Security & Privacy Overview

Top Tier Plan — Dealership Training, Task & Process Management Platform | toptierplan.com/security

Top Tier Plan ("TTP") is a hosted platform automotive dealerships use for employee training, daily tasks, process documentation, internal messaging, and pre-hire assessments. This document summarizes the safeguards that protect your dealership's data. It is written to support your vendor oversight under the FTC Safeguards Rule (16 CFR Part 314).

Data Isolation

- Each dealership runs on its **own separate database** and its own site address. No tables are shared between dealerships.
- Users of one dealership cannot access another dealership's site or data.
- Dealership administrators control who has an account, each person's role (Admin, Manager, Employee), and their positions, which determine the tools they can use.
- Self-registered accounts cannot sign in until a manager approves them.

Encryption

- All traffic uses **HTTPS with TLS 1.2 or 1.3**; TLS 1.0/1.1 are refused, plain HTTP is redirected to HTTPS, and HSTS is enabled for one year.
- Passwords are stored only as **bcrypt** hashes. Sign-in codes and remembered-device tokens are stored as SHA-256 hashes.
- Session tokens are long random values tied to one user, with an expiry, and are deleted on sign-out.
- Backup copies are transferred off-site over SFTP (encrypted).

Authentication & Access

- **Two-step sign-in (MFA)** for administrators and managers: a 6-digit code emailed after the password; expires in 15 minutes; 5 tries. Users may remember a device for 30 days.
- **Password policy:** 12+ characters; common, repetitive and username-based passwords blocked; checked on the server.
- Temporary passwords are random and must be changed at first sign-in.
- Website sessions end after **30 minutes of inactivity**. Changing or resetting a password signs out the user's other devices.
- Role and position checks are enforced on the server for every request. The API only accepts browser requests from Top Tier Plan's own pages.

Logging & Monitoring

- A **Sign-in Activity log**, visible to your administrators, records sign-ins, failed sign-ins, wrong codes, sign-outs, password changes and resets, accounts added/approved/removed, and role changes, with time, IP address and device. Kept for one year.
- **Support access** by Top Tier Plan staff uses a one-time pass valid for a single site, expires within 2 minutes if unused, gives a session of at most 1 hour, and is recorded in your activity log.
- Our hosting provider keeps server access and error logs.

Hosting & Backups

- Hosted in the **United States** by a commercial hosting provider (Hostinger) that manages the physical data center, network protection, and server operating system, web server, PHP and MySQL updates.
- **Nightly database backups** of every dealership, kept 30 days; **weekly** backups of site files and uploads, kept 5 weeks.
- Backups are copied **off-site daily**, in addition to the hosting provider's own backups. Restores have been tested.

Data Handling & Privacy

- Core data: employee names, work email, phone, extension, employee number, positions, training and task history, messages, and applicant assessment results.
- Optional tools (Open ROs, Loaners, warranty uploads, extended-warranty schedules) may contain **your customers' names, RO and stock numbers, and VINs**. This stays in your dealership's database. We do not ask for SSNs, driver's license, bank or card numbers.
- Messages are deleted after 3 months; warranty uploads after 60 days.
- We use data only to provide the service. We do not sell or share it, and we use no advertising or analytics trackers.

Incident Response

- We follow a written incident response plan (part of our WISP).
- If we confirm a security incident affecting your dealership's data, we notify your designated contact **within 72 hours** and coordinate containment, investigation, and any notices you are required to send (including FTC notification under the Safeguards Rule).
- A written summary of the incident and corrective actions is provided within 14 days of resolution.

Compliance Posture. Top Tier Plan's safeguards are designed to support your dealership's compliance with the **FTC Safeguards Rule**, the **Gramm-Leach-Bliley Act (GLBA)** service-provider oversight requirements, and applicable state privacy laws. We maintain a **Written Information Security Program (WISP)** with a designated Qualified Individual, provide a signed **Data Processing Agreement (DPA)**, carry **cyber liability insurance**, and can complete standard vendor security questionnaires (SIG-Lite, CAIQ, or your own). SOC 2 Type II is on our roadmap for enterprise customers.

Your Data, Your Control

- Your dealership **owns** all data entered into its site.
- Data export in standard formats (CSV / SQL) on request.
- On termination, data is available for export for 30 days, then deleted from active systems, and from backups within 90 days.
- Individual access, correction, and deletion requests are handled within 45 days (or sooner where law requires).

Contact & Documentation

Security or privacy questions, or to report a concern: **support@toptierplan.com** (subject "Security"). Public summary: **toptierplan.com/security**.

Available on request:

- Data Processing Agreement (DPA)
- Written Information Security Program (WISP), under NDA
- Certificate of cyber liability insurance
- Security questionnaire responses

This document is provided for informational purposes and reflects our practices as of the date below. It is not a contract; the subscription agreement and DPA govern the legal relationship between Top Tier Plan and your dealership. Last updated: October 4, 2026.