Mobile devices: what to control on work and personal phones?

This month, require a compliant device or Intune app protection for every phone that reaches work data, and set a date to block iOS older than the previous major release and Android older than 14. Then manage company phones fully, protect only work apps on personal ones and harden high-risk users' phones.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.1**

Written for

IT teams of any size in the EU and Germany managing company phones and work data on personal ones, mostly with Intune, some with Jamf or Google

Latest version

sheets.einblick.dev/mobile-devices/

If you only do five things

1. **Gate every phone in Conditional Access.** Require a compliant device or app protection. Give every device a compliance policy, then set **Mark devices with no compliance policy assigned as** to Not compliant; by default they count as compliant[2].
2. **Block outdated OS versions.** Allow the current and previous iOS major release[3] and Android 14 or later, the oldest Google still patches[21]. Set a cutoff date first.
3. **Keep work data in managed apps.** Use Level 2 app protection, as the endpoints and email sheet says, and, going beyond Level 2, block **Sync policy managed app data with native apps or add-ins**[6]; it also stops Outlook add-ins. WhatsApp can upload the address book regularly[28].
4. **Harden high-risk users' phones.** Enroll first, then turn on Lockdown Mode or Advanced Protection: a phone in Lockdown Mode can't enroll, and MDM can't turn it on[14].
5. **Require two admins to wipe phones.** Multi Admin Approval makes a second admin approve each wipe, retire and delete[10], so one stolen admin account can't wipe the fleet. See also the privileged access sheet.

Choose the model for each phone

1. **Does the company own it?** Enroll it supervised or fully managed via Apple Business or Android zero-touch. Only supervised iPhones can block marketplaces[18].
2. **Personal, with only Microsoft 365 apps?** Use app protection without enrollment. IT manages, and can wipe, only the work data in those apps[5]; the joiners and leavers sheet covers offboarding.
3. **Personal, but needs Wi-Fi, VPN or certificates?** Use an Android work profile, which keeps personal apps and data outside Intune[7], or Apple User Enrollment, where Intune collects no serial number, IMEI or phone number[8].
4. **Is the user at high risk?** Issue a company phone with Level 3 policies, which add mobile threat defense[3].
5. **Is it written down?** The BSI requires a policy on who may reach which data from phones[25]. In Germany, agree with the works council what IT can see[30].

Versions, patches and end of support

- **Enforce iPhone updates with declarative management.** Use Intune's **Software Update Enforce Latest** with a delay of a few days. It needs device or automated enrollment[9]; elsewhere, block access.
- **Move every iPhone off iOS 18.** Apple's October 2026 iOS 18 update covered only the iPhone XS, XS Max, XR and iPad 7th generation[17].
- **Set an Android patch floor you can keep.** Check that your devices get updates first[4], then block patches older than 6 months and tighten toward 90 days.
- **Buy for the support period, retire on time.** For phones placed on the EU market since 20 June 2025, makers that issue OS updates must offer them for at least 5 years after the model leaves the market[24]. The BSI requires replacing devices that no longer get updates[25].

High-risk users and mercenary spyware

- **Lockdown Mode** blocks most message attachments, link previews, complex web technologies, FaceTime from people not called in 30 days, 2G and 3G, and new configuration profiles[14].
- **Advanced Protection** blocks sideloading and unauthorized USB access while locked, and reboots phones locked for 72 hours. Turn on its Intrusion Logging too[20].
- **Treat threat notifications as incidents.** Apple's arrive on the iPhone and by email, never ask you to click a link and show at account.apple.com[15]; bring in your incident response provider. Google Workspace alerts admins to government-backed attacks[22].

App stores, sideloading and messaging

- **EU app marketplaces.** Notarization is only a baseline check, and Apple can't help with scams in those apps[16]. Block them on supervised iPhones with the `allowMarketplaceAppInstallation` and `allowWebDistributionAppInstallation` restrictions[18]; on personal ones, rely on app protection.
- **Android sideloading.** Block unknown sources, even in the personal profile, as Microsoft's Level 2 examples do[4].
- **Name one work messenger.** Without guidance, staff may turn to insecure channels such as SMS[27]. The security awareness sheet covers vishing.

Lost phones, SIM swaps and eSIMs

- **Report, lock, remove sign-ins.** The BSI requires reporting a lost device at once[25]. Lock it in Intune[11] or wipe work apps' data[5], then remove its passkeys (see the passkeys and MFA sheet).
- **Block resets on company phones.** Disable **Erase All Content and Settings** on supervised iPhones[18] and **Factory reset** on managed Android[12].
- **Make SIM swaps harder.** Most carriers ENISA surveyed check callers with personal details such as date of birth[29]. Set a password on the business account and block eSIM changes on supervised iPhones[18]. If the signal vanishes, call the carrier at once[29].

What changed in 2026

- **iOS 27 dropped the old MDM update restrictions.** Since 14 September 2026[17], update deferrals work only through declarative device management[18].
- **The approved client app grant is read-only.** Since 30 June 2026, admins can't create or edit policies with it; existing ones still apply. Use Require app protection policy[1].
- **Spyware vendors overtook state spies.** For 2025, Google attributed more zero-days to them than to state espionage groups, a first, and counted 15 mobile zero-days, up from 9[23].
- **EU iPhones can forward notifications to third-party accessories.** Since iOS 26.5 in May 2026, companion apps can receive them[17,19]; set **Org data notifications** to Block Org Data, which covers wearables[6].

