TOMORIS
MORE THAN IT

FREE DOWNLOAD

TEMPLATE · TOMORIS TOOLBOX

Smartphones and Tablets: Policy for Company and Personal Devices

Model text with placeholders for company devices and BYOD, minimum requirements based on BSI SYS.3.2.1 and NIST SP 800-124, implementation with Microsoft Intune

UPDATED
Oct 25, 2026

LENGTH
PDF, 12 pages

ONLINE
tomoris.com/en/downloads/mobile-geraete-richtlinie-vorlage

AT A GLANCE

A1
Policy before deployment: BSI SYS.3.2.1.A1

2
Variants: company devices only or BYOD as well

Never
Does Intune see personal photos, emails, contacts

30 days
Offline, then delete company data (Microsoft)

WHO IT IS FOR

- IT management and administrators who approve and secure company and personal devices for email, chats, and files
- HR departments that coordinate use, loss, and departure with the employment contract, data protection, and the works council
- Executive management of small and medium-sized companies that approves the policy and is responsible for it

Adaptation for your own use permitted; redistribute unchanged

WHAT THIS COVERS

Anyone who allows smartphones or tablets to be used for work data needs a policy first; in IT-Grundschutz, the BSI requires it as basic requirement SYS.3.2.1.A1. This template contains model text with placeholders for company devices and, as a variant, for personal devices (BYOD): approval, minimum requirements for updates, screen lock, and encryption, apps, loss and theft, return upon departure. It shows how work and personal data can be separated with app protection policies or a work profile without managing the entire personal device, and what IT can and cannot see in the process.

This template must be adapted to your company, your devices, and your MDM and does not replace legal advice, in particular not on the ArbVG, AVRAG, and GDPR; the statutory text in its current version is authoritative. IT-Grundschutz and NIST are recommendations, not legal obligations. Microsoft features, names, menus, and licenses may change.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01 What the policy is for 2
02 Company device or personal device: the variants 3
03 What IT sees on personal devices 4
04 Minimum requirements for every device 5
05 Implementation with Microsoft Intune and Entra ID 6
06 Loss, theft, and departure 7
07 Model text, part 1: scope, approval, and minimum requirements 8
08 Model text, part 2: personal devices, loss, and return 9
09 Checklist: introducing the policy 10
10 Sources 11

01

What the policy is for

What BSI and NIST require of a policy for smartphones and tablets and how binding this is.

Smartphones and tablets are more easily lost than an office computer and are used in places the company does not control (NIST SP 800-124 Rev. 2, 3.1.2). The IT-Grundschutz Compendium of the German BSI (Edition 2023) sets out a basic requirement: before an institution uses smartphones or tablets, it MUST define a policy for the use and control of the devices, including who may access which information with them (SYS.3.2.1.A1). The module applies to all devices used for work; its threat landscape explicitly also mentions personal devices (BYOD).

A binding policy for employees SHOULD govern use, care, storage, and loss reporting and prohibit removing management software, rooting the device, or changing security settings (SYS.3.2.1.A10). Anyone who uses mobile device management (MDM) MUST define a written strategy that also governs the operating model: personal devices, personally assigned or shared company devices (SYS.3.2.2.A1).

> Mandatory or recommended? In Austria, IT-Grundschutz and NIST are not laws but recognized standards. The BSI divides requirements into basic (B), standard (S), and requirements for elevated protection needs (H); within each requirement, MUST is to be met unconditionally, and SHOULD may only be deviated from after careful consideration and with sound justification. The template is a TOMORIS recommendation. The main legal requirements to observe are the GDPR, the ArbVG, and the AVRAG (section 03), and for NIS2 entities also § 32 para. 4 lit. i NISG 2026 (section 06).

02

Company device or personal device: the variants

Which operating models exist, who owns the device and the data, and how company data can be separated on personal devices.

