Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Empfehlungen zum sicheren mobilen Arbeiten im Home-Office

Inhalt

1 Einleitung

Aufgrund der aktuellen Pandemie-Situation möchten viele Institutionen ihren Mitarbeitenden das Arbeiten von zu Hause ermöglichen. Herausforderungen bestehen nun in der schnellen Bereitstellung einer sicheren technischen Infrastruktur, die möglichst langfristig verwendet werden kann und situativ bedingte Verzögerungen in Arbeitsabläufen minimiert. Zudem muss auch im Home-Office ein effektiver Informationsfluss zwischen den Mitarbeitenden gewährleistet sein.

Am 18.03.2020 veröffentlichte das BSI eine Pressemeldung mit ersten Empfehlungen zum sicheren Arbeiten im Home-Office [1].

Unter dem Begriff Home-Office werden in diesem Dokument alle Arbeitsformen adressiert, bei denen Mitarbeitende ihre Arbeit nicht in den Gebäuden ihrer Institution, sondern in ihren privaten Räumlichkeiten verrichten; andere gängige Bezeichnungen sind z.B. "Telearbeit" oder "mobiles Arbeiten".

Ziel dieses Dokumentes ist die Bereitstellung einer umfänglichen Übersicht zu wesentlichen Maßnahmen rund um das sichere Arbeiten im Home-Office. Je nach Status einer ggf. vorhandenen Home-Office-Infrastruktur in einer Institution müssen die Maßnahmen auf ihre Anwendbarkeit und Umsetzbarkeit geprüft werden.

Der externe Home-Office-Arbeitsplatz erhält über das Internet Zugriff auf die interne IT-Infrastruktur der jeweiligen Institution. Damit die Home-Office-Infrastruktur nicht zum unsicheren Provisorium und Einfallstor für Cyber-Angriffe wird, müssen die neu entstehenden Informationssicherheitsrisiken erkannt und behandelt werden. Zur weiteren Orientierung bei der Aufrechterhaltung des Betriebs während der Corona-Pandemie dienen daher die folgenden ergänzenden bzw. konkretisierten Maßnahmen sowie Hilfestellungen auf organisatorischer und technischer Ebene. Die Maßnahmen basieren auf etablierten BSI-Veröffentlichungen und wurden zur Wahrung der Grundwerte der Informationssicherheit ausgewählt; Vertraulichkeit, Integrität und Verfügbarkeit sollten auch in dieser besonderen Situation gewährleistet sein. Ergänzend wurden Empfehlungen zum Einsatz von Videokonferenzsystemen und Messengern aufgenommen.

Bei ad hoc eingerichteten Lösungen für mobiles Arbeiten können in der Regel nicht alle Anforderungen der Informationssicherheit von Anfang an vollständig umgesetzt werden. Es empfiehlt sich, zunächst die Maßnahmen auszuwählen, welche durch die Institution zeitnah umgesetzt werden können. Dadurch soll von Beginn an zumindest ein Mindestmaß an Sicherheit gewährleistet und dies durch klare und verbindliche Regelungen für die Mitarbeitenden begleitet werden. Priorisiert werden sollten grundsätzliche Schutzmaßnahmen wie das regelmäßige Einspielen von Sicherheits-Updates, die Verwendung aktueller Virenschutzprogramme und eines VPN (Virtual Private Network), das Durchführen von Datensicherungen sowie der Einsatz von Firewalls. Dabei gilt es auch, die für das Home-Office genutzte private Netzinfrastuktur (u.a. Router) zu betrachten und zu schützen. Im weiteren Verlauf und vor Übernahme in den Regelbetrieb sollte das Informationssicherheitsniveau der Home-Office-Infrastruktur Schritt für Schritt erhöht werden, z.B. unter Zuhilfenahme des IT-Grundschutzes des BSI.

Die Sicherheitsberatung des BSI steht für Rückfragen und weitergehende Beratungsanliegen für den Bund unter sicherheitsberatung@bsi.bund.de sowie für Länder und Kommunen unter sicherheitsberatung-regional@bsi.bund.de gerne zur Verfügung.

Das BSI wünscht eine produktive und sichere Zeit im Home-Office, bleiben Sie gesund!

