Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

E026 – Einsatzrichtlinie Arbeitsplatzsystem

IKT-Vorgabe

Klassifizierung:[1]	Nicht klassifiziert
Verbindlichkeit; Erlass (Typ):[2]	Weisung; Verwaltungsverordnung
Planungsfeld:[3]	Bundesweite IKT-Grundleistungen
Typ der IKT-Vorgabe:[4]	IKT-Einsatzrichtlinie
Diese Version:	1.0
Status (diese Version):	Genehmigt
Ersetzt Version:	Initialversion
Beschlussdatum / Datum der Inkraftsetzung (diese Version):	IKT-Beschluss Bund: 11. Juni 2019 / Inkraftsetzung: 1. Juli 2019
Erlassen durch (alle Versionen), Datum (Version 1-0), Rechtsgrundlage (alle Versionen):	Informatiksteuerungsorgan des Bundes (ISB), am 11.6.2019 (Version 1-0), gestützt auf Artikel 17 Absatz 1 der Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV), SR 172.010.58
Sprachen:	Deutsch (Original), Französisch
Beilagen:	keine

[1] Zu den Klassifizierungsstufen: INTERN und VERTRAULICH vgl. *2. Abschnitt Verordnung vom 4. Juli 2007 (Stand 1. Januar 2018) über den Schutz von Informationen des Bundes, SR 510.411*

[2] Zur Erlassform und zur Verbindlichkeit vgl. *Bundesamt für Justiz: Gesetzgebungsleitfaden, 3. verbesserte Auflage, 2007, Rz 575-582.*

[3] Planungsfelder gemäss *IKT-Strategie des Bundes 2016-2019 vom 4. Dezember 2015, Anhang A (SB000)*

[4] IKT-Vorgabentypen gemäss *Artikel 3 der Bundesinformatikverordnung vom 9. Dezember 2011 (SR 172.010.58)*

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Rechtliche Grundlagen und übergeordnete Bestimmungen

[1] Die vorliegende Einsatzrichtlinie ist eine IKT-Vorgabe im Sinne von Art. 17 Abs. 1 Bst. d Bundesinformatikverordnung [BinfV].

[2] Sie ergänzt die übergeordneten Bestimmungen des Bundesrechts und die Weisungen des Bundesrates zur IKT-Sicherheit in der Bundesverwaltung [WIsB].

1.2 Gegenstand

[1] Diese IKT-Vorgabe umfasst die grundsätzlichen Bestimmungen für die Nutzenden des Services "Arbeitsplatz" und - sofern anwendbar - des Services "Virtueller Desktop" des *IKT-Standarddienstes Büroautomation* (SD BA).[5]

[2] Sie bezweckt, den rechtmässigen, sicheren und wirtschaftlichen Einsatz des Arbeitsplatzes zu gewährleisten und diesen sowie die damit verbundenen Umsysteme vor Missbrauch und Beschädigung zu schützen.

[3] Sie regelt die Grundsätze zur Bearbeitung der Daten mit den Mitteln des SD BA.

[4] Die Departemente und deren Verwaltungseinheiten sowie die Bundeskanzlei sorgen dafür, dass die Bestimmungen dieser IKT-Vorgabe sinngemäss in ihren Weisungen übernommen werden.

[5] Verschärfende oder ergänzende Bestimmungen sind in deren Zuständigkeitsbereich möglich.

1.3 Geltungsbereich

[1] Der Geltungsbereich dieser IKT-Vorgabe ist identisch mit dem Geltungsbereich der Bundesinformatikverordnung [BinfV].

[2] Diese IKT-Vorgabe gilt für die Nutzenden des Services «Arbeitsplatz» und - sofern anwendbar - des Services «Virtueller Desktop».

[5] Ausgeschlossen davon sind Endgeräte, welche nicht gemäss «AR007 Architektur Standard Build APS» und «A029 Standard Software BA-Client» aufgesetzt und betrieben werden, wie z.B. Entwicklerarbeitsplätze, Labor PC-Systeme, spezifische Administrationsgeräte u.ä. Diese IKT-Vorgabe soll aber - sofern anwendbar – auch in diesen Fällen sinngemäss angewendet werden.