Operating models according to NIST SP 800-124 Rev. 2 (5.1.3); variant A of the template allows company devices only, variant B also personal devices

MODEL	OWNERSHIP	TYPICAL MANAGEMENT
Company device for work use only	Device and all data: company	Fully managed, only approved apps (allowlist)
Company device with personal use (COPE)	Device and data: company, even with personal use	Managed, official app stores, blocklist for apps
Personal device (BYOD), including from a company device list (CYOD)	Device: employee; company data on it: company	Company apps and data only; app management (MAM) instead of device management can ease privacy concerns (4.2.2)

Three ways to separate company data on personal devices (Microsoft Intune example)

App protection policies without enrollment (MAM)	Intune protects company data in apps such as Outlook, Word, or OneDrive without enrolling the device, only when the app is used with the company account; personal accounts remain unaffected. Certificates, Wi-Fi, and VPN are not deployed; on Android, the Company Portal is required.
Android: personally owned work profile	A separate partition at the operating system level for company apps and data that Intune manages; certificates, Wi-Fi, and VPN can be deployed. Microsoft recommends the work profile if you need such MDM features, otherwise MAM; both can be combined.
iPhone and iPad: account-driven user enrollment	From iOS/iPadOS 15, the person adds their company account in Settings under "VPN & Device Management". Company data is stored on a separate volume and in managed apps, separate from personal data; Intune has only limited functions, for example VPN only per app.

For BYOD, the BSI warns that a wipe via MDM can also affect personal data and that company data may be viewed without authorization during a repair or remain on the device in an unregulated way upon departure (SYS.3.2.1, threat 2.9). TOMORIS recommendation: for personal devices, app protection policies are sufficient in many SMEs; enrollment is worthwhile if certificates, Wi-Fi, or VPN profiles are needed. According to NIST, very restrictive requirements or requirements that appear to be monitoring can tempt employees to resort to shadow IT (3.1.13).

03

What IT sees on personal devices

Which data Intune, according to Microsoft, never, always, or only under certain circumstances sees, and what HR and the works council need to clarify.

With app protection policies and the Android work profile, administrators, according to Microsoft, can neither read nor delete data that belongs to or is controlled by the users. The table shows what the organization sees for a device enrolled in Intune; for other MDM products, check the vendor's information.

What the organization sees for enrolled devices (Microsoft Learn, as of August 20, 2026)

INFORMATION	COMPANY DEVICE	PERSONAL DEVICE
Calls, browsing history, emails, text messages, contacts, calendar, passwords, photos, personal documents	Never	Never
Owner, device name, model, manufacturer, operating system and version	Yes	Yes
Serial number and IMEI	Yes	Yes; not with Apple user enrollment
Phone number	Full; on Android with a work profile, the last four digits	The last four digits; not with Apple user enrollment
Location	Only if lost; iPhone and iPad then show a notice on the lock screen	No
Installed apps	All; on Android with a work profile, only those in the work profile	The managed apps, more depending on configuration

For HR: control measures and technical systems for monitoring employees that affect human dignity require the consent of the works council (§ 96 para. 1 no. 3 ArbVG). Systems that collect, process, or transmit employee data by automated means beyond general personal information and professional qualifications also require its consent, insofar as their use goes beyond obligations arising from law, collective agreements, or the employment contract; this consent can be replaced by the arbitration board (§ 96a para. 1 no. 1 and para. 2 ArbVG). Without a works council, control measures that affect human dignity are only permitted with the consent of the employee (§ 10 para. 1 AVRAG). Whether this applies to your configuration must be clarified case by case; this note does not replace legal advice.

Before enrollment, provide information on purposes and legal basis, recipients, and retention period (Art. 13(1)(c) and (e) and (2)(a) GDPR), name the device data collected, and collect only what is necessary (Art. 5(1)(c) GDPR). According to NIST, location data should only be used with consent and a clear description (3.1.11); geofencing creates movement profiles and can be misused for impermissible monitoring (BSI SYS.3.2.2, threat 2.4).

04

Minimum requirements for every device

Updates, screen lock, encryption, apps, and interfaces, with the citation in IT-Grundschutz.