2 Organisatorische Maßnahmen

Für die Tätigkeit im Home-Office müssen durch die Institution Regelungen und Prozesse definiert werden, um effektive Arbeitsabläufe auch im Home-Office sicherzustellen und um organisatorische Schutzvorkehrungen zu treffen, damit sensible Informationen nicht in fremde Hände geraten können.

- **Regelungen erstellen:**
  - Erstellung einer Regelung, welche Mitarbeitenden im Home-Office arbeiten dürfen und welche in der Institution anwesend sein müssen. Es muss geklärt werden, welche Mitarbeitenden zur Aufrechterhaltung der kritischen Geschäftsprozesse unbedingt erforderlich sind und welche Aufgaben nicht im Home-Office bearbeitet werden können oder dürfen.
  - Institutionen müssen Regelungen für die Tätigkeit im Home-Office und den Umgang mit mobiler IT festlegen. Als Hilfestellung bietet das BSI folgende Vorlagen an; die Dokumente können im Word-Format über die Sicherheitsberatung des BSI [2] anfragt werden:
    - Dienstvereinbarung „Alternierende Telearbeit“,
    - Dienstvereinbarung „Mobiles Arbeiten“,
    - Dienstanweisung „Dienstliche Nutzung mobiler IuK-Technik“.
- **Mitarbeitende sensibilisieren:** Mitarbeitende müssen hinsichtlich der durch die Arbeit im Home-Office entstehenden Risiken sensibilisiert werden. Sie benötigen außerdem Informationen, wie im Home-Office eine sichere Arbeitsumgebung geschaffen werden kann. Vorschläge für den Aufbau einer Meldung an die Mitarbeitenden können dem Anhang „Informationsblatt für Mitarbeiter im Home-Office“ entnommen werden.
- **Telefonische Erreichbarkeit sicherstellen:** Die telefonische Erreichbarkeit der Mitarbeitenden im Home-Office muss sichergestellt werden. Es wird empfohlen, Listen zu erstellen, aus denen die jeweilige telefonische Erreichbarkeit der Mitarbeitenden hervorgeht.
- **Informationsfluss aufrechterhalten:** Um den Informationsfluss auch über die Gebäudegrenzen hinweg aufrecht zu erhalten, sollten Prozesse und Abläufe zur Einbindung der Mitarbeitenden etabliert werden. Hilfreich könnte hier z.B. der Einsatz eines internen Chat-Systems sein.
- **Geschäftsprozesse und Richtlinien prüfen:** Existierende Geschäftsprozesse und Richtlinien sollten unter Berücksichtigung der neuen Situation geprüft und angepasst werden, u.a.:
  - Passwortrichtlinien, da viele Systeme nun zusätzlichen äußeren Einflüssen ausgesetzt sind;
  - Vorfallsreaktionspläne, aufgrund der veränderten Präsenz der Mitarbeitenden;
  - VPN-Firmenrichtlinien, um einer größeren Anzahl entfernt arbeitender Beschäftigter Zugänge bereitzustellen;
  - Support-Prozesse, welche kurzfristig technische Unterstützung an mobilen Arbeitsplätzen gewährleisten.

3 Technische und weiterführende Maßnahmen

Folgende technische und weiterführende Maßnahmen bei Planung, Einrichtung und Betrieb mobiler Arbeitsplätze dienen als Hilfestellung, um im Home-Office ein Mindestmaß an Sicherheit zu gewährleisten.

3.1 Härtung der eingesetzten IT-Systeme

Um die Sicherheit im Home-Office zu erhöhen, sollten die eingesetzten IT-Systeme u. a. durch folgende Maßnahmen gehärtet werden.