1.4 Begriffe

[1] In dieser IKT-Vorgabe bedeuten

a. *Arbeitsplatzsysteme*: Die Arbeitsplatzsysteme bestehen aus dem *Service "Arbeitsplatz" [SD105]* und dem *Service «Virtueller Desktop» [SD119]*, welcher im SD BA//UCC gemäss dem vom Bundesrat genehmigten *Markmodell* [SD003] angeboten wird. Es ist in die Büroautomationsumgebungen des Bundes eingebunden und ermöglicht den Zugriff auf die Fachanwendungen. Es wird dem Benutzer gemäss *Art. 18 BPG*[6] und *Art. 69 BPV*[7] für die Erledigung der dienstlichen Aufgaben zur Verfügung gestellt.

b. *Arbeitsplatzsystem APS*: Das Arbeitsplatzsystem ist ein Endgerät, welches durch den Service gemäss *«Servicespezifikation Arbeitsplatz» [SD105]* angeboten wird.

c. *Virtueller Desktop*: Der Service «Virtueller Desktop» ist in der *Servicespezifikation «Virtueller Desktop» [SD119]* beschrieben. Der Service enthält keine Hardware und ermöglicht den Zugriff auf den virtualisierten Arbeitsplatz.

d. *Geschäftsrelevante Daten:* Als geschäftsrelevant gelten Daten, die für den Nachweis der Verwaltungstätigkeit im Sinne von *Artikel 22* der *Regierungs- und Verwaltungsorganisationsverordnung (RVOV)* notwendig sind.

e. *Geschäftliche Daten*: Geschäftliche Daten sind alle Daten, welche in Zusammenhang mit einer dienstlichen Rolle oder Tätigkeit anfallen. Diese Daten gehören der Verwaltungseinheit und damit dem Arbeitgeber Bundesverwaltung und nicht einer dedizierten Person - dies im Unterschied zu privaten und persönlichen Daten.

f. *Private Daten:* Daten, die keinen Bezug zur einer dienstlichen Aufgabe haben oder dediziert einer Person gehören (z.B. private Korrespondenz, private Personaldaten).

g. *Persönliche Daten:* Persönliche Daten sind geschäftliche Daten, welche in einer dienstlichen Tätigkeit anfallen, welche jedoch an eine Person gebunden sind und dieser gehören (z.B. persönliche Notizen, Anmerkungen, persönlich Mitarbeiterbeurteilung, persönliche Korrespondenz in Zusammenhang mit der Anstellung, Lohnabrechnung, persönliche Fotos, Arbeitskopien).

h. *SD Datenablagen:* Daten- bzw. Dokumentablagen, welche im SD Servicekatalog spezifiziert sind, durch die Leistungserbringer (LE) angeboten und durch die Benutzer genutzt werden, z.B. Collaboration (*Sharepoint*), Dateiablage (*Shares*), Geschäftsverwaltung (*GEVER*).

i. *Schutzniveau:* Die Definition Schutzniveau gibt einen Hinweis darüber, welche Informationen maximal mit dem Service, ohne zusätzliche Schutzmassnahmen, bearbeitet, transportiert und gespeichert werden dürfen. Die Definition berücksichtigt die Aspekte des Daten- und Informationsschutzes gemäss *DSG*[8] und *ISchV*[9]. Diese Definition entbindet den Anwender in keiner Weise von seiner Eigenverantwortung zur korrekten Verwendung eines Standarddiensts oder Teilen davon.

