DATA SECURITY & CORPORATE COMPLIANCE STATEMENT

Document Reference: DS-SEC-2026
Classification: Public Operational Security Statement
Effective Date: July 2026

1. OVERVIEW

This document outlines the core data governance, encryption protocols, and infrastructural resilience frameworks enforced across the Driverseat Innovations Telematics Platform (accessible via portal.driverseat.co.nz). Our architecture is engineered to satisfy the strict information security and data governance requirements mandated by Tier-1 enterprise commercial transport and civil infrastructure partners.

2. DATA IN TRANSIT (TRANSPORT SECURITY)

All data communication passing through our ecosystem is cryptographically secured to prevent interception, spoofing, or tampering:

End-User Access:
All connections to the tracking dashboards via web browsers are strictly enforced over secure HTTPS using TLS 1.2 or TLS 1.3 protocols. Non-encrypted HTTP traffic is rejected by default.

Hardware Telemetry Streams:
Data transmitted from field telematics gateways (Teltonika FMC650 units) over cellular networks utilizes standard secure communication protocols, ensuring the integrity of raw sensor packages (including weight utilization metrics and tire pressure data) from the vehicle to the processing engine.

Network Signatures:
The portal domain is secured with cryptographically signed DNSSEC (Domain Name System Security Extensions) and backed by premium cloud-level DDoS mitigation architecture to prevent malicious traffic redirection and maintain service availability.

3. DATA AT REST (STORAGE SECURITY)

Industrial Encryption Standards:
All historical fleet telemetry, historical asset events, user account profiles, and configuration baselines stored within the persistent database layer are encrypted using AES-256 block-level encryption.

Credential Isolation:
Operational secrets, application programming interface (API) tokens, and system authentication keys are structurally isolated via hardware/software security vaults resolved strictly at runtime.

4. MULTI-TENANT DATA ISOLATION (PRIVACY CONTROLS)

The Driverseat Innovations platform operates on a rigid Multi-Tenant Role-Based Access Control (RBAC) architecture:

Database Segregation:
Client data structures, fleet tracking groups, mapping assets, and user spaces are structurally isolated at the database level.

Zero-Cross Visibility:
Authorized client personnel can interact exclusively with their own assigned fleet inventory. Third-party entities, external transport fleets, or unauthorized users are structurally blocked from viewing, intercepting, or querying your operational telemetry streams.

5. UPSTREAM INFRASTRUCTURE & PHYSICAL RESILIENCE

The processing core of our platform is deployed via highly available, multi-zone ThingsBoard Cloud Software-as-a-Service (SaaS) infrastructure, hosted across hyper-scale Tier-1 cloud data centers (Amazon Web Services / Google Cloud Platform). The underlying physical and network virtualization layers strictly maintain the following international compliance frameworks:

- **ISO/IEC 27001:** International Standard for Information Security Management Systems.
- **SOC 2 Type II:** Independent Service Organization Control attestation covering system Security, Availability, and Confidentiality.
- **High Availability & Redundancy:** Operational data is continuously replicated across independent availability zones with automated daily backup retention loops, ensuring a 99.9% operational uptime availability baseline.

6. CONTACT & VALIDATION

Driverseat Innovations Limited is fully committed to maintaining absolute data integrity and security compliance for our corporate fleet partners. For specific technical inquiries, architectural audits, or corporate procurement onboarding requests, please contact our operations desk.

Michael
Director | Driverseat Innovations Limited
Email: michael@driverseat.co.nz
Web: www.driverseat.co.nz