12-Step MDVR Tampering Prevention Checklist

Detect, prove and prevent tampering with your fleet MDVR recordings

Use this checklist to implement tamper controls in stages. Tick each item when complete. Keep a signed copy per incident in your chain-of-custody records.

Phase 1 — Immediate (this week)

- [ ] Step 1: Draft a "video evidence handling" policy
  Who: Ops manager + Legal
  Sets responsibilities — who handles media, retention rules, chain-of-custody.

- [ ] Step 2: Train drivers: do not remove SD cards
  Who: Fleet trainer
  Issue a one-page reminder card for every cab.

- [ ] Step 3: Print and distribute incident capture checklists
  Who: Ops
  Drivers need a tiny laminated checklist for high-stress situations.

- [ ] Step 4: Audit 10% of vehicles for vulnerabilities
  Who: Maintenance lead
  Check for loose mounts, exposed SD slots, accessible ports.

- [ ] Step 5: Run a hashing pilot on 5 vehicles
  Who: IT + depot technicians
  Test extraction, SHA256 hashing and manifest workflow end-to-end.

- [ ] Step 6: Verify cloud sync upload rates and timestamps
  Who: IT / Telematics
  Confirm cloud copy timestamps match local files; flag gaps.

Phase 2 — Short Term (30 days)

- [ ] Step 7: Fit tamper-evident seals and lockboxes on MDVRs
  Who: Install team
  Document seal IDs (format: BW-EV-YYYY-MM-DD-VEH-SEAL###). Photograph during audits.

- [ ] Step 8: Configure devices correctly
  Who: Install team / IT
  UTC timestamps, system logging, auto-upload, event-triggered locking, parking mode.

- [ ] Step 9: Harden access control
  Who: IT
  Unique admin accounts, rotate passwords, disable debug ports, remove default credentials.

Phase 3 — Mid Term (90 days)

- [ ] Step 10: Deploy central evidence management
  Who: IT + Ops

Automated hashing, central storage, retention rules and role-based access controls.

☐ Step 11: Create an incident response runbook
Who: Ops + Legal
Chain-of-custody template, export procedures, forensic contacts, insurer notifications.

☐ Step 12: Continuous improvement and supplier contracts
Who: Procurement + Fleet manager
Monthly audits. Require firmware signing and agreed SLAs from MDVR suppliers.

Acceptance criteria — all 12 steps complete when:

Policy drafted and approved	Ops manager + Legal	Week 1
Driver guidance issued + reminder cards in cabs	Fleet trainer	Week 1
Incident checklists printed and distributed	Ops	Week 1
Baseline audit of 10% vehicles complete	Maintenance lead	Week 1
Hashing pilot on 5 vehicles complete	IT	Week 2
Cloud sync verified on pilot vehicles	IT / Telematics	Week 2
Tamper-evident seals fitted and documented	Install team	Month 1
Devices configured (UTC, logs, auto-upload)	Install team / IT	Month 1
Access controls hardened (accounts, ports)	IT	Month 1
Central evidence management deployed	IT + Ops	Month 3
Incident response runbook complete	Ops + Legal	Month 3
Supplier firmware-signing clauses added	Procurement	Month 3

■ Red flags — act immediately if you see:

■ Gap in footage that aligns with a parked or incident period
■ SD card or device handled before hashes were computed
■ Timestamp reset or jump inconsistent with surrounding files
■ Unsigned firmware version found during audit
■ Seal broken or removed with no maintenance record