- **Schnittstellenkontrolle prüfen:** Im häuslichen Umfeld kann die Hemmschwelle zur Verwendung privater, extern angeschlossener Geräte (z.B. USB-Sticks) niedriger sein. Um eine Infektion des Systems mit Schadsoftware zu vermeiden, kann eine Schnittstellenkontrolle diesen potentiellen Infektionsweg absichern. Vorhandene Regelungen zur Schnittstellenkontrolle sollten überprüft werden (siehe hierzu auch Mindeststandard des BSI zur Schnittstellenkontrolle [9]).
- **Absicherung des genutzten privaten Netzes:** Die Mitarbeitenden sollten sensibilisiert und angehalten werden, Maßnahmen zur Absicherung des ggf. genutzten privaten Heimnetzes zu treffen; hierzu zählt insbesondere die Anwendung der Sicherheitsfunktionen des privaten Routers.
- **Authentifizierung einrichten:** Mobile Arbeitsplätze sind durch einen Authentifizierungsprozess zu schützen und dürfen nur nach einer erfolgreichen Authentifizierung entsperrt werden. Es sollte eine automatische Bildschirmsperre eingerichtet sein; schon beim kurzzeitigen Verlassen des Arbeitsplatzes ist das System durch den Nutzer zu sperren. Die Zeitspanne bis zum Aktivieren der automatischen Bildschirmsperre sollte an die neuen Gegebenheiten angepasst werden, da auch Familienangehörige keinen Zugriff auf das System erhalten dürfen.
- **Virenschutz überprüfen:** Die Verwendung eines Virenschutzprogramms ist unabdingbar. Eine regelmäßige Aktualisierung der Virendefinitionen (Update-Prozess) muss auch für mobile Arbeitsplätze sichergestellt werden.
- **Sicherheits-Updates einspielen:** Die regelmäßige Aktualisierung der Software auf den mobilen Arbeitsplätzen (Update-Prozess) muss sichergestellt werden.
- **Bootvorgang absichern:** Mobile IT hat ein erhöhtes Risiko eines direkten und unbemerkten Zugriffs und somit einer Manipulation. Insbesondere der Bootvorgang muss zur Erhaltung der Integrität weitestgehend geschützt werden (z.B. Trusted Boot).
- **Protokollierung aktivieren:** Verbindungen zum institutionsinternen Netz sollten protokolliert und die Protokolle regelmäßig ausgewertet werden, um Risiken und Angriffe zeitnah zu erkennen.

Die Verwendung durch das BSI zugelassener Produkte zur Umsetzung der Maßnahmen sollte geprüft werden. Die Sicherheitsberatung des BSI führt eine Übersicht der vom BSI zugelassenen Produkte [8].

3.2 Umgang mit dienstlichen Informationen

Beim Umgang mit dienstlichen Informationen im Home-Office sollten folgende Aspekte beachtet werden.

- **Verschlüsselung einrichten:** Beim Transport sensibler Daten zwischen der Institution und dem Home-Office ist auf eine angemessene Verschlüsselung zu achten. Bei einer

Netzverbindung übernimmt ein eingerichtetes VPN diese Aufgabe. Unverschlüsselte Datenspeicher (externe Festplatten, USB-Sticks etc.) müssen durch zusätzliche Software oder Hardware ertüchtigt werden; eine permanente Datenträgerverschlüsselung sollte in Betracht gezogen werden, damit der Zugriff auf dort gespeicherten Daten der Institution nach einem Verlust verhindert wird.

- **Backups durchführen:** Alle Daten, die im Home-Office erstellt und bearbeitet werden, müssen zeitnah in der Institution gesichert werden. Dafür gibt es zwei Ausbaustufen:
    - Den Mitarbeitenden steht ein lokaler, verschlüsselter Datenträger für Backups zur Verfügung. Die Datensicherung kann darauf in einem festen Zyklus erstellt werden, z.B. bei Beendigung eines Arbeitstages. Eine lokale Datensicherung unterliegt jedoch ggf. schädigenden Einflüssen im Umfeld des Home-Office (Diebstahl, Brand etc.).
    - Die Datensicherung erfolgt über eine gesicherte Netzwerkverbindung auf den Servern der Institution. Die Datensicherung sollte dabei in Absprache während einer Phase geringerer Server- und Netzwerkaktivität durchgeführt werden (Nebenzeiten). Dadurch werden Kapazitätsengpässe vermieden.
- **Zugriffsschutz sicherstellen:** Mitarbeitende müssen dienstliche Unterlagen, Datenträger und IT-Systeme am häuslichen Arbeitsplatz so aufbewahren, dass kein Unbefugter darauf zugreifen kann. Dafür eignen sich verschließbare Behältnisse wie ein abschließbarer Schreibtisch, Rollcontainer oder Schrank. Jeder Mitarbeitende hat an seinem häuslichen Arbeitsplatz sicherzustellen, dass sensible Informationen nicht einsehbar und unzugänglich sind (Clean-Desk-Policy).

