Coordinated Vulnerability Disclosure (CVD) Policy

Version: August 2026

1. Purpose

The Pütz Group places great importance on the security of its products, systems and services. This Coordinated Vulnerability Disclosure Policy describes the process for handling security vulnerabilities within the companies of the Pütz Group. It is intended to provide all users of our products and solutions with the information they need to prepare for potential cybersecurity issues or vulnerabilities discovered in our products.

Our goal is to work together with those reporting vulnerabilities to analyze identified vulnerabilities, assess the associated risks and develop appropriate measures to remediate or mitigate them before security-relevant information is disclosed.

2. Legal Requirements

This vulnerability handling process complies with the requirements of the EU Cyber Resilience Act (CRA).

3. Scope

This Policy applies to products, software and services of the Pütz Group, including in particular:

- Pütz Group software products
- Industrial PCs, embedded systems and edge devices
- Process automation solutions
- Visualization systems (HMI)
- SCADA and control system components
- Communication solutions and gateways
- Remote service and remote maintenance solutions
- Pütz Group cloud services and web applications
- Pütz Group mobile applications

The following are outside the scope of this Policy:

- Products from other manufacturers
- Customer-specific networks or system configurations
- Systems that have been modified by customers or integrators and whose behavior no longer corresponds to the condition in which they were originally delivered

4. Reporting a Security Vulnerability

Security vulnerabilities can be reported at any time to: **E-Mail: security@puetzgroup.de**

Please provide the following information whenever possible:

- Name of the affected product
- Software or firmware version
- Description of the vulnerability
- Prerequisites for exploitation
- Step-by-step instructions for reproducing the vulnerability
- Proof of Concept (PoC), if available
- Assessment of the potential impact
- Contact details for follow-up questions

If confidential information is being transmitted, we recommend using encrypted communication.

5. Handling of Vulnerability Reports

Upon receipt of a vulnerability report, the following process is followed:

Step:	**Ziel:**
Acknowledgement of receipt	within 5 business days
Initial technical assessment	within 10 business days
Feedback on next steps	as soon as the evaluation is complete
Development of countermeasures	depending on criticality and complexity
Publication of a Security Advisory	after implementing appropriate countermeasures or mitigation measures

In cases involving particularly complex issues or when third-party providers are involved, longer processing times may be required. In such cases, we will keep the person who submitted the report regularly informed of the status of the case.

6. Coordinated Vulnerability Disclosure

The Pütz Group adheres to the principle of coordinated disclosure of security vulnerabilities.

This means::

- The reported vulnerability is initially treated as confidential.
- DeThe reporter receives updates on the status of the investigation.
- Public disclosure occurs only after appropriate mitigations are available or the remaining risk has been adequately assessed.
- The timing and content of the disclosure are coordinated with the reporter, to the extent possible.

7. Safe Harbor

The Pütz Group supports responsible security research.
We will not take legal action against individuals who:

- act in good faith
- act solely for the purpose of identifying and responsibly reporting security vulnerabilities
- do not alter, delete, or publish any data
- do not misuse any personal data or trade secrets
- do not compromise the availability of our systems
- do not carry out social engineering attacks
- do not carry out denial-of-service attacks
- do not use malware
- cease their activities immediately upon discovering a vulnerability and notify us

This assurance applies exclusively to actions taken within the scope of this policy and to the extent permitted by law.

8. Handling CVEs

If a reported vulnerability warrants the assignment of a Common Vulnerabilities and Exposures (CVE) identifier, the Pütz Group will:

- coordinate or assist with the assignment of a CVE
- work with the relevant CVE Numbering Authorities (CNA)
- publish the CVE number in its security advisories
- clearly identify the affected products.

9. Security Advisories

For confirmed security vulnerabilities, the Pütz Group publishes security advisories as needed.

These include, in particular:

- a description of the vulnerability
- affected products and versions
- severity (e.g., CVSS)
- potential impact
- available security updates
- recommended mitigation measures
- references to CVE numbers (if available)

10. Characteristics of industrial systems

Pütz Group products are used in industrial environments where system availability and functional safety are top priorities. As a result, security updates cannot always be released or installed immediately. In such cases, we publish appropriate mitigation measures to reduce risks until an update is available.

Before security updates are released, they are thoroughly tested for functionality, stability, and compatibility.

11. Confidentiality

All reports received will be treated confidentially.

Personal data will be used solely for the purpose of processing the report and will be handled in accordance with applicable data protection regulations.

The name of the person submitting the report will be published only with their express consent

12. Recognition

The Pütz Group would like to thank everyone who contributes to improving the security of our products by submitting responsible reports.

We do not currently offer a financial reward (bug bounty).

13. Changes

This Coordinated Vulnerability Disclosure Policy is reviewed regularly and updated as needed to reflect new regulatory or technical requirements.