B to B - Praxistools für Unternehmen und Freiberufler

knowNOW
TOOLS FOR BUSINESS SUCCESS

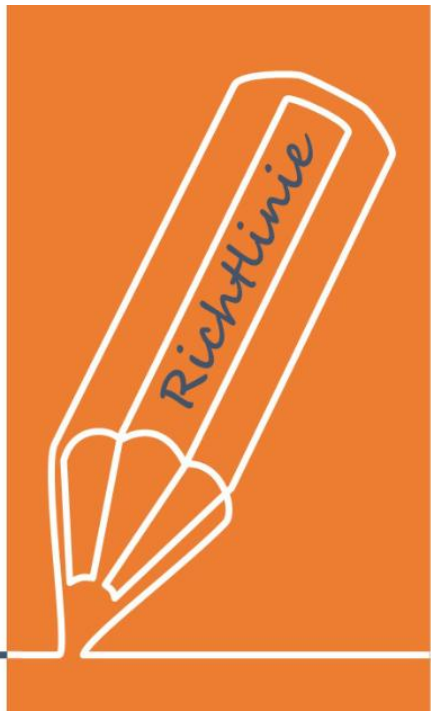
Richtlinie mobiles Arbeiten

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Richtlinie mobiles Arbeiten

des Unternehmens



Inhaltsverzeichnis

1. Zweck und Zielsetzung

Diese Richtlinie wurde erstellt, um flexible Arbeitsmodelle in Unternehmen zu fördern und trotzdem die IT-Sicherheit und Produktivität zu gewährleisten. Mobiles Arbeiten umfasst Tätigkeiten aus dem Homeoffice, von unterwegs in einem Café oder innerhalb unseres Unternehmens, mit wechselnden Standorten.

Der Zweck dieser Richtlinie zum mobilen Arbeiten ist es, mobile Endgeräte innerhalb und außerhalb unseres Unternehmens so zu betreiben, dass die auf diesen Geräten gespeicherten Daten nicht durch unbefugte Dritte genutzt werden können.

Im Zusammenhang mit mobilen Endgeräten gibt es verschiedene potenzielle IT-Vorfälle, die sowohl durch menschliches Fehlverhalten als auch durch technische Schwachstellen verursacht werden können. Nachfolgend sind einige typische zu vermeidende Vorfälle und deren Auswirkungen aufgelistet, die spezifisch für mobiles Arbeiten sind:

- Verlust oder Diebstahl des mobilen Endgerätes, mit der möglichen Offenlegung vertraulicher Daten, die auf dem Gerät gespeichert sind.
- Abfangen von Daten während der Übertragung, was zur Offenlegung vertraulicher Informationen führen kann.
- Kompromittierung von Zugangsdaten, was unbefugten Zugriff auf Systeme ermöglicht.
- Potenzielle Sicherheitslücken durch Installation unautorisierter Software oder versehentlichen Datenzugriff, was unbefugten Zugriff auf Systeme ermöglicht.
- Versehentliche Speicherung vertraulicher Daten außerhalb des Unternehmensnetzwerks, was potenziellen Datenverlust bedeuten kann.
- Nutzung des Dienstgeräts durch Dritte (Familienangehörige oder Freunde), die unbewusst Sicherheitsrisiken schaffen.
- Nichtdurchführung einer Mobilgeräts ohne sichere Datenlöschung.

Da mobile Endgeräte in wechselnden Umgebungen eingesetzt werden, stellen diese eine Verbindung zwischen unserem internen Unternehmensnetz und externen IT-Netzen dar. Ein nicht ausreichend geschütztes oder in fahrlässiger Weise genutztes mobiles Gerät kann somit zur Kompromittierung unserer IT-Infrastruktur führen.

2. Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten, Dienstleister und alle anderen relevanten Anwender, die auf die auf sicherheitsrelevante Bereiche unserer IT-Systeme und geschützten Informationen des Unternehmens mit mobilen Endgeräten zugreifen.

Wichtiger Hinweis:
Die Nutzung der mobilen Endgeräte ist ausschließlich zu dienstlichen, bzw. zu dienstlich veranlassten Zwecken gestattet. Falls Nutzer auf den mobilen Endgeräten private Daten speichern, sind diese selbst für diese Daten verantwortlich. Es besteht kein Anspruch, dass die gespeicherten privaten Daten durch das Unternehmen geschützt werden.