What you can skip

- **Mobile antivirus for everyone.** The NCSC says iOS and Android don't need it in their default configuration[26]; Level 3 adds threat defense[3].
- **Full enrollment of personal phones.** A work profile or app protection covers most needs.
- **Lockdown Mode for all staff.** Apple built it for the very few people personally targeted[14].
- **Passcode expiry and long passcodes.** Microsoft's Level 2 examples use 6 digits and no expiry; only Level 3 adds yearly expiry[3,4].

Mistakes that cost the most

- **Exempting executives.** They need the strictest policies, not exceptions.
- **Accepting rooted or uncertified Android phones.** Require Play Integrity's device integrity check, and strong integrity where all phones support it[4].
- **Showing message previews on the lock screen.** The BSI requires hiding confidential information there[25].
- **Turning on Android web enrollment in a passkey-only tenant.** Users can't complete it yet, and the setting can't be reversed[7].

What this looks like at your size

Small team, no security staff

- Protect personal phones with app protection; enroll only company phones.
- Buy company phones from resellers that register them in Apple Business or Android zero-touch.
- Raise the minimum OS versions each quarter.

Growing, with IT or security staff

- Supervise every company iPhone; block marketplaces and eSIM transfers.
- Report weekly on OS versions, patch levels and devices without a policy.
- On Jamf, feed compliance to Entra ID through Intune's partner integration[13].

Enterprise or regulated

- Keep a named high-risk group on company phones with Level 3 policies.
- Pilot mobile threat defense for that group.
- Where regulators expect records, choose an enterprise messenger with audit[27].

Version history

5 Nov 2026, version 1.1	Reviewed for company readers: lost phones are locked in Intune or have work data wiped instead of using consumer Find My pages, company phones block resets through MDM restrictions instead of user-enabled theft protection, and Access Now is dropped because it serves civil society only.

Sources

1. Migrate approved client app to app protection policy. Microsoft Learn, 29 May 2026. learn.microsoft.com
2. Device compliance policies in Intune. Microsoft Learn, 2 Jul 2026. learn.microsoft.com
3. iOS/iPadOS device compliance security configurations. Microsoft Learn, 20 Mar 2025. learn.microsoft.com
4. Security configurations for Android work profiles. Microsoft Learn, 26 Mar 2025. learn.microsoft.com
5. Data protection framework using app protection policies. Microsoft Learn, 12 Jun 2025. learn.microsoft.com
6. iOS/iPadOS app protection policy settings. Microsoft Learn, 18 Nov 2025. learn.microsoft.com
7. Android Enterprise work profile enrollment. Microsoft Learn, 18 Jun 2026. learn.microsoft.com
8. Overview of Apple User Enrollment in Intune. Microsoft Learn, 19 Aug 2024. learn.microsoft.com
9. Configure update policies for Apple devices. Microsoft Learn, 24 Feb 2026. learn.microsoft.com
10. Use Multi Admin Approval in Intune. Microsoft Learn, 30 Jul 2026. learn.microsoft.com
11. Intune Lost mode. Microsoft Learn, 27 Oct 2025. learn.microsoft.com
12. Android device restrictions. Microsoft Learn, 2 Oct 2026. learn.microsoft.com
13. Third-party device compliance partners. Microsoft Learn, 24 Jun 2026. learn.microsoft.com
14. About Lockdown Mode. Apple Support, 14 Sep 2026. support.apple.com
15. About Apple threat notifications. Apple Support, 13 Aug 2026. support.apple.com
16. About alternative app distribution. Apple Support, 26 Oct 2026. support.apple.com
17. Apple security releases. Apple Support, 30 Oct 2026. support.apple.com
18. Restrictions (Device Management). Apple Developer, checked 5 Nov 2026. developer.apple.com
19. Accessory Notifications. Apple Developer, checked 5 Nov 2026. developer.apple.com
20. Improve device security with Advanced Protection for Android. Android Help, checked 5 Nov 2026. support.google.com
21. Android Security Bulletin, November 2026. Android Open Source Project, 2 Nov 2026. source.android.com
22. Government-backed attack alerts. Google Workspace Help, updated 26 Oct 2026. knowledge.workspace.google.com
23. Look What You Made Us Patch: 2025 Zero-Days in Review. Google Threat Intelligence Group, 5 Mar 2026. cloud.google.com
24. Regulation (EU) 2023/1670 (ecodesign for phones). EUR-Lex, 16 Jun 2023. eur-lex.europa.eu
25. SYS.3.2.1 Allgemeine Smartphones und Tablets. BSI, Edition 2023. bsi.bund.de
26. Antivirus and other security software. NCSC (UK), reviewed 13 May 2025. ncsc.gov.uk
27. Choosing enterprise instant messaging. NCSC (UK), 13 May 2025. ncsc.gov.uk
28. WhatsApp Privacy Policy (EEA). WhatsApp, 2 Jul 2026. whatsapp.com
29. Countering SIM-Swapping. ENISA, Dec 2021. enisa.europa.eu
30. BetrVG, § 87. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de