Technical minimum requirements (B, S, H = requirement category; SHOULD parts in basic requirements are marked)

AREA	REQUIREMENT	BASIS
Updates	Check the manufacturer's update period at procurement, retire devices without security updates, stop using such apps (SHOULD); deploy updates promptly, for example weekly, first to a pilot group	SYS.3.2.1.A5 (B); NIST 4.3.6
Screen lock	Reasonably complex passcode, automatic lock after a short time, no confidential content on the lock screen; reset after several failed attempts (SHOULD); biometrics only if they protect at least as well	SYS.3.2.1.A4 (B), A18 (S)
Encryption	Encrypt device storage and SD cards containing sensitive data	SYS.3.2.1.A11 (S)
Apps	Define permitted sources, technically prevent others; only approved apps (SHOULD)	SYS.3.2.1.A8 (B)
Tampering	No rooting or jailbreak; detect and block tampered devices	SYS.3.2.1.A10 (S); SYS.3.2.2.A17 (H); Microsoft, level 1
Permissions and interfaces	Restrictive app access to camera, microphone, location, and health data; turn off unneeded functions and interfaces (SHOULD)	SYS.3.2.1.A3, A6 (B), A16 (S)
Cloud services	Define which cloud services are permitted for company data and whether for personal use	SYS.3.2.1.A2 (B)

The BSI does not specify concrete values such as the lock time or passcode length; the model text contains TOMORIS suggestions for these. On personal devices without enrollment, app protection policies check, for example, the minimum operating system version, jailbreak or root, and on Android the device lock when the company app starts, and otherwise block access (Microsoft, data protection framework).

05

Implementation with Microsoft Intune and Entra ID

Licenses, app protection policy, Conditional Access, and enrollment in four steps.

1 **Clarify licenses and roles**

App protection policies: one Microsoft Entra account per user with an assigned Intune license; for Outlook, additionally an Exchange Online mailbox with a Microsoft 365 license, for Word, Excel, and PowerPoint Microsoft 365 Apps for Business or Enterprise. App-based Conditional Access: Microsoft Entra ID P1 or P2, also for the users covered; Security Administrators and Conditional Access Administrators can set it up.

2 **Create app protection policies**

In the Microsoft Intune admin center, one policy each for iOS/iPadOS and Android. For most mobile users, Microsoft recommends level 2 of its data protection framework: encrypt organization data, PIN, block backups, copies only in OneDrive for Business, SharePoint, and the photo library, cut and copy only into managed apps (pasting into company apps remains allowed), minimum operating system version, delete company data after 30 days offline, block jailbroken or rooted devices.

3 **Require Conditional Access**

Only once the app protection policies apply: in the Microsoft Entra admin center under Entra ID › Conditional Access › Policies, require the grant "Require app protection policy" for all users and resources on Android and iOS, exclude an emergency account, and test first in "Report-only" mode. "Require approved client app" has been read-only since June 30, 2026: policies using it can no longer be created or edited, only disabled or deleted; existing ones continue to work. The devices register in Entra ID via Microsoft Authenticator (iOS) or the Company Portal (Android).

4 **Enroll devices**

Enroll company devices in the MDM in factory state before handing them out (SYS.3.2.2.A4), for example via Apple's automated device enrollment or Android zero-touch (NIST 5.3.4.2). Personal devices via the Android work profile, Apple user enrollment, or only with app protection policies.

Decide on deviations deliberately: the BSI recommends managing smartphones and tablets via MDM (SHOULD, SYS.3.2.1.A32); module SYS.3.2.2 does not cover BYOD. Anyone who secures personal devices only with app protection policies justifies this in a comprehensible way and documents it, for example in the security concept. To enforce app protection policies, Microsoft advises using Conditional Access. Menus and names: Microsoft Learn, October 2026.

06

Loss, theft, and departure

What to do immediately, which wipe action suits which device, and what happens upon departure.

Procedure in case of loss or theft

Immediately

Report

The person immediately reports the loss or unauthorized changes to the device and software to the responsible contact (SYS.3.2.1.A7).