3. Definitionen und Begriffe

Die nachfolgenden Aufzählungen erläutern wichtige Begriffe, die in dieser Richtlinie Anwendung finden.

3.1 Mobile Endgeräte

Unter mobilen Endgeräten im Sinne dieser Richtlinien werden solche tragbaren Endgeräte verstanden, die über ein Betriebssystem verfügen (tragbare Rechner (Notebooks bzw. Laptops), Mobiltelefone, Smartphones). Nicht betrachtet wird in dieser Richtlinie Equipment, auf dem Daten transportiert werden, wie z. B. USB-Sticks, mobile Festplatten und ähnliches Equipment.

3.2 Apps

Programme (meist für Smartphones und Tablets), die durch die Nutzer selbst installiert werden können. Die Installation geschieht oftmals über sogenannte „App-Stores“.

3.3 Geräteverwaltung, Mobile Device Management (MDM)

Unter einer Geräteverwaltung wird typischerweise eine Software verstanden, in der mobile Endgeräte erfasst, überwacht und gesteuert werden können. Solche Systeme bieten zum Beispiel Möglichkeiten zur Lokalisierung, Sperrung, Deaktivierung oder Fernlöschung der Geräte.

3.4 IrDA, Bluetooth, Wlan

Diese Schnittstellen eines Gerätes, dienen meist der Kommunikation mit anderen Geräten oder dem Austausch von Daten.

3.5 NFC

NFC (Near Field Communication) bezeichnet eine Schnittstelle, um Daten mit anderen Geräten über einen sehr kurzen Abstand (meist nur wenige Zentimeter) zueinander auszutauschen. Häufig wird NFC für Zahlungsvorgänge genutzt.

3.6 Kensington Schloss

Ein standardisiertes System mit dem meist Notebooks bzw. Laptops mittels eines Stahlkabels und einem Schloss gegen Diebstahl gesichert werden können.

3.7 Personal Firewall

Eine „Personal Firewall“ ist ein Programm, welches verhindert, dass ein IT-System über offene Schnittstellen bzw. Dienste vom Netzwerk aus angegriffen werden kann. Die Personal Firewall blockiert und verhindert diese Zugriffe.

3.8 VPN

VPN (Virtual Private Network) ist eine sichere Netzwerkverbindung, die von Unbeteiligten nicht eingesehen werden kann. „Virtuell" bedeutet in diesem Zusammenhang, dass die verschiedenen Endgeräte in dem Netzwerk nicht direkt physisch miteinander oder mit einem zentralen Router verbunden sind.

4. Voraussetzungen für mobiles Arbeiten

Die Voraussetzungen für mobiles Arbeiten ist eine vorherige Genehmigung. Dies erfordert die Zustimmung der Vorgesetzten und die Anmeldung bei der IT-Abteilung. Die mobilen Endgeräte sowie die erforderliche Software werden vom Unternehmen bereitgestellt.

5. IT-Sicherheitsanforderungen

Bei der Nutzung mobiler Endgeräte ist eine Richtlinie zu beachten und die Kenntnisnahme ist mit der Aushändigung des mobilen Endgerätes per Unterschrift zu bestätigen. Auf mobilen Endgeräten dürfen unverschlüsselt grundsätzlich nur Daten und Informationen folgender Vertraulichkeitsstufe gespeichert werden:

- ☐ öffentlich
- ☐ intern

Für vertrauliche sowie streng vertrauliche Daten ist die Zustimmung bzw. Erlaubnis der Geschäftsführung notwendig. Für den Fall, dass auf den Geräten vertrauliche sowie streng vertrauliche Daten oder personenbezogene Daten gespeichert sind, ist sicherzustellen, dass diese Daten durch Verschlüsselung geschützt werden. Der Datenschutzbeauftragte bzw. die IT-Abteilung ist über die Speicherung / Verarbeitung zu informieren. Die nachfolgenden Informationen geben eine Erläuterung, wie die Zielsetzungen dieser Richtlinie in die operative Büroorganisation umzusetzen sind.

5.1 Benutzerverantwortung

Grundsätzlich gilt, dass Nutzer mobiler Endgeräte sicherstellen müssen, dass sie bei der Eingabe von Passwörtern oder PINs nicht beobachtet werden.

Bei betrieblichen Telefonaten in der Öffentlichkeit per Smartphone, ist darauf zu achten, dass kein unbefugter Dritter den Gesprächsinhalt mithören kann. Scheint dies in der aktuellen Situation nicht möglich, ist der Gesprächspartner darüber zu informieren und es ist ein späterer Gesprächstermin zu vereinbaren.