3.3 Einrichten des Fernzugriffs über ein VPN (Virtual Private Network)

Der Fernzugriff aus dem Home-Office in das Netz der Institution sollte ausschließlich über kryptografisch gesicherte Verbindungen (VPN) zugelassen werden. Der gesamte Datenfluss der mobilen Arbeitsplätze sollte ausschließlich über das VPN in das Netz der Institution geleitet werden, um die dortigen Sicherheitsstrukturen zu nutzen; dies betrifft insbesondere die durch Webbrowser erzeugten Datenströme. Ein Umgehen der VPN-Verbindung sollte unbedingt unterbunden werden, um eine risikoreiche direkte Kopplung des internen Netzes mit dem Internet zu verhindern.

Zur Realisierung der benötigten hohen Anzahl mobiler Arbeitsplätze müssen ausreichende Kapazitäten in der IT-Infrastruktur der Institution bereitgestellt werden. Wesentlich ist hier eine Bestandsanalyse der verfügbaren Kapazitäten. Die Netzverbindung an den Netzübergabepunkten kann dabei doppelt belastet werden (ein- und ausgehender Datenfluss); dies ist bei der Bestandsanalyse zu beachten. Bei einem knappen und kurzfristig nicht erweiterbaren Ressourcenkontingent kann eine Absprache zum lokalen Arbeiten – z.B. in Form alternierender Arbeitsweise – hilfreich sein. Folgende Fragen können bei der Planung behilflich sein:

- Wie viele mobile Arbeitsplätze können sich zeitgleich via VPN anmelden (Netzkapazität)?
- Wie viele VPN-Lizenzen bzw. Sicherheitstoken sind verfügbar?
- Welche mobilen Arbeitsplätze sind zur Erledigung wichtiger oder kritischer Geschäftsprozesse essentiell und sollten priorisiert Fernzugriff erhalten, sofern Kapazitätsengpässe bestehen?
- Welche Kapazitäten benötigt der typische Mitarbeitende?
- Kann der Fernzugriff bei Kapazitätsengpässen zeitlich aufgeteilt werden (z.B. zwei Stunden pro Mitarbeitenden)?

Um einen möglichst sicheren Fernzugriff zu gewährleisten, ist neben dem Einsatz eines VPN auch die Umsetzung weiterer technischer Sicherheitsmaßnahmen sinnvoll. Dazu gehört unter anderem die Verwendung von Zwei-Faktor-Authentifizierung (2FA).

Die Wahrscheinlichkeit, Angriffe und Abweichungen vom Normalbetrieb zu erkennen, wird durch eine zusätzliche Überwachung der für den Remote-Zugriff verwendeten VPN-Dienste, z.B. OpenVPN (UDP 1194), SSL VPN (TCP/UDP 443 oder IPsec/IKEv2 UDP 500/4500), erhöht. Anhaltspunkte für potenziellen Missbrauch können z. B. eine große Anzahl fehlgeschlagener Verbindungsversuche oder Login-Versuche von ungewöhnlichen IP-Adress-Geolokationen liefern. Aufgrund seiner Anfälligkeit für Angriffe sollte die Verwendung von RDP nach Möglichkeit vermieden werden. Insbesondere sollten keine Systeme per RDP aus dem Internet erreichbar sein.

Ist es nicht möglich, dienstliche Geräte für die Verwendung im Home-Office auszugeben, wird mitunter die Verwendung privater IT-Systeme der Mitarbeitenden in Betracht gezogen (BYOD - Bring your own Device). Dabei ist abzuwägen, in welchem Maße diesen Geräten vertraut werden kann. Anforderungen an die Absicherung privater IT-Systeme können in einer speziellen Richtlinie, die sich ggf. aus der Richtlinie für interne IT-Systeme ableitet, konkretisiert werden. Mögliche Bestandteile sind z.B. Sicherheits-Updates, Virenschutzprogramme, VPN und Festplattenverschlüsselung. Um das vom niedrigeren Sicherheitsniveau privater IT-Systeme ausgehende Risiko zu minimieren, sind die Berechtigungen der Mitarbeitenden auf das erforderliche Mindestmaß zu reduzieren. Beispielhaft sind die Zugriffsmöglichkeiten Mitarbeitender auf Netzwerke, IT-Systeme oder Freigaben entsprechend anzupassen und ggf. (gänzlich) einzuschränken. Der institutionelle Zugriff auf private IT ist auch von rechtlicher Seite zu betrachten.

