Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Der Delegierte für digitale Transformation und IKT-Lenkung

E021 - Einsatzrichtlinie Smartphone / Smarttablet Sync

Weisung zur Bundesinformatik

Klassifizierung:[1]	nicht klassifiziert
Verbindlichkeit:[2]	Weisung
Vorgabentyp:[3]	(E) Einsatzrichtlinie
Planungsfeld:[4]	Bundesweite IKT-Grundleistungen
Diese Version:	2.2
Ersetzt Version:	2.1
Status (diese Version):	Genehmigt
Beschlussdatum / Datum der Inkraftsetzung:	15.11.2022 Inkraftsetzung:03.01.2023
Erlassen von, Rechtsgrundlage:	Die oder der Delegierte für digitale Transformation und IKT-Lenkung (D-DTI), gestützt auf Artikel 17 Absatz 1 Buchstabe e der Verordnung vom 25. November 2020 über die digitale Transformation und die Informatik (VDTI, SR 172.010.58)
Sprachen:	Deutsch (Original), Französisch (Übersetzung), Englisch (Übersetzung)
Beilagen:	keine

[1] Zu den Klassifizierungen INTERN und VERTRAULICH vgl. *Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. Januar 2021)*; SR 510.411

[2] Zur Erlassform und zur Verbindlichkeit vgl. *Bundesamt für Justiz: Gesetzgebungsleitfaden, 4. verbesserte Auflage, 2019*

[3] vgl. Informationsplattform DTI-BK

[4] Planungsfelder gemäss *IKT-Strategie des Bundes 2020-2023 vom 3. April 2020 (SB000)*

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Gegenstand

Die mobilen Geräte der Mitarbeitenden der Bundesverwaltung müssen gemäss den organisatorischen und technischen Bundesvorgaben aufgesetzt, verwaltet und betrieben werden. Für die Umsetzung ist ein *Sicherheits- und Device Management System* erforderlich. Diese *Einsatzrichtlinie Smartphone/Smarttablet Sync [E021]* regelt die Nutzung von IKT-Anwendungen des Bundes mit *Smartdevices* über fremde Netze durch ein sicheres Zugangssystem mittels der Applikation *Secure Hub* (Sandbox-Lösung).

1.2 Gewährleistung des Datenschutzes

[1] Der Schutz der Daten wird wie bisher und jederzeit gewährleistet. Insbesondere ist es dem Betreiber des MDM-Systems nicht möglich, geschäftliche und ggf. private Daten des Nutzers einzusehen.

[2] Die Daten (Datensammlung), welche im Rahmen des Managements der Smartdevices anfallen, wurden dem *Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)* gemeldet.

1.3 Geltungsbereich

[1] Diese IKT-Vorgabe richtet sich an alle Mitarbeitenden der Bundesverwaltung, die über bundeseigene oder private *Smartdevices* auf IKT Ressourcen der Bundesverwaltung zugreifen.

[2] Der Geltungsbereich dieser Weisung ist identisch mit dem Geltungsbereich *Artikel 2* der *Verordnung über die digitale Transformation und die Informatik (VDTI).*

[3] Der Verbindlichkeitsgrad[5] der einzelnen Bestimmungen in Kapitel 2 dieser Weisung ist gemäss den Schlüsselwörtern in Anhang B festgelegt.

1.4 Begriffe

[1] In dieser Weisung bedeuten

a. *Smartdevice:* durch die Bundesverwaltung geprüfte und homologierte Geräte wie *Smartphones* und *Smarttablets*.

b. *Datensynchronisation:* Verschlüsselte Kommunikation zwischen *Smartdevice* und der Bundesnetzzone mittels *Over-the-Air*-Zugriff.

c. *MDM: Mobile Device Management*, für die zentralisierte Verwaltung von bundeseigenen und privaten *Smartdevices* durch den Bund mit Hilfe der Sandbox-Lösung.

d. *Sandbox-Lösung:* eine Applikation (Software) für die Synchronisation von Geschäftsdaten mit Apps wie *Secure Mail*, *Secure Tasks*, *Secure Notes*.

