SECURITY

Coordinated Vulnerability Disclosure Policy

Scope, safe harbour, expected timelines and reporting process for security researchers.

Document	Terravek_Vulnerability_Disclosure_Policy.pdf
Revision	3
Date of issue	02 April 2026
Author	Laura Peeters, Security Engineer, Application Security
Author e-mail	laura.peeters@terravek.com
Department	Information Security & IT
Approved by	Ingrid Halvorsen
Classification	Public
Template	TVK_Policy_A4.dotx
Prepared using	Microsoft® Word for Microsoft 365

Terravek Systems N.V. · Zuidpoortlaan 118, 2628 XK Delft, Netherlands · +31 15 251 8400 · info@terravek.com
KvK 27381164 · VAT NL818472093B01 · LEI 7245009XKQVTPZ4NRK18

This document is fictional and forms part of a training environment.

Reporting

Report security vulnerabilities to security@terravek.com. Our PGP key fingerprint is published at https://www.terravek.com/.well-known/security.txt in accordance with RFC 9116. You do not need to sign anything before reporting and we will not ask you to.

Our commitments

- Acknowledgement within 72 hours (2025 median: 11 hours)
- An assessment within ten working days, with the severity and our reasoning
- Progress updates at least every fourteen days until closure
- Credit in our hall of thanks, with your consent, under any name you choose
- A reply written by an engineer rather than by a lawyer
- Safe harbour for good-faith research conducted under this policy

Scope

- terravek.com and its subdomains
- api.terravek.com — the ATLAS API
- portal.terravek.com and partners.terravek.com
- identity.terravek.com
- ORBIS Viewer web application
- FIELDKIT companion mobile application and device firmware
- Open-source repositories at github.com/terravek

Out of scope

- Third-party hosted services on our domains (report to the vendor, and tell us)
- Missing headers, cookie flags or TLS configuration without demonstrated impact
- Automated scanner output with no validation
- Social engineering of staff, customers or suppliers
- Physical attacks against offices or the Svalgrund site
- Denial of service or volumetric testing

What we ask

- Give us reasonable time before publishing — we suggest 90 days and will discuss it
- Do not access, modify or delete data that is not yours
- Use test accounts; ask us and we will provide one
- One issue per report, with enough detail to reproduce
- Do not condition a report on payment — we do not operate a paid bounty

Handling

Reports are triaged by Laura Peeters (Security Engineer, Application Security) and escalated as needed to Riina Tamm (Head of Security Operations) and Ingrid Halvorsen (Chief Information Security Officer). Severity uses CVSS 4.0 with a documented environmental adjustment.

2025 statistics

31 reports received: 8 valid and fixed, 3 valid and risk-accepted with reasoning shared with the reporter, 11 out of scope, 9 duplicates. Median first response 11 hours; median time to fix 19 days; slowest 94 days (third-party dependency, reporter informed at day 20).