---

[6] SR 172.20.1 Bundespersonalgesetz BPV

[7] SR 172.220.111.3 Bundespersonalverordnung BPV

[8] SR 235.1 Bundesgesetz v über den Datenschutz DSG

[9] SR 510.411 Informationsschutzverordnung (ISchV)

Klassifizierungs- und Sicherheitseinstufung gemäss *Schutzbedarfsanalyse* [P041][10]:

	Definitionen ISchV	**Definition DSG**
SN0 Basis	Bearbeitung von nicht-klassifizierten Informationen	Bearbeitung von öffentlichen Personendaten und Datensammlungen
SN1	Bearbeitung von Informationen mit einer maximalen Klassifizierung «INTERN»	Bearbeitung von nicht öffentlich zugänglichen Personendaten und Datensammlungen
SN2	Bearbeitung von Informationen mit einer maximalen Klassifizierung «VERTRAULICH»	Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen
SN3	Verarbeitung von Daten mit einer maximalen Klassifizierung «GEHEIM»	Bearbeitung von Personendaten, deren Missbrauch für den Betroffenen Gefahren für Leib & Leben bedeutet

Für Abkürzungen und weitere allgemeine Begriffe siehe *Anhang*.

[10] P041 - Schutzbedarfsanalyse (Schuban)

2 Bestimmungen Arbeitsplatzsystem

2.1 Allgemein

[1] Die Nutzenden des Arbeitsplatzsystems sind beim Einsatz dieses IKT-Mittels für die Einhaltung der vorliegenden IKT-Vorgabe sowie der IKT-Sicherheitsvorgaben des Bundes persönlich verantwortlich.[11]

[2] Bei Verlust oder Diebstahl des Arbeitsplatzsystem hat der Nutzende den *Service Desk* des zuständigen LE's sowie die gemäss Prozess der Verwaltungseinheit verantwortlichen Stellen unverzüglich zu informieren.[12]

[3] Die Nutzung des Arbeitsplatzsystems soll für dienstliche Zwecke zur Erledigung der zugewiesenen Aufgaben erfolgen und darf in verhältnismässigem Rahmen auch privat genutzt werden. Dabei darf die Arbeitsleistung nicht tangiert werden.

2.2 Arbeitsplatz Nutzung

[1] Eine Nutzung des Arbeitsplatzsystems, die gegen die schweizerische Rechtsordnung[13] verstösst oder den Interessen der Bundesverwaltung zuwiderläuft[14], ist verboten.
Dies gilt insbesondere für:

a. Beschaffen oder Beschädigen von fremden Informationen;

b. Eindringen in fremde IKT-Systeme;

c. Beschaffen von besonders schützenswerten Personaldaten;

d. Beschaffen und weitergeben von nach ISchV klassifizierten Informationen an nicht autorisierte Personen;

f. das Verändern von IKT-Sicherheitseinstellungen des Arbeitsplatzes;

g. das Installieren bzw. Deinstallieren jeglicher Software, welche nicht durch den LE ordentlich angeboten wird.

2.3 Sicherer Umgang mit Informationen und Daten

[1] Daten bis und mit *Schutzniveau 1* dürfen

a. mit dem Arbeitsplatzsystem bearbeitet werden;

b. auf *SD Datenablagen* gespeichert werden.

[2] Daten der Klassifizierungsstufe *Schutzniveau 2* dürfen unter Beachtung der Bearbeitungsvorschriften zum Informationsschutz [ISchV] und zum Datenschutz [DSG] bearbeitet werden.

---

[11] WIsB, Kap. 2.2, Art. 5

[12] IKT-Grundschutz Kap 6.2

[13] Z.B. Aufrufen, Betrachten, zur Verfügung stellen, Herunterladen oder Versenden von harten pornografischen, Gewalt verherrlichenden, rassistischen oder diskriminierenden Inhalten

[14] Z.B. Meinungsäusserungen, die dem Ansehen des Bundes und seiner Mitarbeitenden schaden

[3] Beim Verlassen des Arbeitsplatzes ist das Arbeitsplatzsystem zu sperren.

2.4 Datenablage

[1] Jedes Departement bzw. jede Verwaltungseinheit hat sicherzustellen, dass eine Datenablage einem Verantwortlichen (*Owner*) zugeordnet ist. Nur der Verantwortliche einer Datenablage ist berechtigt, diese zu löschen.