---

[5] Verbindlichkeitsgrade gemäss *Request of Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* Die Angabe von Verbindlichkeitsgraden gemäss [RFC 2119] ist eine verbreitete Praxis in der internationalen Standardisierung.

e. *Public Cloud:* ist ein frei zugängliches Angebot eines privaten Providers, der seine Dienste offen über das Internet für jedermann zugänglich macht, wie *iCloud*, *Google One*, *OneDrive*.

f. *OTA-Sync:* Applikation des Bundes zur Synchronisation von Geschäftsdaten mit nativen (ursprüngliche) Apps des Herstellers wie Mail-Client, Kalender, usw.

g. *Selektiver Wipe:* Löschung von Geschäftsdaten und Apps innerhalb der Sandbox-Lösung. Einstellungen, Daten und Apps ausserhalb der Sandbox-Lösung bleiben erhalten.

h. *Full Wipe:* Vollständige Löschung der Daten auf dem Smartdevice (einschliesslich Apps und Mails). Das *Smartdevice* wird in den Auslieferungszustand zurückgestellt.

i. *Biometrische Authentifikation:* Ist ein zum PIN alternatives Authentifizierungsverfahren (z. B. Touch ID oder Face ID).

j. *Jailbreak:* Unautorisiertes entfernen von Nutzungsbeschränkungen des Herstellers

k. *Malware:* Schadprogramm / Schadsoftware

2 Einsatzrichtlinie für geschäftlich genutzte Smartdevices

2.1 Geräte-Code, Secure Hub-PIN und Passwörter

[1] Für das *Smartdevice* MUSS ein 6-stelliger Geräte-Code verwendet werden.

[2] Für die Sandbox-Lösung MUSS ein 6-stelliger Secure Hub-PIN verwendet werden.

[3] Eine *biometrische Authentifikation* KANN als Ersatz zum Geräte-Code oder Secure Hub-PIN eingesetzt werden.

[4] Bei einem bundeseigenen *Smartdevice* MUSS ein *Full Wipe* erfolgen, wenn der Geräte-Code acht Mal falsch eingegeben wird.

[5] Es MUSS ein neuer *Secure Hub*-PIN erstellt werden, wenn der *Secure Hub*-PIN acht Mal falsch eingegeben wird.

[6] Falls das *Smartdevice* mehr als drei Minuten nicht genutzt wird, MUSS vom Benutzer die erneute Eingabe des Geräte-Codes verlangt werden.

[7] Für die Verwaltung von Passwörtern KANN eine App auf dem *Smartdevice* eingesetzt werden. Zur Authentifikation MUSS ein eigenständiges, komplexes Master-Passwort verwendet werden. Das Master-Passwort DARF NICHT mit weiteren Geräten synchronisiert werden.

2.2 Geschäftsdaten

[1] Auf *Smartdevices* sind klassifizierte Informationen der Stufe VERTRAULICH[6] oder höher, sowie besonders schützenswerte Personendaten oder Persönlichkeitsprofile verboten und DÜRFEN NICHT erstellt, gelesen oder bearbeitet werden.

---

[6] Zu den Klassifizierungen INTERN und VERTRAULICH vgl. 2. Abschnitt Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes, SR 510.411

[2] Für die Bearbeitung und Speicherung von Geschäftsdaten bei Apps aus dem *App Store* Bund und *App Store* des Herstellers (betrifft Eigenentwicklungen), liegt es in der Verantwortung des Auftraggebers resp. der zuständigen VE entsprechende Sicherheitsvorgaben zu erlassen oder zu implementieren. Geschäftliche Fotos DÜRFEN mit der Foto-App erstellt werden, jedoch MÜSSEN diese anschliessend in die Sandbox kopiert und ausserhalb gelöscht werden. Grössere Datenmengen, z. B. Videos, DÜRFEN per Kabel auf den Bundesarbeitsplatz übernommen werden.

[3] Geschäftsdaten DÜRFEN NICHT ausserhalb des *Smartdevices* (z. B. im Internet, auf externen Cloud-Dienste etc.) gespeichert werden. Ausgenommen davon sind Backupdienste des Herstellers für verschlüsselte Datensicherungen[7].

[4] Geschäftsdaten, die die Bundesverwaltung im Internet für autorisierte Benutzer bereitstellt, wie beispielsweise *E-Government*-Fachanwendungen oder *Collaboration Extranet*, DÜRFEN auch ausserhalb der Sandbox gelesen und bearbeitet werden.