Then

Block and wipe

IT blocks access to company data and wipes remotely: company devices completely, personal devices only the company data (NIST 4.3.3, 4.3.11).

Within 72 h

Check data protection

If personal data was affected, the breach must be reported to the supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it, unless it is unlikely to result in a risk (Art. 33(1) GDPR); every breach is documented (para. 5).

Wipe actions in Microsoft Intune

ACTION	WHAT IT REMOVES	SUITABLE FOR
Wipe	The entire device to factory settings, all user data and settings	Enrolled company devices
Retire	Managed apps, settings, and profiles, and for the Android work profile its entire content; personal data remains	Enrolled personal devices
Selective wipe	Only the company data in apps with an app protection policy, as soon as the app runs	Personal devices without enrollment

> Remote wipe alone does not protect: with the built-in tools of iOS and Android, it only works when the device is on and connected, and attackers can extract data beforehand (NIST 4.3.3). Passcode and encryption are the first layer of protection. Never wipe personal devices completely without consent; according to NIST, deleting data that does not belong to the company can cause legal problems (4.3.12).

Upon departure, IT resets returned company devices to factory settings before passing them on. This does not erase SIM and SD cards: remove and erase SD cards, handle SIM cards according to the rules on the phone number; for disposal, NIST recommends removing and destroying both (5.5). After decommissioning, no sensitive data should remain on the device or storage media (SYS.3.2.2.A22).

NIS2 entities: § 32 para. 4 lit. i NISG 2026 requires measures for human resources security, access control, and asset management. This is specified in annex point 12 of Implementing Regulation (EU) 2024/2690, which § 2 NISV 2026 (Austrian NIS Regulation 2026) makes applicable to all essential and important entities: under point 12.5, the handover, return, or deletion of assets such as devices at the end of employment must be regulated and documented; otherwise, they must no longer be able to access the systems.

07

Model text, part 1: scope, approval, and minimum requirements

Sections 1 to 5. Replace everything in square brackets and choose variant A or B.

Replace the placeholders in square brackets, choose one option where alternatives are separated by |, and delete what does not apply; in variant A (company devices only), § 6 is omitted. Numbers such as [5] minutes are TOMORIS suggestions ([30] days offline is Microsoft's value from level 2); rules without a citation are organizational additions by TOMORIS. Coordinate the text with data protection, HR, and, if there is one, the works council.

Policy for smartphones and tablets of [Company], version [version] of [MM/DD/YYYY]

§ 1 Purpose and scope	This policy governs the use of smartphones and tablets for work at [Company]. It applies to all employees and [external persons, e.g., temporary agency workers], to company devices, and to every device used to access work emails, files, chats, or applications. [Name, role] is responsible; the point of contact is [IT team, contact] (SYS.3.2.1.A1).
§ 2 Approved devices	Variant A: Work data may only be processed on company devices that [Company] has procured and enrolled in [MDM, e.g., Microsoft Intune]. Variant B: In addition, personal devices are permitted if they meet § 3 and are integrated in accordance with § 6; [rules on costs and phone plan]. Approved are [operating systems and minimum versions] (SYS.3.2.2.A2).
§ 3 Minimum requirements	Every device with work data still receives security updates from the manufacturer; you install offered updates within [7] days. A passcode of at least [6] digits protects the device; it locks after no more than [5] minutes and shows no preview of confidential messages on the lock screen. Biometrics only after approval by [IT team]. Storage is encrypted; rooting or jailbreaking is prohibited. Devices that do not meet these requirements receive no access (SYS.3.2.1.A4, A5, A10, A11, A18).
§ 4 Apps and cloud services	On company devices, you install apps only from [the Apple and Google app stores | the Company Portal]. You edit work data only in the apps listed in Annex 1 with your company account and store it only in [OneDrive for Business, SharePoint]; private cloud storage, messengers, and email accounts are not permitted for this. Apps receive only the necessary permissions, for example for camera, microphone, or location (SYS.3.2.1.A2, A6, A8).