[2] Private Daten sind in einem gesonderten Verzeichnis „PRIVAT“ zu speichern, dies gilt auch für E-Mails. Die Departemente mit ihren Verwaltungseinheiten und die Bundeskanzlei bestimmen den Speicherort.

[3] Private und persönliche Daten des Mitarbeitenden sind vor seinem Austritt durch ihn zu löschen. Restdaten werden gemäss Austrittsprozess der Verwaltungseinheit nach einer Karenzfrist gelöscht. Dies gilt auch im Fall einer Freistellung, eines Todesfalls oder nach Abschluss eines Verfahrens.

[4] Die geschäftlichen Daten müssen in den dafür vorgesehenen *SD Datenablagen*, Geschäftsverwaltungssystemen oder den Gefässen von Fachanwendungen gespeichert werden. Für die offline Bearbeitung ist eine lokale Synchronisation erlaubt.

2.5 Kommunikation

[1] Die Bundes-E-Mail Adresse darf nur für den dienstlichen Gebrauch genutzt und weitergegeben werden.[15]

[2] Für den Versand von Mailtext mit *Schutzniveau 2* muss die im E-Mail Client (*Outlook*) eingebaute Verschlüsselungsfunktion (*Secure Messaging Standard*) verwendet bzw. angehängte Dateien mit *Schutzniveau 2* unter Verwendung eines zugelassenen Verschlüsselungsprogrammes gemäss *Servicekatalog SD [SD100]*, verschlüsselt werden.

[3] Geschäftsrelevante Nachrichten und deren Anhänge sind in den entsprechenden Anwendungen zu verarbeiten und abzulegen. *Outlook* ist kein Ablage- bzw. Archivierungssystem für geschäftsrelevante Daten.

[4] Die *Unified Communication* (UC) basierte Kommunikationsmittel dürfen nur für die Übertragung bis und mit *Schutzniveau 1* verwendet werden.

[5] Die Kommunikation mit sensitiven Informationen auf *Schutzniveau 2* ist mit der Nutzung der verschlüsselten Sprachkommunikation (VSK) [E027] erlaubt.

2.6 Drucken

[1] Das Drucken von einem Arbeitsplatz aus auf ein lokal angeschlossenen Drucker darf nur dann erfolgen, wenn dieser von der Bundesverwaltung beschafft wurde und direkt über eine Kabelverbindung am Gerät angeschlossen ist. Das gilt insbesondere auch für VDI-Sessions (*Service Managed VDI* und *Managed Mobile VDI intern*).

[15] Die Bundes-E-Mail Adresse darf nicht für die Registrierung oder als Eintrag in sozialen Netzwerken, Blogs, Chat-Foren, News-Groups, Wettbewerbe, Newsletter usw. zu privaten Zwecken genutzt werden.

2.7 Passwörter

[1] Passwörter dürfen nicht in Klartext gespeichert werden, zur Speicherung von Passwörter steht das Tool «Persönliche Passwortverwaltung» gemäss *Servicekatalog SD [SD100]* zur Verfügung.

2.8 Administrationsrechte

[1] Der Benutzer verfügt über keine lokalen Administrationsprivilegien auf den Arbeitsplatzsystemen.[16]

2.9 Systemprotokollierung

[1] Daten, welche bei der Nutzung der Arbeitsplatzsysteme anfallen, werden aufgezeichnet.[17]

[16] Siehe IKT-Grundschutz [Si001] 7.1.5

[17] SR 172.010 RVOG Art. 57

3 Schlussbestimmungen

3.1 Aufhebung bisheriger Vorgaben

[1] Die IKT-Vorgabe «E011 – Microsoft Office OneNote 2013», Version 1.1, wird mit Inkraftsetzung dieser IKT-Vorgabe ausser Kraft gesetzt.

