Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

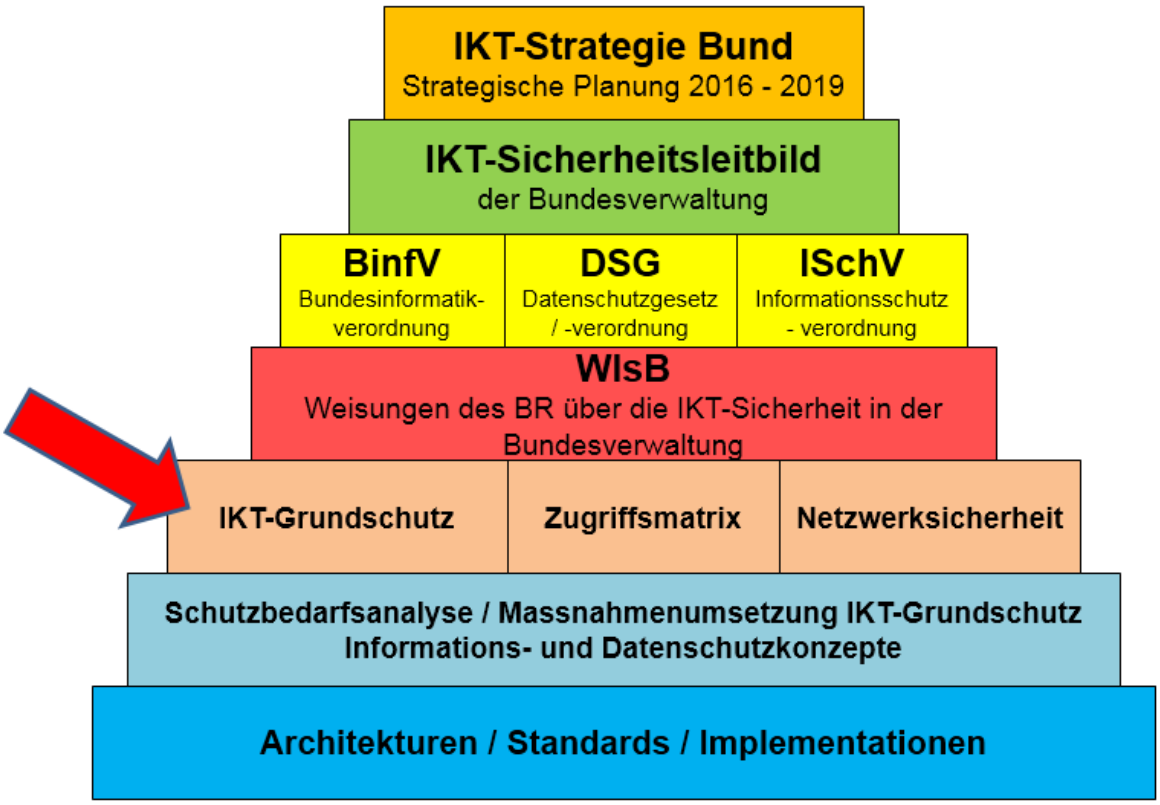
Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
IKT -Sicherheit

Version 4.0

IKT-Grundschutz in der Bundesverwaltung

vom 19. Dezember 2013 (Stand 1. März 2017)

Das ISB erlässt gestützt auf Ziffer 3.1 der Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB[1]) vom 1. Juli 2015 nachfolgende Vorgabe.



[1] Fundort: www.isb.admin.ch / IKT-Vorgaben / Sicherheit

Inhaltsverzeichnis

1 Anforderungen an den IKT-Grundschutz

1.1 Allgemeine Bestimmungen zum IKT-Grundschutz

Der IKT-Grundschutz legt die minimalen organisatorischen, personellen, technischen und baulichen Sicherheitsvorgaben (Grundschutz) im Bereich IKT-Sicherheit verbindlich fest.

Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verpflichtete VE zu dokumentieren und zu überprüfen (WIsB, Ziff. 2.2 Abs. 2, Ziff. 2.3 Abs. 2 und Ziff. 3.2 Abs. 3). Weiter ist zu beachten das Dokumentationen wie bspw. Betriebshandbücher, Berechtigungslisten revisionsgerecht geführt werden.

1.2 Geltungsbereich

Der Geltungsbereich dieser Vorgaben richtet sich nach Artikel 2 BinfV.

1.3 Ausnahmen zu den Vorgaben des IKT-Grundschutzes

Das ISB kann Ausnahmen bewilligen (WUBinfV[2], Art. 4.3) und führt ein aktuelles Verzeichnis aller erteilten Ausnahmen.