2.3 Unerlaubte Modifikationen

[1] Auf einem geschäftlich genutzten *Smartdevice* DÜRFEN KEINE Manipulationen an der *Betriebs- und Sicherheitssoftware* (z. B. *Jailbreak*) vorgenommen werden.

[2] Entsprechen diese nicht den Erfordernissen der Bundesverwaltung, KANN der Leistungserbringer (LE) die Synchronisation deaktivieren. Die Synchronisation wird unmittelbar nach Erkennung einer Manipulation automatisch gesperrt und die Synchronisation wird unterbunden.

2.4 Softwareaktualisierung

[1] Die *Smartdevice*-Betriebssystemversion MUSS auf dem von dem LE offiziell unterstützten Stand gehalten werden.

[2] Die Softwareaktualisierung des Betriebssystems MUSS nach der Benachrichtigung bzw. Freigabe durch den LE erfolgen.

[3] Softwareaktualisierungen MÜSSEN *Over-the-Air* installiert werden.

[4] Bei Verwendung von nicht freigegebenen Betriebssystemversionen (älteren oder neueren) KANN die Synchronisation vom LE jederzeit blockiert werden.

2.5 Mobile Apps

[1] Apps MÜSSEN entweder über den *App Store* des Bundes oder einen *App Store* des jeweiligen Anbieters installiert werden.

[2] Einzelne Apps KÖNNEN aus Sicherheitsgründen durch den LE gesperrt oder verboten werden.

[7] Mit dem Programm CEBA wird ein Microsoft365 (M365) Angebot für Nutzer der Bundesverwaltung aufgebaut. Die einzelnen M365 Apps für das Smartdevice dürfen im Rahmen der Nutzung CEBA verwendet werden.

2.6 Lokale Synchronisation und Backup

[1] Auf der Büroautomation der Bundesverwaltung DARF KEINE Synchronisations-Software (z. B. *iTunes*) installiert werden.

[2] *Smartdevices*, die mit der Sandbox-Lösung Geschäftsdaten synchronisieren, KÖNNEN mit dem privaten PC Daten synchronisieren oder Datensicherungen erstellen.

2.7 Verlust oder Diebstahl eines Smartdevice

[1] Bei Verlust oder Diebstahl eines *Smartdevice* MUSS der zuständige *Servicedesk* unverzüglich informiert werden. Wieder gefundene Geräte sind ebenfalls dem *Servicedesk* zu melden.

[2] Nach Eingang der Meldung MUSS für bundeseigene *Smartdevices* ein *Full Wipe* und für private *Smartdevices* ein *selektiver Wipe* durch den zuständigen *Servicedesk* durchgeführt werden.

2.8 Reparatur

[1] Reparaturen von Bundesgeräten MÜSSEN über den ordentlichen Reparaturprozess ausgelöst werden. Dazu MUSS der Anwender den *Servicedesk* kontaktieren. Die *Smartdevices* MÜSSEN durch den Benutzer vor Versand an den Reparateur per *Full Wipe* über das *MDM Self Service*-Portal (SSP) gelöscht werden. Ist ein *Full Wipe* über das *Self Service*-Portal nicht mehr möglich, kann im Ausnahmefall das Gerät durch den Benutzer manuell auf Werkeinstellung zurückgesetzt werden. Ist ein *Full Wipe über das SSP oder manuell* nicht mehr möglich, so MUSS das Gerät vernichtet werden (z.B. über den BIT-Entsorgungsprozess)

[2] Bei privaten Smartdevices MUSS der Benutzer vor der Reparatur einen *selektiven Wipe* über den *Servicedesk* oder das *MDM Self Service*-Portal veranlassen. Die Reparatur bzw. Entsorgung MUSS durch den Anwender erfolgen.

[3] Vor der Reparatur MUSS der Benutzer bei *iOS-Geräten* die Menüfunktion *Mein iPhone/iPad suchen* (*find my iPhone*) deaktivieren.

