



ELD Mandate Endpoint Compliance Checklist

Practical checklist for fleet endpoints supporting the U.S. FMCSA ELD Rule (49 CFR Part 395) using Codeproof UEM.

Note: ELD compliance is an operational and regulatory responsibility of the motor carrier. Codeproof provides endpoint and application controls that help harden devices running approved ELD/HOS applications (for example, Geotab App and others), but does not replace regulatory processes or carrier policies.

1) Driver & User Authentication

- Require unique driver IDs; integrate SSO/PIN as provided by the ELD vendor.
- Enforce session lock and idle timeout on all in-cab/handheld devices.
- Apply role-based access (driver vs. admin/technician).

2) Device Configuration & Hardening

- Enforce full-disk encryption and strong unlock (passcode/biometric).
- Force OS and app updates; block outdated builds from production use.
- Disable risky features: unknown sources, USB debugging, developer options, tethering (as policy allows).
- Use kiosk mode (single/multi-app) to restrict devices to the ELD, maps, and permitted apps only.
- Standardize time settings and network time synchronization.

3) ELD App Governance

- Allowlist the approved ELD/HOS application(s); block unapproved third-party app stores. For example: Geotab App and others.
- Use managed configurations to grant required permissions (location, Bluetooth, background activity, battery optimization exemptions).
- Enforce app integrity (verify package signatures); prevent uninstall without admin approval.

4) Connectivity & Data Transfer

- Preconfigure cellular/APN and Wi-Fi profiles; ensure reliable connectivity on routes and depots.
- Deploy certificates and trusted roots for secure API connections; support per-app VPN if required.
- Support ELD data transfer methods (as provided by vendor): telematics (web services/email) and local (USB/Bluetooth).

5) Location, Time & Sensors

- Grant high-accuracy location with background access for the ELD app.
- Ensure correct time zone/UTC offset; prevent manual time tampering where supported.
- Maintain permissions needed for ECM/telematics dongle connectivity (Bluetooth/USB).

6) Tamper Prevention & Detection

- Block rooting/jailbreaking; quarantine non-compliant devices automatically.
- Prevent uninstall or settings changes without administrative approval.
- Disable date/time changes and developer options where the platform supports it.
- Enable device and app crash reporting; alert IT on anomalies.

7) Malfunctions & Diagnostics

- Monitor for ELD malfunction categories (e.g., power, timing, positioning, data recording/transfer, communications).
- Provide driver instructions to annotate RODS and use paper logs when required by regulation.
- Track unidentified driving records and assign them promptly per policy.

8) Roadside Inspection Mode

- Ensure the ELD app's inspection mode is easily accessible to officers.
- Lock display orientation and brightness settings suitable for inspection; keep device securely mounted.

9) Incident Response & Support

- Enable remote lock, reboot, and configuration push for field support.
- Define a rapid swap/replacement workflow with zero-touch provisioning.
- Perform selective/full wipe on retired or lost devices; revoke credentials and certificates.

10) Evidence & Recordkeeping

- Maintain inventory of ELD devices with ownership and assignment metadata.
- Export configuration history, policy changes, app/OS versions, and compliance posture for audits.
- Retain logs of remote actions (lock/wipe), incidents, and device replacements.

Copyright © Codeproof Technologies Inc. — This checklist supports endpoint controls for the ELD Rule using Codeproof. It is not legal advice.