3.4 Audio-/Videokonferenzsysteme

Das mobile Arbeiten verhindert die gewohnte Durchführung von Besprechungen. Ersatzweise werden deutlich mehr Audio-/Videokonferenzen durchgeführt. Die Kapazität der dafür benötigten Anlagen muss ggf. entsprechend erhöht werden. Ist dies kurzfristig nicht möglich, ist eine Strategie zur ressourcengerechten Nutzung sinnvoll, z. B. durch Abschalten der Videodienste und Beschränkung auf Audiokonferenzen.

Bei der Nutzung von Videokonferenzsystemen sollte auch in der jetzigen Ausnahmesituation ein Mindestsicherheitsniveau erreicht werden. Die Lösung sollte daher mit den institutionseigenen Sicherheitserfordernissen übereinstimmen. Besonders wichtig sind dabei die eingesetzten Protokolle. Grundsätzlich sollten standardisierte Protokolle gegenüber proprietären Lösungen bevorzugt werden. Sollte dies nicht möglich sein bzw. institutsintern bereits eine proprietäre Lösung im Einsatz sein, so kann bei einem kurzfristigen und temporären Bedarf, mit diesen Systemen über das eigene Netz hinaus kommuniziert werden. In jedem Falle sind u.a. eine Risikoanalyse nach BSI-Standard 200-3 sowie eine Strategie zur Nutzung erforderlich. Zudem müssen Vorkehrungen zur geregelten Beendigung der Nutzung der Übergangslösung getroffen werden.

Beim Einsatz von Audio-/Videokonferenzlösungen sind folgende Fragen zu beantworten:

- Können die eingesetzten Protokolle von der Firewall vollständig geprüft werden?
- Ist eine Schadsoftwareprüfung innerhalb des Datenstroms möglich?
- Sind tiefergreifende Berechtigungen von Clients oder Browser-Plugins (wie Zugriff auf Webcam, Mikrofone, Screensharing oder Fernsteuerung) erforderlich und mit den eigenen Sicherheitsanforderungen vereinbar?

Das BSI veröffentlicht in Kürze ein **Kompendium Videokonferenzanlagen**, in dem neben der Gefährdungslage auch Sicherheitsanforderungen und konkrete Umsetzungshinweise beschrieben werden. Zudem sind Beispiele für die Erstellung entsprechender Sicherheitskonzepte und Leistungsverzeichnisse enthalten, die bei einer möglichen Beschaffung hinzugezogen werden können. Das Kompendium kann kurzfristig über die Sicherheitsberatung des BSI [2] angefragt werden.

3.5 Cloud-Dienste für die Kollaboration

Bei Verwendung von Kollaborationsdienstleistungen Dritter (Public-Cloud) und generell, wenn Institutionssysteme über die Infrastruktur Dritter kommunizieren, sollten Risiken im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit verstärkt bewertet werden. So könnten beispielsweise durch Schwachstellen oder Hintertüren in Clients oder Browser-Plugins Informationen unberechtigt mitgeschnitten oder manipuliert werden. Auch ein möglicher Abfluss von Metadaten sollte bewertet werden.

Die Nutzung von Public-Cloud-Diensten ist durch den **Mindeststandard zur Nutzung externer Cloud-Dienste** [10] geregelt. Der Mindeststandard legt einen Prozess fest, anhand dessen eine Institution eine geregelte Entscheidung zur Nutzung eines externen Cloud-Dienstes zu treffen hat. Unter anderem wird durch den Mindeststandard festgelegt, dass grundsätzlich nur solche Cloud-Dienste zu nutzen sind, welche der Dienststelle die Einhaltung der Transparenz- und Sicherheitsanforderungen vertraglich zusichern, wobei als Minimum auf den **BSI Kriterienkatalog Cloud Computing C5:2020** [11] abgestellt wird.

