Personal Device Security for Medium- to High-Risk Work

A personal device isn't set up the way a work laptop is. Nobody's checked that it's locked down, up to date, or free of other apps and accounts mixed in with work stuff. You can't turn it into a full company laptop that's not realistic. What you can do is either keep the sensitive work in a separate, protected space on the device that can be wiped if needed, or avoid putting it on the device at all.

The basics

Control	What it means	Why it matters
Encryption	Turn on full-disk encryption (BitLocker on Windows, FileVault on Mac) and ensure it's on	Phones and laptops don't always come encrypted by default
Screen lock	Auto-lock after 5 minutes or less, with a PIN/password or fingerprint/face unlock	Stops someone from just picking up an unlocked device and looking through it
Keep devices and browsers updated	Turn on automatic updates	Most break-ins happen through known holes that a software update would close
Two-factor login	Require a second step (code, key, or app approval) to log in anywhere sensitive	A stolen password alone shouldn't be enough to get into anything important
Separate work space	Use a work profile or separate browser profile that keeps work stuff separate from personal photos, texts, apps	Lets the work data get wiped without touching anything personal on the device
No random file syncing	Don't let personal Dropbox, personal Google Drive, etc. touch work files	Keeps sensitive files from quietly ending up in the wrong place
Remote wipe	Make sure the work data can be wiped remotely if the device is lost, using Google Workspace, MS 365 or another service	Losing a device only becomes a real problem if the data on it is still readable

Quick test: if your device were lost tonight, could whoever found it get into sensitive records, passwords, or personal info? If yes, it needs all of the above before it's used for work.

Putting it into practice

New staff: A new staffer's device should meet the basics above before it's allowed anywhere near sensitive work. Check that encryption is on and the software is current.

Handling the data: For medium-risk work, a separate work profile with some basic restrictions (no copying files out, no plugging in random USB drives) is usually enough. For high-risk work, it's better if the sensitive data never lands on the device at all. Access it through a browser-based tool or remote desktop instead.

By how sensitive the work is:

	Medium-risk work	High-risk work
Where the data lives	In a separate work space on the device	Nowhere on the device - accessed remotely only
Copying or downloading files	Restricted	Not allowed
Staying logged in	Fine day-to-day, re-verify for sensitive actions	Log back in often

If a device is lost, stolen, or acting weird

Wipe the work data remotely right away. Cut off that device's access and log it out everywhere. Look back through recent activity on the account for anything unusual. Report it right away.

Revision #1
Created 20 July 2026 12:41:54 by Josh
Updated 20 July 2026 12:51:16 by Josh