KÄSSBOHRER GELÄNDEFAHRZEUG AG

# CYBERSECURITY POLICY

**CYBERSECVA-VS-A 002-0**

## Vulnerability Reporting and Disclosure

**Version: 03.08.2026**

| Prepared | Reviewed | Approved |
|---|---|---|
| Department: DE<br>Name: Stefan Piehler<br>Date: 03.08.2026 | Department: IT<br>Name: Karl Dieing<br>Date / Signature<br>31. August 2026 \| 08:27:37 MESZ<br>Signiert von:<br>ppa. Karl Dieing<br>253DFA6C7E9E4F0... | Department: Executive Board<br>Name: Dr Christian Oberwinkler<br>Date / Signature<br>07. September 2026 \| 08:54:53 MESZ<br>Signiert von:<br>Oberwinkler, Christian<br>B754330E2A87464... |

## 1 Revision History

| Version | Description |
|---|---|
| 03.08.2026 | Initial creation of the document |

## 2 Introduction

Kässbohrer Geländefahrzeug AG is committed to effectively protecting the security of its products with digital elements, its digital services and its publicly accessible IT infrastructure. These are collectively referred to below as “systems within the scope of this Policy”. To this end, Kässbohrer Geländefahrzeug AG operates a defined process for receiving, assessing, handling and coordinating the disclosure of reported vulnerabilities.

We welcome reports from security researchers, customers, partners, CERTs, public authorities, and other members of the security community, provided that they are submitted responsibly, confidentially, and in good faith through the reporting channels described in this Policy.

As a general principle, Kässbohrer Geländefahrzeug AG does not intend to assert civil claims against, or file criminal complaints concerning, reporting parties who act voluntarily, in good faith and in accordance with this Policy. This statement does not authorize unlawful conduct and does not bind public authorities or other third parties.

Accordingly, the reporting party must not engage in unlawful or harmful conduct, collect, use, or disclose data without authorization, impair any system beyond what is necessary for verification, or disclose information about potential vulnerabilities before coordinating disclosure with Kässbohrer Geländefahrzeug AG.

## 3 Contact Information

Reports of potential vulnerabilities may be sent by email to the Security Incident Response Team (SIRT) of Kässbohrer Geländefahrzeug AG at: **cybersecurity@kaessbohrerag.com**.

The initial email is intended to notify us of a potential vulnerability and to establish an appropriate secure communication channel.

In your initial email, provide only the information necessary to establish contact and conduct an initial assessment. Do not send confidential details, personal data, or information that can be directly exploited.

After receiving the initial report, the SIRT will provide an appropriate secure communication channel for exchanging confidential information, such as a TLS-protected communication channel or an equivalent state-of-the-art method.

Confidential technical details, personal data or information that could enable exploitation of the vulnerability must be transmitted only through this secure communication channel.

The SIRT of Kässbohrer Geländefahrzeug AG generally acknowledges receipt of new vulnerability reports within two business days based on the business calendar for its Laupheim, Germany, location and provides information on the next steps. Incoming reports are documented and processed in an internally traceable manner. The SIRT may assign a reference number.

# 4 Vulnerability Handling Process

## 4.1 Reporting a Security Issue

If you wish to report a potential vulnerability in a system within the scope of this Policy, please contact our SIRT using the reporting channels described in the “Contact Information” section.

Coordinated vulnerability reports from the security community make an important contribution to improving the security of systems within the scope of this Policy. This includes reports from security researchers, customers, partners, universities, CERTs, public authorities, and other trusted sources.

We ask reporting parties to treat information about a potential vulnerability as confidential and to disclose it publicly only after coordinating with Kässbohrer Geländefahrzeug AG. This helps reduce risks to customers, users and systems within the scope of this Policy until appropriate remediation or mitigation measures are available.