3.2 Übergangsbestimmungen

[1] Diese IKT-Vorgabe ist durch die Departemente innerhalb von 6 Monaten ab Inkrafttreten sinngemäss in ihren Regelungen zu übernehmen oder diese IKT-Vorgabe ist als verbindlich zu deklarieren.

3.3 Einhaltung

[1] Die Leistungsbezüger und Leistungserbringer sind gemäss *BinfV*[18] [19] für die Einhaltung dieser Richtlinien in ihrem Zuständigkeitsbereich verantwortlich.

3.4 Überprüfung

[1] Das ISB überprüft die Aktualität und Zweckmässigkeit dieser IKT-Vorgabe in Abstimmung mit den anderen Vorgaben jährlich.

3.5 Inkrafttreten

[1] Diese IKT-Vorgabe tritt am 1. Juli 2019 in Kraft.

---

[18] *Art. 21 Abs. 2 BinfV:* «Die Leistungsbezüger sind für die Einhaltung der IKT-Vorgaben und der Beschlüsse des Bundesrates, des EFD, des ISB und der Departemente beziehungsweise der Bundeskanzlei in ihrem Zuständigkeitsbereich verantwortlich.»

[19] *Art. 23 Abs. 2 BinfV:* «Die internen Leistungserbringer sind für die Einhaltung der IKT-Vorgaben und der Beschlüsse des Bundesrates, des EFD, des ISB und der Departemente beziehungsweise der Bundeskanzlei in ihrem Zuständigkeitsbereich verantwortlich.»

Anhänge

A. Weitere Verhaltensempfehlungen

Weitergehende Tipps für die IKT-Sicherheit am Arbeitsplatz sind unter folgendem Link zu finden: *intranet.informatiksicherheit.admin.ch*.

Es sind weiter folgende Empfehlungen zu berücksichtigen:

A.2 Sicherer Umgang mit Informationen und Daten

1 Die Bearbeitung von Informationen auf dem Arbeitsplatz oder am APS angeschlossenen Peripherie Geräte sind in der „Verwendungsrichtlinien bei Informations- und Datenschutzaspekten für Mitarbeitende der Bundesverwaltung“ [Si001 - Hi02] zusammengefasst.

2 Als VERTRAULICH klassifizierte Informationen dürfen weder in den Metadaten noch im Dateinamen als solche gekennzeichnet werden.

3 Der Nutzende des APS schliesst alle Anwendungen am Ende des Arbeitstages und meldet sich vom APS ab (Logout) oder fährt das APS herunter.

A.3 Datenablage

1 Übersicht gängiger Ablageorte und ihre Verwendung (sofern durch die VE nicht anders vorgegeben):

a. GEVER: Geschäftsrelevante Daten gemäss *GEVER Verordnung*[20] sind im *Geschäftsverwaltungssystem (GEVER)* abzulegen.

b. Team / Organisation /Projekt Laufwerke und Ablagen: Nicht geschäftsrelevante Daten (z.B. Team- oder Projektunterlagen) sowie temporär genutzte geschäftsrelevante Daten und Arbeitsversionen davon dürfen in vom LE bereitgestellten Ablagen (z.B. Sharepoint oder Dateiablage, sog. *Fileshares*) abgelegt werden. Müssen Daten mit Personen ausserhalb der Bundesverwaltung gemeinsam bearbeitet werden, so soll der SD Service «Collaboration Extranet» verwendet werden.

c. Benutzerverzeichnis (*Home Drive*): Persönliche Daten sind im *Home Drive* abzuspeichern.

d. Lokales Laufwerk APS: Dieses ist lediglich für die temporäre Speicherung von Daten geeignet. Die Sicherung der Daten obliegt dem Benutzer.

2 Es obliegt den Verwaltungseinheiten, weitere Regelungen für die Datenablagen zu erlassen.

A.4 Kommunikation

1 Wenn immer möglich sollen in E-Mails und Kalendereinträgen anstelle der Dokumente Links (Hyperlink) zu diesen verwendet werden.

2 Kalendereinträge mit Angaben, die missbraucht werden können (z.B. Flug- oder Hotelbuchungen), sind als privat (Schlüsselsymbol) zu markieren.

