrypt your message, you can do this via CERT@VDE. We accept all reports even if a secure channel cannot be used.

Please always enter valid contact details (e.g. e-mail address) so that we can contact you in the event of any queries. We promise to treat every vulnerability report confidentially in accordance with applicable laws. Personal data will not be passed on to third parties without your express consent.

Anonymous report: You can also make a report anonymously.

6. Disclosure strategy and embargo

We follow the principle of coordinated disclosure: Details will not be published until a fix is available. We agree on an appropriate embargo period (typically 90 days), which can be adjusted on a case-by-case basis depending on the complexity and criticality.

7. Publication

After the vulnerability has been fixed, we will publish a security advisory. You can find our published advisories on the CERT@VDE advisory portal: https://certvde.com/de/advisories/vendor/vega/

We do **not** operate a bug-bounty program.

8. Legal framework

We expect that you have not exploited the vulnerability you have found and that you have not attacked, tampered with, compromised or altered VEGA products or VEGA tools.

We promise not to take any criminal action against you as long as you have complied with the policy and principles. This does not apply in cases where criminal intent was or is evident.