2.9 Kündigung

[1] Bei Kündigung oder Austritt, MUSS der Benutzer seinen zuständigen *Integrationsmanager (IM)* informieren. Der *IM* beauftragt die Löschung des *Smartdevices*. Für bundeseigene *Smartdevices* MUSS ein *Full* oder ein *selektiver Wipe* und für private *Smartdevices* ein *selektiver Wipe* durchgeführt werden.

[2] Vor der Rückgabe MUSS der Benutzer bei *iOS-Geräten* die Menüfunktion *Mein iPhone/iPad suchen* (*find my iPhone*) deaktivieren.

2.10 Malware Befall

[1] Bei Verdacht auf *Malware*-Befall oder Manipulation, MUSS das *Servicedesk* umgehend informiert werden.

3 Schlussbestimmungen

3.1 Einhaltung

[1] Die Departemente und die Bundeskanzlei sorgen gemäss *Artikel 3* der *Verordnung über die digitale Transformation und die Informatik (VDTI)* für die Umsetzung dieser Weisungen in ihrem Zuständigkeitsbereich.

3.2 Überprüfung

[1] Der *Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI-BK)* überprüft die Aktualität und Zweckmässigkeit dieser Weisung spätestens vier Jahre nach deren Inkraftsetzung.

3.3 Inkrafttreten

[1] Diese Weisung tritt in der hier vorliegenden Version am 3. Januar 2023 in Kraft.

Anhänge

A. Änderungen gegenüber Vorversion

- Alle ISB-bezogenen Formulierungen wurden entsprechend der *Verordnung über die digitale Transformation und die Informatik (VDTI)* angepasst.
- Diverse Präzisierungen zur Geschäftsdatensynchronisation und Ergänzungen zu biometrischer Authentisierung sowie die Verwendung von Passwort Apps

B. Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades

Der Verbindlichkeitsgrad[8] der einzelnen Bestimmungen in Kapitel 2 dieser Weisung wird mittels folgender Schlüsselwörter in Grossbuchstaben gekennzeichnet:

Schlüsselwort	**Verbindlichkeitsgrad**
MUSS	Bestimmung, die zwingend einzuhalten ist (gewährte Ausnahmen ausgenommen)
DARF NICHT	Option, die nicht gewählt werden darf
DARF	Option ist ausdrücklich erlaubt. Die VE kann entscheiden, ob sie die Option nutzen möchte oder nicht. Betrifft die Bestimmung eine IKT-Lösung, muss der Anbieter dieser Lösung die Wahlmöglichkeit anbieten.
SOLL	Option, die im Normalfall zu wählen ist. Eine VE kann jedoch ohne Ausnahmegewährung des Bereich DTI-BK bzw. des NCSC davon abweichen, wenn dadurch Wirtschaftlichkeit und/oder Sicherheit nicht beeinträchtigt werden. Die Abweichung von der Bestimmung ist gegenüber dem Bereich DTI-BK bzw. dem NCSC schriftlich zu begründen.
KANN	Akzeptierte Option. Betrifft die Vorgabe eine IKT-Lösung, entscheidet der Anbieter der IKT-Lösung darüber, ob er die Option unterstützen will.

[8] Verbindlichkeitsgrade gemäss *Request of Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* Die Angabe von Verbindlichkeitsgraden gemäss [RFC 2119] ist eine verbreitete Praxis in der internationalen Standardisierung.

C. Referenzen

ID	Referenz[9]
SD100	SD100 - Servicekatalog IKT-Standarddienste, Ausgabe 2020
VDTI	Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (Verordnung über die digitale Transformation und die Informatik, VDTI) vom 25. November 2020; SR 172.010.58

D. Abkürzungen

Kürzel	Bedeutung
BIT	Bundesamt für Informatik und Telekommunikation
BK	Schweizerische Bundekanzlei
DTI-BK	Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei
IKT	Informations- und Kommunikationstechnik
ISB	Informatiksteuerungsorgan des Bundes
LE	Leistungserbringer
MDM	Mobile Device Management
OTA	Over-the-Air
PIN	Persönliche Identifikationsnummer (PIN Code)
VE	Verwaltungseinheit

[9] Erlasse auf Bundesstufe werden gemäss der «Systematischen Rechtssammlung» referenziert. Bei einer referenzierten Bundesvorgabe wird die zum Beschlussdatum dieser Weisung gültige Version angegeben.