---

[20] SR 172.010.441 Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung

A.5 Passwörter

1 Der Zugang zum APS erfolgt über die zugelassenen Authentifikationsmittel gemäss *IKT-Grundschutz [Si001]* und der *Zugriffsmatrix [Si002].*

2 Passwörter sind gemäss *IKT-Grundschutz [Si001]* geregelt.

A.6 Malware und Viren

1 Der Umgang mit Schadsoftware Befall ist im *IKT-Grundschutz [Si001]* geregelt.[21]

B. Änderungen gegenüber Vorversion

Keine, da Initialversion

C. Weitere für APS relevante IKT-Vorgaben

ID	Titel
[E017]	E017 - Einsatzrichtlinie UCC
[E019]	E019 - Einsatzrichtlinie Messaging Bund
[E027]	E027 - Einsatzrichtlinie Verschlüsselte Sprachkommunikation (VSK)

D. Referenzen

ID	Referenz
[A029]	A029 - BA Client Software
[BGA]	Bundesgesetz über die Archivierung (Archivierungsgesetz, BGA) vom 26. Juni 1998; SR 152.1
[BinfV]	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) vom 9. Dezember 2011); SR 172.010.58
[DSG]	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992; SR 235.1
[ISchV]	Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007; SR 510.411
[P041]	P041 - Schutzbedarfsanalyse (Schuban)
[SB003]	SB003 - IKT-Teilstrategie Malwareschutz
[SD003]	SD003 - Marktmodell Standarddienst: Büroautomation (BA) inkl. UCC
[SD100]	SD100 - Servicekatalog SD

[21] Siehe auch [Si001] IKT-Grundschutz, 12.2.2

[SD105]	SD105 - Servicespezifikation Arbeitsplatz
[SD119]	SD119 - Servicespezifikation Virtueller Desktop
[Si001]	Si001 - IKT-Grundschutz in der Bundesverwaltung
[Si001-Hi02]	Si001-Hi02: Verwendungsrichtlinien bei Informations- und Datenschutzaspekten für Mitarbeitende der Bundesverwaltung («oranges Blatt»)
[Si002]	Si002 - Zugriffsmatrix
[VBP]	Verordnung über die Bearbeitung von Personendaten Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012; SR 172.010.442
[WIsB]	W002 - Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB)

E. Abkürzungen und allgemeine Begriffe

Kürzel/Begriff	Bedeutung
APS	Arbeitsplatzsystem → s. Begriffe
BA	Büroautomation
DSG	Datenschutzgesetz
GEVER	Geschäftsverwaltungssystem der Bundesverwaltung.
ISchV	Informationsschutzverordnung
LE	Leistungserbringer
OE	Organisationseinheit – In der BVerw kann das ein Amt, eine Abteilung, eine Sektion, ein Team usw. sein.
Secure Messaging	Secure Messaging gewährleistet den verschlüsselten - und daher sicheren - Transport von E-Mails (inkl. Anhängen) zwischen E-Mail Partnern, welche jeweils mit gültigen Zertifikaten ausgerüstet sind.
SD	Standarddienst (SD) gemäss *BinfV* s. auch Intranet ISB > Themen > Standarddienste
SN	Schutzniveau.
Unified Communication (UC)	Der Service «Unified Communication» umfasst die Integration verschiedener synchroner Kommunikationsmedien in einer einheitlichen Anwendungsumgebung einschliesslich erweiterter Funktionalitäten wie Erreichbarkeitsstatus oder Konferenzen und ist in die Büroautomation voll integriert.
VE	Verwaltungseinheit – in der BVerw meist ein Amt
Verschlüsselung	Verschlüsselung (Chiffrierung) heisst der Vorgang, bei dem lesbarere Informationen mit Hilfe eines Verschlüsselungsverfahrens in eine „unleserliche", das heisst nicht interpretierbare Zeichenfolge (Chiffrat) umgewandelt wird.