5.1.1 Diebstahlschutz / Verlust

Mobile Endgeräte dürfen nie unbeaufsichtigt gelassen werden. Bei Bedarf sind diese gegen Diebstahl zu schützen z.B. durch Einsatz eines Kensington-Schlosses, Aufbewahrung im Hotelsafe, Mitführung nahe am Körper. Wird das mobile Endgerät nicht benutzt ist dies umgehend auszuschalten oder zu sperren (ggf. Sim-Karte entfernen).

Der Verlust oder Diebstahl eines mobilen Endgeräts ist umgehend der IT-Abteilung zu melden. Falls auf dem mobilen Endgerät personenbezogene Daten gespeichert sind, ist der Verlust auch dem Datenschutzbeauftragten mitzuteilen.

5.1.2 Datensicherung

Die betrieblichen Daten und Informationen auf mobilen Endgeräten sind, sobald diese mit dem Unternehmensnetzwerk verbunden sind, mit den betrieblichen Systemen zu synchronisieren. Eine exklusive Speicherung von Unternehmensdaten ausschließlich auf dem mobilen Endgerät ist nicht zulässig.

5.1.3 Keine Nutzung freier WLANs ohne VPN

Die Nutzung eines freien WLANs oder Hotspots ist nur zum Zweck der Verbindungsaufnahme mittels VPN in das Unternehmensnetz zulässig. Verfügt das mobile Endgerät über ein LTE- bzw. 5G-Modem, ist ein Verbindungsaufbau über das Mobilfunknetz eines Verbindungsaufbaus über freies WLAN vorzuziehen.

5.1.4 Keine Nutzung öffentlicher USB-Ports

Die Nutzung kostenloser öffentlicher USB-Anschlüsse, wie sie in Bahnhöfen, Flughäfen oder Hotels zu finden sind, ist ausnahmslos verboten.

Zum Laden oder Betrieb der Geräte sind ausschließlich die vom Unternehmen zur Verfügung gestellten Ladegeräte zu nutzen. Die Nutzung von USB-Geräten an mobilen Endgeräten ist grundsätzlich nicht erlaubt. Für den Fall, dass der Nutzer ausnahmsweise befugt ist, USB-Geräte an sein mobiles Endgerät anzuschließen, dürfen nur freigegebene Geräte angeschlossen werden.

5.1.5 Keine unautorisierte Installation von Apps

Die Installation von nicht freigegebener Software oder Apps durch den Nutzer ist nicht zulässig. Eine Installation erfolgt durch die IT-Abteilung.
Diese Anordnung betrifft nicht die Sicherheits-Updates der Apps bzw. des Betriebssystems, die von den Herstellern zur Verfügung gestellt werden. Diese Updates sind durch den Nutzer durchzuführen.

5.1.6 Infektion mit Schadsoftware

Bei Verdacht auf Virenbefall ist das mobile Endgerät nicht mehr mit dem Unternehmensnetz zu verbinden, sondern es ist unverzüglich die IT-Abteilung zu informieren.

5.2 Technische Anforderungen

Die nachfolgend genannten technischen Anforderungen beziehen sich auf alle mobilen Endgeräte, mit denen Daten verarbeitet oder auf denen Daten und Informationen gespeichert werden, sofern dies mit den Geräten technisch möglich ist.

5.2.1 Sichtschutz

Mobile Endgeräte, die regelmäßig in der Öffentlichkeit genutzt werden, sind mit einer Sichtschutzfolie zu versehen. Für den Fall, dass keine Sichtschutzfolie verwendet wird, ist durch technische Einstellungen sicherzustellen, dass eine Nutzung des mobilen Gerätes an Orten nicht zulässig ist, wo die Gefahr einer Einsichtnahme durch unbefugte Dritte besteht.

5.2.2 Verschlüsselung

Die mobilen Endgeräte sind grundsätzlich mit einem geeigneten Verschlüsselungsverfahren zu verschlüsseln.
Siehe Richtlinie „Kryptografie“

Bei der Verschlüsselung ist darauf zu achten, dass möglichst alle Nutzdaten, d. h. auch Daten, die sich in temporären Verzeichnissen befinden, verschlüsselt werden. Es sind Vorkehrungen zu treffen, dass nach Kenntnis [illegible] eines Verlustes des Nutzer-Passwortes, des Nutzer-Schlüssels bzw.-Zertifikates durch die IT-Abteilung auf die Daten zugegriffen werden kann. Diese Informationen sind sicher und [illegible]

5.2.5 Schutz vor Schadsoftware

Sofern technisch realisierbar, sind Maßnahmen zum Schutz vor Schadsoftware (Firewall, Virenscanner) zu implementieren. Es muss dabei sichergestellt werden, dass auch die mobilen Endgeräte zeitnah und regelmäßig die aktuellen Antivirensignaturen erhalten und die Firewalls nach neustem Stand konfiguriert sind.