§ 5 Personal use of company devices	[Company devices are for work purposes only. | Personal use is permitted to a limited extent, personal apps only from the official app stores.] The device and company data remain the property of [Company]. You back up personal data yourself; in the event of loss and upon return, the device is wiped completely. You do not change management software or security settings (SYS.3.2.1.A10).

08

Model text, part 2: personal devices, loss, and return

Sections 6 to 10, Annex 1 on approved apps, and the acknowledgment for signature.

§ 6 Personal devices (variant B only)	On personal devices, [Company] protects only company apps and company data with [app protection policies | Android work profile | Apple user enrollment]; personal apps and data remain unmanaged. Company data stays in these apps; copying into personal apps and personal backups are blocked. The company apps require [a PIN]; after [30] days offline, their company data is deleted. Before a repair, have [IT team] remove the company data.
§ 7 Data protection	On personal devices, [Company] sees only [information from the table in section 03 depending on the method, for enrollment, for example, owner, device name, model, operating system, serial number, IMEI, last four digits of the phone number, managed apps], but not call and browsing history, emails, text messages, contacts, calendar, passwords, photos, personal documents, or location. [IT team] retrieves the location of a company device only if it is lost. [No monitoring of performance or behavior takes place.] Details: [privacy notice, works agreement].
§ 8 Loss, theft, suspicion	Report loss, theft, or suspected tampering immediately to [IT team, phone, also outside working hours] (SYS.3.2.1.A7). [IT team] then blocks access and wipes remotely: company devices completely, personal devices only the company data. In addition, report a theft to the police. Do not leave devices unattended, for example visible in the car (storage, SYS.3.2.1.A10).
§ 9 Return and departure	You return company devices including accessories to [contact] no later than on [last working day]; back up personal data beforehand, after which the device is reset to factory settings. [Rules on the phone number]. On personal devices, [IT team] removes company data and management; personal data is retained. Return and deletion are documented (SYS.3.2.2.A6, A22; NIS2: annex point 12.5 Implementing Regulation (EU) 2024/2690).
§ 10 Exceptions, violations, review	[Name, role] approves exceptions in writing and for a limited time. In the event of violations, [IT team] may block the device's access to company data; [further consequences, coordinated with HR and the works council]. [Contact] reviews the policy and settings at least [annually] and before new operating system versions (SYS.3.2.2.A20). Valid from [MM/DD/YYYY], approved by [Name, role].

Annex 1: Approved apps and storage locations (example row in square brackets)

APP OR SERVICE	PURPOSE	COMPANY DEVICE	PERSONAL DEVICE
[e.g., Outlook]	[Email, calendar]	[Yes]	[Yes, with app protection]
_____	_____	_____	_____
_____	_____	_____	_____

Acknowledgment per person and device (does not replace a works agreement or consent under § 10 AVRAG)

ITEM	ENTRY
Name, department	_____
Company device with inventory number or personal device with model	_____
Policy received and read: date, signature	_____
For [Company]: name, date, signature	_____

09

Checklist: introducing the policy

Ten steps from taking stock to regular review.

- [ ] Take stock of which devices access email, chats, and files today (NIST 5.1.2); decide on variant A or B and on personal use of company devices (SYS.3.2.2.A1).
- [ ] Define approved devices and minimum versions, check the update period at procurement (SYS.3.2.2.A2, SYS.3.2.1.A5).
- [ ] Check licenses: Microsoft Intune, Microsoft Entra ID P1 or P2.
- [ ] Involve HR and the works council, clarify a works agreement or consent (§§ 96, 96a ArbVG, § 10 AVRAG).
- [ ] Prepare a privacy notice (Art. 13 GDPR) and adapt the privacy text in the Company Portal.
- [ ] Set up app protection policies (level 2), test Conditional Access first in "Report-only" mode, then turn it on.
- [ ] Start with a small pilot group, then roll out to everyone (NIST 5.3.6).
- [ ] Train employees: phishing, updates, apps from trusted sources, which data is collected (NIST 4.3.10).
- [ ] Set up a reporting channel for losses, practice wipe actions on a test device, add to the departure process.