Will eine VE im Einzelfall aus organisatorischen, technischen oder wirtschaftlichen Gründen vom IKT-Grundschutz - im Sinne einer Unterschreitung - abweichen, liegt eine bewilligungspflichtige Ausnahme vor (BinfV[3], Art. 17 Abs. 1 Bst. e und f).
Die VE hat die dadurch entstehenden Risiken identifiziert, quantifiziert und in einem detaillierten Antrag dem ISB oder ISBD zur Beurteilung und Entscheidung zu unterbreiten.

Der oder die Informatiksicherheitsbeauftrage des Departements (ISBD) kann

a) selbständig Abweichungen (Unterschreitungen) des IKT-Grundschutzes bewilligen, wenn nachfolgende Rahmenbedingungen (kumulativ) eingehalten werden;
b) die Kompetenz zur Bewilligung von Abweichungen (Unterschreitungen) des IKT-Grundschutzes an den ISBO delegieren, wenn nachfolgende Rahmenbedingungen (kumulativ) eingehalten werden und sichergestellt ist, dass der ISBD entsprechend im Ausnahme-Prozess miteinbezogen wird, damit er seine Verantwortung jederzeit wahrnehmen kann.

- Das IKT-Schutzobjekt hat keinen erhöhten Schutzbedarf.
- Die IKT-Grundschutz-Unterschreitung betrifft nicht die Standarddienste und gefährdet ausschliesslich die eigene Verwaltungseinheit (VE).
- Der Informatiksicherheitsbeauftragte hat geprüft, ob keine amtsinternen, departementsinternen oder gesetzlichen Regelungen eine Abweichung vom IKT-Grundschutz verhindern/verbieten.
- Der Antragssteller hat die dadurch entstehenden Risiken identifiziert, quantifiziert und in einem detaillierten Antrag dem Informatiksicherheitsbeauftragten zur Prüfung und Genehmigung unterbreitet. Der Auftraggeber (u.a. bei Projekten) und der Geschäftsprozessverantwortliche / Anwendungsverantwortliche entscheiden somit zusammen mit dem Informatiksicherheitsbeauftragten über eine mögliche Abweichung (Unterschreitung) vom IKT-Grundschutz Stufe Bund gemäss WIsB, Ziffer 3.2, Abs. 6.
- Die Risiken die sich durch die IKT-Grundschutz Unterschreitung ergeben, müssen wenn immer möglich mit ergänzenden/alternativen Massnahmen reduziert werden. Die Restrisiken sind gemäss WIsB, Ziffer 3.4, Abs. 1 auszuweisen und den Auftraggeberinnen und Auftraggebern und den Geschäftsprozessverantwortlichen

[2] WUBinfV: Weisungen des EFD zur Umsetzung der Bundesinformatikverordnung

[3] SR 172.010.58

schriftlich zur Kenntnis zu bringen.
- Der Leiter oder die Leiterin der Verwaltungseinheit entscheidet ob die Restrisiken in Kauf genommen werden. (WIsB Ziffer 3.4, Abs. 2).
- Der ISBD führt ein aktuelles Verzeichnis und bringt Entscheide über Abweichungen mindestens einmal jährlich dem ISB zur Kenntnis.

Es werden in der Regel nur zeitlich befristete Ausnahmen bewilligt.

1.4 Ausführungsbestimmungen zum IKT-Grundschutz

Das ISB erlässt mit der "Zugriffsmatrix" verbindliche Ausführungsbestimmungen zum IKT-Grundschutz.
Daneben publiziert es Empfehlungen und Muster-Lösungen zum IKT-Grundschutz. Diese Unterlagen finden sich auf der Homepage des ISB[4] unter der entsprechenden Rubrik.

1.5 Übergeordnete Rahmenbedingungen

1.5.1 Archivierung

Die Anforderungen an die Archivierung von elektronischen Informationen richten sich nach den Vorgaben des Bundesarchives (Archivierungsgesetz, BGA[5]). Es koordiniert die Aktenführung und unterstützt die Organisationseinheiten bei deren Umsetzung.

1.5.2 Rechtsgrundlagen, Datenschutz und Informationssicherheit

Gestützt auf Artikel 13 der schweizerischen Bundesverfassung und die datenschutzrechtlichen Bestimmungen des Bundes hat jede Person Anspruch auf Schutz ihrer Privatsphäre sowie auf Schutz vor Missbrauch ihrer persönlichen Daten. Die Bundesbehörden halten diese Bestimmungen ein.

Die Anforderungen an den Datenschutz sind im Bundesgesetz über den Datenschutz (DSG[6]) und in der Verordnung zum Bundesgesetz über den Datenschutz (VDSG[7]) geregelt.

Für eine korrekte Grundlage eines IKT-Vorhabens sind die Artikel 6 - 8 der Bundesinformatikverordnung (BinfV) ein wesentlicher Bestandteil.

