EV Software Diagnostics and Data Security Checklist

Electric Vehicle & Charging Station Industry

COMPLIANCE - DATA PRIVACY & CONFIDENTIALITY

Data from vehicle diagnostics does not include customer personal data.

Yes No NA

All software development follows secure coding standards (e.g., ISO/SAE 21434).

Yes No NA

Third-party software components used in diagnostics are vetted and approved.

Yes No NA

Incident response plan exists for cybersecurity breaches or data loss.

Yes No NA

CRITICAL - DIAGNOSTICS & CALIBRATION

Diagnostic sessions are logged with VIN, user ID, and purpose.

Yes No NA

All diagnostic laptops and equipment have updated antivirus and firewall enabled.

Yes No NA

Parameter calibration is performed only with OEM-approved datasets.

Yes No NA

Software used for diagnostics is licensed and updated to the latest OEM release.

Yes No NA

Testing after calibration ensures all safety and performance parameters are within range.

Yes No NA

Diagnostic connector ports are protected when not in use.

Yes No NA

CYBERSECURITY - ACCESS CONTROL

User authentication is required before accessing vehicle software tools.

Yes No NA

Multi-factor authentication (MFA) is enabled for all remote software access.

Yes No NA

Login sessions time out automatically after inactivity.

Yes No NA

User access rights are reviewed monthly for technicians and engineers.

Yes No NA

All password policies meet company security standards (length, complexity, expiry).

Yes No NA

CYBERSECURITY - NETWORK & COMMUNICATION

Vehicle communication networks (CAN, LIN, Ethernet) are protected from unauthorized access.

Yes No NA

Wireless interfaces (Bluetooth, Wi-Fi, LTE) use secure protocols.

Yes No NA

Diagnostic systems are not connected to public Wi-Fi networks.

Yes No NA

Periodic vulnerability scanning is performed on all diagnostic devices.

Yes No NA

VPN or secure tunnels are used for remote diagnostics and software uploads.

Yes No NA

DOCUMENTATION & RECORDS - AUDIT TRAILS

All diagnostic and firmware changes maintain automated audit trails.

Yes No NA

System audit logs retained for minimum of 2 years and reviewed quarterly.

Yes No NA

MAINTENANCE - DATA BACKUP & STORAGE

All system backups (firmware, configs, user data) are performed regularly.

Yes No NA

Backups are encrypted and stored in secure servers or cloud storage.

Yes No NA

Access to backup repositories is limited to authorized IT or engineering personnel.

Yes No NA

Periodic data restoration drills are performed to ensure backup reliability.

Yes No NA

Firmware distribution systems maintain version history and deployment logs.

Yes No NA

SUPER CRITICAL - SOFTWARE VALIDATION & FIRMWARE MANAGEMENT

All ECUs, BMS, and vehicle controllers are running approved firmware versions.

Yes No NA

Firmware updates are verified using checksum or digital signature before installation.

Yes No NA

All software updates follow formal approval workflow with traceable authorization.

Yes No NA

Reprogramming tools (VCI, OBD interface, or service laptop) are OEM-approved.

Yes No NA

Rollback or recovery image is created before any software update.

Yes No NA

SYSTEM TESTING & VALIDATION

Software validation testing includes fail-safe and functional safety checks.

Yes No NA

Regression tests are conducted after every major firmware update.

Yes No NA

Cyberattack simulations or penetration tests are performed annually.

Yes No NA

Diagnostic software logs error codes and abnormal system events automatically.

Yes No NA

ECU and BMS firmware integrity is verified via checksum at each ignition cycle.

Yes No NA

TRAINING & COMPETENCY - WORKFORCE

Technicians handling firmware tools trained in cybersecurity and IT protocols.

Yes No NA

Periodic awareness sessions conducted for engineers on phishing and malware prevention.

Yes No NA

Only designated cybersecurity officers can approve firmware uploads.

Yes No NA