- [ ] Review the policy and settings [annually] and before new operating system versions (SYS.3.2.2.A20).

The checklist and model text are TOMORIS recommendations. The obligations cited from the GDPR, ArbVG, and AVRAG are required by law, and for NIS2 entities additionally those from § 32 para. 4 lit. i NISG 2026, § 2 NISV 2026, and annex point 12.5 Implementing Regulation (EU) 2024/2690.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)
tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

10

Sources

All statements are supported by sources. Legislation applies in its current version.

1 **BSI IT-Grundschutz Compendium, Edition 2023 (complete PDF)**
Chapter on the structure of the modules and modal verbs; accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...

2 **BSI IT-Grundschutz, Edition 2023: SYS.3.2.1 General Smartphones and Tablets**
1.3, 2.9, A1 to A8, A10, A11, A16, A18, A32; accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...

3 **BSI IT-Grundschutz, Edition 2023: SYS.3.2.2 Mobile Device Management**
1.3, 2.4, A1, A2, A4, A6, A17, A20, A22; accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...

4 **NIST SP 800-124 Rev. 2: Security of Mobile Devices in the Enterprise**
3.1.2, 3.1.11, 3.1.13, 4.2.2, 4.3.3, 4.3.6, 4.3.10 to 4.3.12, 5.1.2, 5.1.3, 5.3.4.2, 5.3.6, 5.5
doi.org/10.6028/NIST.SP.800-124r2

5 **Microsoft Learn: App protection policies overview**
Benefits, devices without enrollment, requirements, wipe
learn.microsoft.com/de-de/intune/app-management/protection/over...

6 **Microsoft Learn: Data protection framework using app protection policies**
Level 1 and 2, conditional launch; accessed October 25, 2026
learn.microsoft.com/de-de/intune/app-management/protection/data...

7 **Microsoft Learn: What information can my organization see?**
Never, always, and possibly visible; as of August 20, 2026
learn.microsoft.com/de-de/intune/user-help/enrollment/data-visi...

8 **Microsoft Learn: Apple user enrollment in Intune**
Methods, settings, limitations; as of August 20, 2026
learn.microsoft.com/de-de/intune/device-enrollment/apple/user-e...

9 **Microsoft Learn: MAM and personally owned work profiles (Android)**
Privacy, scenarios, summary; as of August 19, 2026
learn.microsoft.com/de-de/intune/app-management/protection/mam-...

10 **Microsoft Learn: App-based Conditional Access with Intune**
Licenses, roles, how it works; as of August 20, 2026
learn.microsoft.com/de-de/intune/device-security/conditional-ac...

11 **Microsoft Learn: Migrate approved client app to app protection policy**
Read-only from June 30, 2026, policy for mobile devices; as of June 1, 2026
learn.microsoft.com/de-de/entra/identity/conditional-access/mig...

12 **Microsoft Learn: Retire device action**
Platforms, user experience; as of August 20, 2026
learn.microsoft.com/de-de/intune/device-management/actions/reti...

13 **ArbVG, current daily version in the RIS**
§ 96 para. 1 no. 3, § 96a para. 1 no. 1 and para. 2; accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

14 **AVRAG, § 10 Control measures, RIS**
§ 10 para. 1; accessed October 25, 2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...

15 **Regulation (EU) 2016/679 (GDPR), EUR-Lex**
Art. 5(1)(c), Art. 13(1) and (2), Art. 33(1) and (5)
eur-lex.europa.eu/eli/reg/2016/679/oj/deu

16 **Implementing Regulation (EU) 2024/2690, EUR-Lex**
Annex points 12 and 12.5; applicable under § 2 NISV 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu

17 **NISG 2026, § 32 Risk management measures, RIS**
§ 32 para. 4 lit. i, valid from October 1, 2026; accessed October 25, 2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...

18 **NISV 2026, BGBl. II No. 290/2026, RIS**
§ 2, promulgated on October 1, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290