VERO FLEET // DEALER COMPLIANCE

Dealer Compliance & Data Security Checklist

A practical control checklist for automotive dealers and rental operators. Aligned to the FTC Safeguards Rule and common state privacy requirements. Use this as a self-audit; Vero Fleet can help you close every gap.

1. Program Governance (FTC Safeguards Rule §314.4)

- ■ Written Information Security Program (WISP) is documented and current.
- ■ Qualified Individual is designated to oversee the security program.
- ■ Annual written report delivered to ownership or the board.
- ■ Risk assessment performed in writing within the last 12 months.
- ■ Service-provider list maintained with security obligations in contracts.

2. Customer Data Protection

- ■ Customer PII and financial data encrypted at rest and in transit.
- ■ Multi-factor authentication enforced on DMS, email, and admin systems.
- ■ Role-based access controls limit data access to job function.
- ■ Access reviewed quarterly; departing employees offboarded within 24 hours.
- ■ Secure disposal procedure for paper deal jackets and retired hardware.

3. Network & Endpoint Security

- ■ Business-grade firewall with segmented guest, sales, and service VLANs.
- ■ Wi-Fi uses WPA3 (or WPA2-Enterprise); guest network isolated from internal.
- ■ Endpoint detection & response (EDR) deployed on every workstation.
- ■ Operating systems and DMS clients patched within 30 days of release.
- ■ Backups tested at least quarterly; one copy stored offsite or in cloud.

4. Monitoring, Detection & Response

- ■ Continuous monitoring of endpoints, network, and identity events.
- ■ Logging retained for at least 12 months in a tamper-resistant system.
- ■ Documented incident response plan with named contacts and timelines.
- ■ Penetration test or vulnerability assessment within the last 12 months.
- ■ Tabletop exercise run with management at least annually.

Checklist (continued)

5. Document Retention & Audit Trail

- ■ Retention schedule defined for deal jackets, F&I docs, and e-signatures.
- ■ Digital deal files stored in a system with immutable audit logging.
- ■ Records retrievable on demand for state DMV and lender audits.
- ■ Privacy notices delivered and acknowledgements stored with each deal.

6. People & Training

- ■ Annual security awareness training completed by all staff.
- ■ Simulated phishing campaigns run at least quarterly.
- ■ F&I and BDC staff trained on Red Flags identity-theft prevention.
- ■ Acceptable Use Policy signed by every employee at hire and annually.

7. Third-Party & DMS Integration

- ■ Every DMS integration uses least-privilege API credentials.
- ■ Vendor security questionnaires on file for CRM, digital retail, and lenders.
- ■ Data shared with third parties is limited to the minimum necessary.
- ■ Decommissioned integrations have credentials revoked the same day.

Recommended Next Steps

01 Run a 30-minute gap review against this checklist with your IT lead and F&I director.

02 Prioritize any unchecked items in Sections 1–3 first — these are the most common audit findings.

03 Schedule a Vero Fleet compliance review to validate controls and produce auditor-ready documentation.

04 Set a recurring quarterly review so your program stays current as systems and regulations change.

READY TO CLOSE THE GAPS?

Book a compliance review with Vero Fleet.

Vero Beach, FL • hello@verofleet.com • 888.VERO.FLEET