3.6 Messenger-Dienste für die mobile Kommunikation

Messenger-Dienste können gerade in Zeiten verstärkter mobiler Kommunikation den direkten Austausch zwischen Mitarbeitenden erleichtern. Jedoch sollten bei deren Nutzung wesentliche Sicherheitsanforderungen eingehalten werden.

Aus Sicht des BSI sollten auch für eine Krisenkommunikation nur Messenger mit einer Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik zum Einsatz kommen. Dies bieten insbesondere Messenger, die auf das sog. „Double-Ratchet“-Verfahren setzen. Grundsätzlich können auch andere moderne Verschlüsselungsverfahren zum Einsatz kommen.

Regulär nutzen Messenger durch die jeweiligen Hersteller betriebene Infrastrukturen im Internet. Auf diesen Infrastrukturen werden Kommunikationsmetadaten für den Betreiber sichtbar. Außerdem hat die Institution keinen direkten Einfluss auf die Verfügbarkeit der jeweiligen Dienste. Trotzdem ist es unter Berücksichtigung der bestehenden Risiken möglich, diese Dienste für eine Krisenkommunikation heranzuziehen.

Bei der Auswahl eines Messenger-Dienstes sollten die folgenden Kriterien berücksichtigt werden:

- **Anonymität**: Der Messenger-Dienst kann anonym genutzt werden. D. h., zur Registrierung beim Messenger-Dienst ist die Angabe einer Telefonnummer oder E-Mail-Adresse nicht notwendig. Die Messenger-App kann unter Verwendung eines individuell generierten Benutzernamens bzw. einer ID genutzt werden. Dieses Identifikationsmerkmal muss unter den Kommunikationspartnern ausgetauscht werden.
- **Adressbuch**: Messenger-Apps erlauben eine Synchronisation des Geräte-Adressbuchs mit dem Messenger-Dienst, um bereits registrierte Kommunikationspartner automatisch zu finden. Einige Messenger-Apps hashen die im Adressbuch gefundenen Telefonnummern

und senden diese erst anschließend an den Messenger-Dienst. Bei Verwendung der Adressbuch-Synchronisation ist die DSGVO zu beachten.

- **Authentizität:** Messenger-Apps integrieren Funktionen, um die verwendeten Kontakte zu verifizieren. Zur Gewährleistung der Authentizität der jeweiligen Kommunikationspartner sollten diese erweiterten Funktionen verwendet werden. Die Funktionen sind app-spezifisch umgesetzt, z. B. als Überprüfung der Sicherheitsnummer, des Fingerabdrucks oder der ID.
- **Verschlüsselung:** Der Messenger-Dienst muss eine moderne Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik einsetzen.
- **Videochat**: Einige Messenger-Dienste bieten neben der Möglichkeit Sprachanrufe durchzuführen auch die Möglichkeit von Videochats.
- **Vertrauenswürdige Bezugsquellen:** Messenger-Apps dürfen nur aus einer vertrauenswürdigen Quelle bezogen werden. Dazu gehört insbesondere der im jeweiligen Gerät voreingestellte App Store. Falls eine Messenger-App von der Website des Betreibers heruntergeladen wird, muss vor der Installation die Checksumme der heruntergeladenen App überprüft werden.
- **Geschäftsmodell:** Einige Messenger-Dienste verwenden zur Kostendeckung ein werbefinanziertes Geschäftsmodell. Dabei erstellt der Messenger-Dienst Nutzerprofile, um personalisierte Werbung anzuzeigen. Die Verwendung der übermittelten Daten ist anhand der Angaben des Herstellers (Datenschutzerklärung) zu überprüfen und zu bewerten.
- **Europäischer Rechtsraum:** Europäische Messenger-Dienste sind zu bevorzugen, da sie europäischer Rechtsprechung unterliegen (z.B. Datenschutz).

Anhang

Bausteine für ein Informationsblatt für Mitarbeitende im Home-Office

Die Mitarbeitenden müssen sensibilisiert werden, wie sie sich im Home-Office zu verhalten haben und eine sichere Arbeitsumgebung schaffen.

