BYOD Policy Template for Dealerships

> **How to use it.** Replace everything in [brackets] with your store's own details, and change any line that doesn't fit. Fill it in with whoever runs IT, then mark each cell of the access table with what your store allows. **This template is not legal advice. Notice of monitoring and paying staff back for work use of their own phones can be set by state law, so have your attorney review it before anyone signs.** Ask your attorney about the monitoring notice wording for each state where you have a store (line 7.3), whether you owe staff reimbursement for work use of their phones, and the wording of line 6.2.

Dealership name _____ Effective date _____

1 Who and what this covers

1.1 This policy covers anyone who uses a personal phone, tablet or computer for [Dealership Name] work, including part-time staff, temps and contractors.

1.2 Using a personal device for work is [optional / allowed only with approval]. Anyone who would rather not can ask for [a store device / another option].

1.3 The policy owner is [name, title]. Questions go to [name, phone] before you act, not after.

2 Approval and setup

2.1 A personal device reaches dealership email, the CRM or the DMS only after [IT contact] approves it and writes down whose it is, what it is and which systems it may reach.

2.2 What each device may reach follows the access table in this policy. Anything not on the table needs [policy owner]'s approval first.

2.3 Dealership apps and data live only in [the managed work profile or approved apps] that [IT contact] sets up.

3 Required controls

3.1 A screen lock with [a six-digit PIN, fingerprint or face unlock], set to lock after [number] minutes.

3.2 Multi-factor sign-in on every dealership account used on the device.

3.3 Operating system updates installed within [number] days. A device that no longer gets security updates from its maker comes off the list.

3.4 No jailbroken or rooted devices, and apps only from the official app store.

What the FTC and NIST say

FTC Safeguards Rule. 16 CFR 314.4(c)(5) calls for multi-factor authentication "for any individual accessing any information system," unless your Qualified Individual approves an equivalent or stronger control in writing.

FTC FAQs for dealers. The FTC staff's Safeguards Rule FAQ for auto dealers says the rule applies to financial institutions under the FTC's authority, and "That includes most automobile dealers who finance or lease automobiles." Approved financing and lease applications are always customer information, it adds.

NIST SP 800-124. NIST SP 800-124 Revision 2 (May 2023) says many mobile devices, "particularly those that are personally owned," "are not inherently trustworthy," and tells organizations to treat every mobile device as untrusted until they've secured it and keep monitoring it.

State law can add its own rules on monitoring notice and on paying staff back for work use of their phones. Ask counsel.

The access table

Line 2.2. Mark what your store allows in each cell. heliontechnologies.com/dealership-byod-policy-template/

The system	Personal phone	Personal computer	Store-issued device
Email and calendar	Only inside [the work profile or approved email app], with multi-factor sign-in and a screen lock.	[Web browser only, nothing downloaded / Not allowed].	Allowed.
The CRM	[The CRM's own app], with multi-factor sign-in. No exports and no screenshots of customer lists.	[Not allowed / Web browser only].	Allowed.
The DMS	[Not allowed / The approved DMS app only], with multi-factor sign-in.	Not allowed.	Allowed, at the store or through [approved remote access].
Calls and texts with customers	From a company number in [the store's phone app], never the personal number.	[The store's phone app], same rule.	Through the store's phone system.
Driver's licenses and deal paperwork	Never photographed, saved or texted. Scan it at the desk into [the DMS or deal system].	Never saved or opened.	Into [the DMS or deal system] only.
Shared files	Opened in [approved app]. Nothing saved to the phone itself.	[Not allowed].	Allowed.
Remote access to store systems	Not allowed.	[Not allowed / Through approved remote access, with multi-factor sign-in].	Through [approved remote access], with multi-factor sign-in.
[Other system]			

4 What never goes on a personal device

4.1 Photos of driver's licenses, insurance cards, credit applications or any other deal paperwork.

4.2 Customer lists, exports or reports from the CRM or the DMS.

4.3 Customer or employee information in personal email, personal cloud storage, personal messaging apps or personal AI accounts.

4.4 Passwords for dealership systems, unless they're kept in [approved password manager].

5 Calling and texting customers

5.1 Staff call and text customers from a company number in [the store's phone app], not from their personal number.

5.2 Texts to customers follow the store's consent and opt-out rules.

5.3 If a customer reaches you on your personal number, move the conversation to the company number.

6 Lost, stolen or replaced devices

6.1 Report a lost or stolen device to [name, phone] within [number] hours.

6.2 The store can then remove dealership apps and data from the device remotely, and only those.

6.3 Before you sell, trade in or give away a device, tell [IT contact] so dealership data comes off it first.

7 Privacy on a personal device

7.1 The store can see [device model, operating system version, whether the screen lock is on, the work apps installed]. [IT contact] keeps this list current.

7.2 The store's setup is chosen so it doesn't see [personal apps, photos, texts, email, browsing, or location outside the work apps]. If that changes, staff are told in writing first.

7.3 Any notice of monitoring uses the wording counsel approves for [state].

8 When someone leaves

8.1 On the last day, [IT contact] removes the work profile and every dealership account from the person's personal devices.

8.2 Their company number is rerouted to [manager or team].

8.3 The person confirms in writing that no dealership or customer information is left on any personal device.

9 Review and sign-off

9.1 [Policy owner] reviews this policy [every year] and whenever we add a system, an app or a store.

9.2 Signed by the employee and approved by the dealership

Employee name _____ Employee signature _____ Date _____

Approved by (name and title) _____ Signature _____ Date _____

Finished the policy?
A complimentary IT and cybersecurity assessment reviews your current technology and where the store stands against the FTC Safeguards Rule, and puts the findings in a written report.

heliontechnologies.com/it-assessment/

BYOD policy template from Helion Technologies. A starting point, not legal advice. The final policy is the dealership's own. © 2026 Helion Technologies.