5.2.4 Patch- und Updatemanagement

Mobile Endgeräte sind in das betriebliche Patch- und Updatemanagement einzubinden. Es muss dabei sichergestellt werden, dass auch die mobilen Endgeräte zeitnah und regelmäßig aktuelle Patches und Updates erhalten (Siehe auch 5.1.5).

5.2.5 Zugang zum Unternehmensnetzwerk

Waren mobile Endgeräte, z. B. nach einer Urlaubs- oder Krankheitsphase, längere Zeit nicht mit dem Unternehmensnetzwerk verbunden, müssen diese vor einer erneuten Verbindung mit dem Unternehmensnetzwerk aktualisiert werden. Dies betrifft alle ausstehenden Updates und Patches sowie die Virensignaturen.

5.2.6 Datensicherung

Es sind geeignete technische Maßnahmen zur Datensicherung bzw. Synchronisation der Daten zu implementieren, die für den Nutzer intuitiv anwendbar sind (siehe 5.1.2). Die Nutzer sollten bei der Anmeldung am Unternehmensnetzwerk auf die Sicherung, bzw. Synchronisation hingewiesen werden.

5.2.7 MDM, Mobile Device Management

Mobile Endgeräte sind mit geeigneten Maßnahmen zu inventarisieren und zu verwalten. Die Geräteverwaltung sollte, für den Fall eines Verlusts oder Diebstahls des mobilen Endgerätes, Ortungs- und Fernlöschfunktionen unterstützen. Die Mitarbeiter sind über diese Funktionen zu informieren.

5.2.8 Passwortschutz, Displaysperre

Jedes mobile Endgerät muss über Schutzfunktionen wie Passwortschutz, Fingerabdruck-Scanner oder sichere Gesichtserkennung verfügen. Es sind Vorgaben für die Passwortstärke zu treffen. Jedes mobile Endgerät ist so zu konfigurieren, dass es [illegible] automatisch sperrt. Eine Deaktivierung der Schutzfunktionen durch den Nutzer ist entweder technisch zu verhindern oder organisatorisch zu untersagen.

5.2.9 Personal Firewall, WLAN, Hotspots, VPN

Falls ein mobiles Endgerät die Funktionalität besitzt, ist eine „Personal Firewall“ zu installieren und „restriktiv“ zu konfigurieren:

- Es muss verhindert werden, dass der Nutzer die Firewall deaktivieren kann.
- Das mobile Endgerät darf sich nicht automatisch mit unbekannten oder freien WLAN-Hotspots verbinden.
- Nur mit einer Firewall geschützte Geräte, dürfen sich zur Verbindungsaufnahme in das Unternehmensnetz mittels VPN an freien WLANs oder Hotspots anmelden.
- Eine Nutzung der mobilen Geräte als mobiler Hotspots ist zu unterbinden.

Die Funktion „Split Tunneling“ ist bei der Verbindungsaufnahme in das Unternehmensnetz über VPN zu deaktivieren.

5.2.10 Konfiguration von Schnittstellen

Bluetooth-Verbindung sind nur mit explizit gekoppelten Geräten (Fahrzeugen, Head-Sets, Tastaturen, etc.) zulässig. Um zu verhindern, dass andere Bluetooth-fähige Geräte über eine automatische Umgebungssuche (Sniffing) die aktive Schnittstelle des eigenen mobilen Geräts feststellen, muss bei Bluetooth-Aktivierung in den unsichtbaren Modus geschaltet werden. Nach einer Kopplung, muss weder das mobile Gerät noch das gekoppelte Gerät sichtbar bleiben, um kommunizieren zu können. Kommen keine Bluetooth-Geräte zum Einsatz, ist Bluetooth zu deaktivieren.

Die Nutzung von IrDA, NFC, und sonstiger Schnittstellen, über die Daten/Informationen übertragen werden können ist zu verhindern, bzw. eine Nutzung restriktiv zu handhaben.