To enable an efficient assessment of the vulnerability, please provide the following information where possible:

- **Name of the reporting party:** Providing your name is voluntary. Reports may be submitted anonymously.
- **Contact details:** Providing an email address and telephone number is voluntary. Where possible, an appropriate means of contact should be provided for follow-up questions and status updates.
- **Affiliation:** Providing your organizational affiliation is voluntary.
- **Type of reported vulnerability:** How would you describe the type of vulnerability (e.g., XSS, buffer overflow, or hard-coded credentials)?

- **Technical evidence:** Can you provide technical evidence or a proof of concept (PoC) that allows the vulnerability to be reproduced? Alternatively, you may submit network traces (e.g., pcap files) or a description of how the vulnerability may be triggered. Transmit directly exploitable information only through the secure communication channel provided by the SIRT.
- **Impact of the vulnerability:** Have you observed any impact caused, or capable of being caused, by the vulnerability?
- **Affected system:** In which system within the scope of this Policy did you identify the vulnerability? Include all information available to you that enables the affected system to be uniquely identified, in particular its designation, product family and group, location, and firmware or software version.
- **Confidentiality of the vulnerability:** Has the vulnerability already been reported elsewhere, particularly to component manufacturers, suppliers, CERTs or other affected organizations? Has the vulnerability already been disclosed, or do you have specific plans to disclose it?

## 4.2 Analysis

Kässbohrer Geländefahrzeug AG reviews the report received, assesses its relevance and attempts to verify or reproduce the reported vulnerability.

If additional information is required, the Security Incident Response Team will contact the reporting party.

Confidential information is exchanged exclusively through the secure communication channel provided by Kässbohrer Geländefahrzeug AG.

In addition to potential impacts on information security, the assessment also considers potential impacts on functional safety, operational safety, and the protection of human life, physical integrity, and health.

## 4.3 Handling

Kässbohrer Geländefahrzeug AG handles confirmed vulnerabilities using a risk-based approach in cooperation with the responsible specialist and development departments. Appropriate measures are defined to remediate, mitigate, or safely manage the vulnerability. Where necessary, responsible CERTs, affected suppliers, component manufacturers, or other relevant parties may be involved while maintaining confidentiality.

During the handling process, the SIRT provides the reporting party with appropriate periodic updates on the status of the assessment and takes relevant additional information into account where this is necessary to assess or remediate the vulnerability.

Where available and appropriate, pre-release versions of fixes or measures may be provided to the reporting party for verification.

### 4.4 Disclosure

Kässbohrer Geländefahrzeug AG decides, using a risk-based approach and in compliance with mandatory statutory, regulatory, and official duties to inform, warn, disclose, and report, whether, when, and in what form customers, users, or other relevant parties will be informed about a confirmed vulnerability. Publication is generally coordinated and takes available remediation or mitigation measures into account.

Where a confirmed vulnerability may affect customers, operators or other affected parties, Kässbohrer Geländefahrzeug AG provides appropriate information about the vulnerability and available remediation or risk-mitigation measures in a suitable form.

The Security Incident Response Team (SIRT), in coordination with the responsible management system officer and the Executive Board, decides on the nature, scope, and timing of a disclosure.

Kässbohrer Geländefahrzeug AG does not operate a bug bounty program and does not offer compensation for reported or disclosed vulnerabilities. Reporting parties are publicly acknowledged only following prior coordination and with their express consent.

## 5 Final Remarks

This Policy is intended exclusively for receiving, reviewing, and handling vulnerability reports. It does not give rise to any contractual or other claims against Kässbohrer Geländefahrzeug AG and does not constitute an admission of a defect, breach of duty, security incident, or liability.

Kässbohrer Geländefahrzeug AG does not guarantee that a reported vulnerability will be confirmed, remediated or handled within a specific period. The nature, scope and timing of any measures depend on the risk-based assessment and the applicable statutory, regulatory and official requirements.

The liability of Kässbohrer Geländefahrzeug AG remains limited to cases of mandatory statutory liability, including, in particular, cases involving intent, gross negligence, or injury to life, physical integrity, or health.

Where statutory, regulatory, or official obligations are affected, Kässbohrer Geländefahrzeug AG assesses and fulfills them in accordance with the applicable internal processes.