Im Folgenden sind Anregungen und Vorschläge für den Aufbau einer Meldung an die Mitarbeitenden zusammengestellt, die zum einen Hilfestellungen für das Verhalten im Home-Office geben, zum anderen grundsätzliche Schutzmaßnahmen für Tätigkeiten in der mobilen Arbeit beschreiben.

1. Ich muss nur kurz...
    - Geben Sie mobile Geräte unterwegs nicht aus der Hand. Lassen sie mobile Geräte nicht unbeobachtet liegen, auch nicht nur kurzzeitig.
2. Ich hatte es doch noch eben...
    - Wenn Sie ein mobiles Gerät verlieren oder es Ihnen gestohlen wird, melden Sie dies unverzüglich auch dem IT-Support.
    - Notieren Sie sich für alle Fälle die Kontaktdaten des IT-Supports, z.B. am Kühlschrank.
3. Pausen sind wichtig...
    - Mobile Geräte sind bei Nichtnutzung zu sperren (PIN/Bildschirmsperre/Token ziehen) oder auszuschalten.
    - Katzenvideos sind süß, belasten aber die Datenleitung unnötig; verwenden Sie bitte nur datensparsame Anwendungen auf den mobilen Geräten.
4. Ich brauche das ganz, ganz schnell...
    - Nutzen Sie nur dienstliche Mail-Accounts für dienstliche Angelegenheiten oder dienstlichen Informationsaustausch.
    - Laden Sie dienstliche Dateien bei Cloud-Bedarf ausschließlich in dienstlich freigegebenen Cloud-Speicher.
5. Eine tolle App, und was die alles kann...
    - Kameras, Mikrofone und weitere Sensoren in mobilen Geräten können unbemerkt durch Software aktiviert werden. Wenn möglich, erlauben Sie den Zugriff nur auf zwingend notwendige Schnittstellen/Sensoren (Rechtevergabe der Apps).
    - Schalten Sie Standortinformationen (GPS) sowie weitere drahtlose Schnittstellen (Bluetooth/WLAN) bei Nichtnutzung ab, um die Erstellung von Bewegungsprofilen zu erschweren; es spart zusätzlich Strom.
6. Dünne Wände und offene Fenster: Meine Nachbarn wissen alles...
    - Bei Telefonaten mit sensiblem Inhalt ist der Ort so auszuwählen, dass Unbefugte das Gespräch nicht mithören können.
        - Achten Sie grundsätzlich darauf, die Übermittlung sensibler Informationen auf ein Mindestmaß zu beschränken.
        - Führen Sie Gespräche mit vertraulichen dienstlichen Inhalten nur mit mobilen Geräten, die eine verschlüsselte Kommunikation ermöglichen, es sei denn, es besteht eine zwingende dienstliche Notwendigkeit, anders zu handeln.
    - Stellen Sie den Bildschirm bzw. das Notebook so auf, dass nur Sie die Inhalte auf dem Bildschirm lesen können.
    - Benutzen Sie unterwegs Sichtschutzfolien für Bildschirme. Auch im Home-Office sollte bei der Bearbeitung sensibler Daten der Einsatz erwogen werden.
7. Der Akku ist schon wieder leer...

- Laden Sie Ihre dienstlichen mobilen Geräte nur mittels mitgelieferter Netzteile auf.
- Meiden Sie unterwegs unbedingt öffentlich zugängliche USB-Auflademöglichkeiten (Ladeterminals).

8. Feierabend...
    - Bewahren Sie Ihre dienstlichen mobilen Geräte, Akten und Datenträger an einem sicheren Ort auf; das kann schon eine verschließbare Schublade sein.
    - Weitere Informationen rund um die Informationssicherheit finden Sie unter https://www.bsi-fuer-buerger.de.

Quellen

[1] https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html

[2] Für den Bund: sicherheitsberatung@bsi.bund.de , Für Länder und Kommunen: sicherheitsberatung-regional@bsi.bund.de

[3] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.html

[5] https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html

[6] https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Fern/fern_node.html

[7] https://www.bsi.bund.de/cln_174/DE/Themen/Sicherheitsberatung/InternerBereich/internerbereich_node.html

[8] https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/mobile_Arbeitsplaetze/mobileArbeitsplaetze_node.html

[9] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Schnittstellenkontrolle_Version_1_2.pdf

[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.pdf

[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf