

# Trekea Information Security Summary

Issued May 2026

Valid until superseded

This document describes the administrative, physical, technical and organisational security measures maintained by Trekea Mobile in connection with the delivery of FieldLogs to customers.

## 1. FieldLogs Service Security Architecture

### 1.1 Hosting Platform

The FieldLogs service can be hosted on a variety of cloud service providers, among others:

- Amazon Web Services (ISO 27001, SOC 2 Type II certified). Details at the AWS Trust Center.
- Microsoft Azure (ISO 27001, SOC 2 Type II certified). Details at the Microsoft Trust Center.

### 1.2 Tenant-Isolated Multi-Tenant Architecture

FieldLogs is a multi-tenant capable Cloud platform, organized around separate customer grids/environments (physically separated operating system instances) with strict tenant (customer instance) isolation controls by design. Tenant data is physically segregated, while authentication and deployment configuration may vary by customer grid.

### 1.3 Encryption

- Data in transit: HTTPS/TLS 1.2 or higher.
- Data at rest: AES-256 or equivalent as provided by the hosting platform providers. All storage accounts, drives and backups encrypted.
- Encryption keys managed via key vault (Azure: Azure Key Vault; AWS: AWS Key Management Service (KMS)) within the agreed data centre region.

### 1.4 Monitoring & Threat Protection

- 24x7x365 Monitoring, Detection and Remediation using advanced enterprise-grade toolsets.
- Platform-level DDoS detection and protection.
- Virus and malware protection.

### 1.5 Backup & Disaster Recovery

- Multi-level backups with geographically separated storage within the agreed deployment region.
- Trekea will not replicate or move data outside the agreed region without the customer's formal consent.
- Multi-level restoration capability.
- Disaster recovery to a geographically separate location within the agreed region is available upon request.

### 1.6 Data Residency

Customers select from supported Cloud Provider geographies. The applicable data centre location is specified in the Order Form. For cloud deployments, cloud infrastructure security controls apply to the customer's chosen hosting environment.

## 2. Information Security Management System (ISMS)

### 2.1 Security Operations Centre



Trekea operates a SOC providing 24x7x365 monitoring, detection and remediation, using enterprise-grade conventional.

## 2.2 Access Control

- Access is controlled on a least-privilege basis.
- SSO and MFA are enforced across the Trekea estate.
- FieldLogs: infrastructure support team access is via SSH key with secured controls.
- Access rights reviewed periodically; revoked immediately on role change or termination.

## 2.3 Cryptography

- In transit: HTTPS/TLS 1.2 or higher enforced at all service entry points.
- At rest: AES-256 or equivalent encryption for all storage, databases and backups. SQL TDE used for ESM Assyst databases.
- Encryption keys managed via Microsoft Key Vault / Azure KMS, held within the agreed data centre region.

## 2.4 Third-Party Supplier Security

Trekea applies a formal Supplier Management and Partner Management process. All third-party suppliers with access to FieldLogs or customer information must comply with Trekea information security policies, GDPR and applicable privacy requirements in relevant regions. Audit rights over supplier security practices are maintained.

## 3. Personnel Security

- Extensive pre-employment background screening for all Trekea personnel with access to customer environments or data.
- Security induction training at onboarding; annual security awareness training programme.
- Formal on- and off-boarding processes ensuring prompt access revocation and continued confidentiality obligations post-employment.

## 4. Product Security

### 4.1 Secure Product Development Lifecycle (SPDLC)

- Environment segregation (development, test, production).
- Formal change management for all production changes with tooling enforcement.
- Secure coding based on globally recognised guidelines such as OWASP Top 10.
- Team independent test and validation prior to release.
- Strictly controlled software release and distribution with tightly controlled and tool enforced access.
- External specialist penetration testing throughout the development lifecycle.

### 4.2 Through-Life Security

Trekea continuously tests released products against evolving threats, including embedded third-party components. Security patches are provided for all identified vulnerabilities. FieldLogs customers receive automated patching.

## 5. Data Privacy

### 5.1 Privacy Programme

Trekea operates a global privacy programme covering GDPR and CCPA, overseen by Trekea's Global Privacy Officer. Ongoing staff training, comprehensive privacy policies and procedures, and an active compliance framework are maintained.



---

## 5.2 Roles

**Customer (Controller):** Determines purposes and means of processing Personal Data.

**Trekea (Processor):** Processes Personal Data solely on Customer's documented instructions, for the limited purposes set out in the DPA.

**Trekea and third-party sub-processors: Process Personal Data on behalf of Trekea as listed in the Sub-Processors List.**

## 5.3 Data Processing Addendum & Transfers

The DPA governs all processing of Personal Data and incorporates EU SCCs (Module 2) and UK IDTA as applicable. Cross-border transfers are covered by SCCs, DPF or other appropriate mechanisms per the Sub-Processors List.

## 6. Incident Response

- SOC monitoring for security events 24x7x365.
- Formal incident classification, investigation and root cause analysis.
- Customer notification within 72 hours of becoming aware of a Personal Data Breach, per the DPA.
- Retrospective incident reports for emergency maintenance events within five (5) business days.
- Coordination with supervisory authorities and data subjects as required by applicable law.
- Overall approach based on the NIST 800 framework standard.

## 7. Updates

Trekea will not materially decrease the overall security of any services during the term of the Agreement.