Nicht benötigten USB-Schnittstellen sind, sofern dies möglich ist, zu deaktivieren. Für den Fall, dass die Nutzung dieser Schnittstellen durch den Nutzer aufgrund technischer erforderlich ist, ist dieser über die Möglichkeit einer Kompromittierung seines mobilen Gerätes zu informieren und zu sensibilisieren.

6. Einhaltung bzw. Nichtbeachtung der Richtlinie

Damit diese Regelung erfolgreich umgesetzt werden kann, bedarf es der Mithilfe aller. Die Einhaltung dieser Regelung wird von den Führungskräften stichprobenartig kontrolliert.

Nichteinhaltung dieser Richtlinie kann zu disziplinarischen Maßnahmen führen, einschließlich Abmahnung, Kündigung oder rechtliche Schritte.

7. Dokumentenlenkung und Änderungshistorie

Diese Richtlinie wird über das Intranet zur Verfügung gestellt.

Dokumentenlenkung

Lenkungskriterien	
Klassifizierung der Wichtigkeit (1-10)	
Klassifizierung der Vertraulichkeit	☐ Öffentlich
	☐ Intern
	☐ Vertraulich
	☐ Streng vertraulich
Speicherort	[z.B. URL der Datei auf dem Server]
Verantwortlicher	
Aktuelle Version	1.0
Datum Erstellung / letzte Änderung	30.10.2025
Nächstes Dokumenten-Review	30.10.2026

Dokumentenhistorie

Version	Freigegeben am	Freigegeben durch	Kommentar
1.0	30.10.2025		

Hinweis zur Nutzung der Vorlage für das Thema

Diese Arbeitshilfe soll nur eine ausführliche Vorlage für eine Richtlinie mobiles Arbeiten darstellen. Sie wurde nach bestem Wissen und Gewissen recherchiert, zusammengestellt und überprüft. Sie erhebt aber keinen Anspruch auf Vollständigkeit oder Eignung für den Einzelfall und erlaubt keine ausschließliche Anwendbarkeit für ein Unternehmen.

Jede Person, die dieses Produkt erwirbt ist verpflichtet, ihre individuellen Ergänzungen und Anpassungen vorzunehmen und alle Inhalte für den eigenen Anwendungsfall zu prüfen, d.h. diese ggf. mit eigenen Texten zu erweitern oder nicht passende Inhalte zu entfernen.

Die nachfolgende Liste gibt Ihnen einige Hinweise, worauf Sie bei der Ergänzung mit eigenen Texten bzw. Textmodulen unbedingt achten sollten:

1. Wählen Sie einfache, allgemein verständliche Formulierungen und schreiben Sie keine „Bandwurmsätze“.
2. Benutzen Sie eine verständliche Wortwahl und vermeiden Sie Fachvokabular.
3. Formulieren Sie nicht zu sehr ins Detail gehend.
4. Sprechen Sie den Leser in der „Wir“-Form an, um den Zusammenhalt in der Firma zu stärken.
5. Geben Sie den Mitarbeitern im Rahmen von Workshops die Gelegenheit auf die Formulierungen Einfluss zu nehmen.
6. Denken Sie daran, ggf. den Betriebsrat einzubeziehen.
7. Schreiben Sie gendergerecht. Die Nennung aller Geschlechter drückt die Wertschätzung gegenüber allen Menschen aus, unabhängig ihres Geschlechts.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweisseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

(1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
(2) Für Garantien haftet der Lizenzgeber unbeschränkt.
(3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
(4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
(5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
(6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
(7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
(8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

Hinweis auf geschützte Abschnitte bei Nutzung als Formular:

Das Dokument ist abschnittsbezogen als Formular geschützt, sodass Sie z.B. die Kontrollkästen oder Dropdown-Felder (im Sinne eines Formulars) am PC direkt anwählen und ausfüllen können. Es ist kein Kennwort festgelegt.

Schutz entfernen in MS Office 2003:
Symbolleiste „Formular“ aktivieren und auf das „Schloss-Symbol“ klicken.

Schutz entfernen in MS Office 2010:
In der Symbolleiste „Überprüfen“ das Symbol „Bearbeitung einschränken“ aktivieren. Daraufhin öffnet sich das Fenster „Formatierung und Bearbeitung“. In diesem Fenster rechts unten auf die Schaltfläche „Schutz aufheben“ klicken.

Wollen Sie die integrierte Funktionalität nicht nutzen, können Sie die Felder aus der Tabelle einfach entfernen.