SECURITY

Information Security Policy v6.0

The top-level ISMS policy under ISO/IEC 27001:2022. Published for customer due diligence.

Document	Terravek_Information_Security_Policy_v6.pdf
Revision	6
Date of issue	18 November 2025
Author	Ingrid Halvorsen, Chief Information Security Officer
Author e-mail	ingrid.halvorsen@terravek.com
Department	Information Security & IT
Approved by	Saskia Bakhuis
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.

1. Purpose and scope

This policy is the top-level statement of Terravek's information security management system, certified to ISO/IEC 27001:2022. It applies to all Terravek Systems N.V. entities, all employees, contractors and interns, and all information assets regardless of format or location.

It is published externally so that customers can assess it without a non-disclosure agreement.

2. Governance

The Chief Information Security Officer owns this policy and reports to the Chief Executive Officer, with a standing quarterly slot with the Supervisory Board's Audit Committee independent of the executive reporting line.

Risk acceptance is a business decision. The Security Operations Centre owns detection, triage and response; it does not own the decision to accept a risk. That decision is made by a named person with authority to make it, and recorded.

3. Control themes

Terravek's Statement of Applicability covers all 93 Annex A controls of ISO/IEC 27001:2022. Exclusions are recorded with justification and reviewed annually.

- Organisational controls — policy, roles, supplier security, incident management
- People controls — screening, terms of employment, awareness, disciplinary process
- Physical controls — perimeter, entry, clear desk, equipment, secure disposal
- Technological controls — access, cryptography, logging, secure development

4. Access control

Access is granted on the principle of least privilege, provisioned through the joiner–mover–leaver process, and recertified quarterly by the system owner.

Privileged access requires a separate account, phishing-resistant authentication and a recorded justification. All privileged sessions are logged.

Support access to customer data is role-based, logged and requires a ticket reference. Customers may disable out-of-region support access per tenancy.

5. Cryptography

Data is encrypted in transit using TLS 1.2 or above with modern cipher suites, and at rest using AES-256. Key management is documented separately in the cryptographic controls standard.

Terravek does not implement its own cryptographic primitives.

6. Secure development

All changes pass code review, automated dependency scanning and static analysis before merge. Threat modelling is required for new services and for material changes to existing ones.

Production access is not granted to development environments and vice versa.

7. Incident management

Security incidents are managed by the Security Operations Centre under a documented process, with severity assigned on a published scale. Customers affected by an incident are notified without undue delay, and in any case within the timescales in their agreement and applicable law.

A post-incident review is published for every incident with customer impact. No individual is named as a cause.

8. Coordinated vulnerability disclosure

Terravek operates a public disclosure programme at security@terravek.com with a 72-hour acknowledgement commitment and safe harbour for good-faith research. See terravek.com/legal/vulnerability-disclosure.html and /.well-known/security.txt.

9. Compliance and audit

Internal audit is independent of the quality organisation and reports to the Audit Committee. External certification is maintained by Kesteren Certificatie B.V. (ISO standards) and Halbrook & Meyers LLP (SOC 2 Type II).

This policy is reviewed at least annually and after any material change to the business or its risk profile.