1.5.3 Verwendungsrichtlinien

Die Verwendungsrichtlinien von Informations- und Datenschutzsoftware für Mitarbeitende der Bundesverwaltung befinden sich auf der Webseite
https://intranet.isb.admin.ch/isb_kp/de/home/themen/sicherheit/projekthilfsmittel.html

1.5.4 Finanzkontrolle

Die Eidgenössische Finanzkontrolle ist das oberste Finanzaufsichtsorgan des Bundes.
Sie richtet ihre Prüfungstätigkeit nach dem Finanzkontrollgesetz (FKG[8]).

[4] intranet.isb.admin.ch
[5] SR 152.1
[6] SR 235.1
[7] SR 235.11
[8] SR 614.0

1.5.5 BBL, armasuisse

Eine der Hauptaufgaben des Bundesamtes für Bauten und Logistik BBL ist die Unterbringung der zivilen Bundesverwaltung. Ziel ist es, möglichst viele Verwaltungseinheiten in bundeseigenen Liegenschaften unterzubringen. Dazu erlässt es in Zusammenarbeit mit dem Bundessicherheitsdienst BSD die technischen und baulichen Vorschriften.

Die armasuisse ist im VBS für die Liegenschaften des Bundes und deren Anforderungen an die baulichen Massnahmen verantwortlich.

1.5.6 Fachstelle PSP[9] VBS und PSP BK

Die Fachstelle für Personensicherheitsprüfungen im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (Fachstelle PSP VBS) führt die Personensicherheitsprüfungen nach PSPV den Artikeln 10, 11 und 12 Absatz 1 in Zusammenarbeit mit den Sicherheitsorganen des Bundes und der Kantone durch.

Die Fachstelle für Personensicherheitsprüfungen in der Bundeskanzlei (Fachstelle PSP BK) führt die Personensicherheitsprüfungen nach PSPV Artikel 12 Absatz 2 mit Unterstützung der Fachstelle PSP VBS durch.

1.6 Inkraftsetzung und kontinuierliche Überarbeitung

Die Vorgaben des ISB zum IKT-Grundschutz, treten auf den 1. Januar 2016 in Kraft.
Das ISB prüft diese sowie die Ausführungsbestimmungen periodisch auf ihre Aktualität. Die aktuellste Version befindet sich der Homepage des ISB.

1.7 Begriff IKT-Schutzobjekte

IKT-Schutzobjekte sind Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der IKT, die in der Bundesverwaltung eingesetzt und somit geschützt werden müssen und entsprechend auch Gegenstand der Weisungen sind.

Bei der Definition und Abgrenzung eines IKT-Schutzobjektes sind die betrieblichen und organisatorischen Aspekte zu berücksichtigen. Wenn notwendig sind mehrere IKT-Schutzobjekte zu definieren, so dass mit der Übergabe von Projekt an den Betrieb die Verantwortlichkeiten, eindeutig und vollumfänglich den zuständigen Betriebsorganisationen, übertragen werden können.

[9] PSPV Art. 3

1.8 Verwendete Abkürzungen und Begriffe

Abkürzungen	***Bezeichnung***
APS	Arbeitsplatzsystem (Desktop, Notebook)
BBL	Bundesamt für Bauten und Logistik
BE	Benutzer
BIT	Bundesamt für Informatik und Telekommunikation
BV	Bundesverwaltung
CA	Certification Authority
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
ID	Identifikator
IKT	Informations- und Kommunikationstechnologie
ISB	Informatiksteuerungsorgan des Bundes
ISBD	Informatiksicherheitsbeauftragter Departement
ISBO	Informatiksicherheitsbeauftragter Verwaltungseinheit
ISDS	Informationssicherheits- und Datenschutz
LB	Leistungsbezüger
LE	Leistungserbringer
MDM	Mobile Device Management
OTA	Over the Air
OTP	One-Time-Password
OWA	Outlook Web Access
OWASP	Open Web Application Security Project
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PSP	Personensicherheitsprüfung
PSPV	Verordnung über die Personensicherheitsprüfung
RAS	Remote Access Service
SIM	Subscriber Identity Module
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VE	Verwaltungseinheit
VPN	Virtual Private Network
WIsB	Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung vom 1. Juli 2015

Begriffe	***Bezeichnung***
Daten	Im vorliegenden Dokument wird der Begriff «Daten» in einem umfassenden Sinne verwendet. Er umfasst sowohl Personendaten als auch andere Daten wie Protokolldaten, Datensammlungen nicht personenbezoger Daten etc. Wo sich eine Vorschrift ausschliesslich auf Personendaten bezieht, wird dieser Terminus gewählt.
Zugriffsmatrix	Vorgaben des Bundes über die Authentisierung, Verschlüsselung und Signatur: Anforderungen an elektronische Zertifikate und weitere Authentisierungsmittel. Es sind Ausführungsbestimmungen zu den vorliegenden Vorgaben.
Bundesnetzzone	Bei der Netzwerksicherheit geht es um das Bilden von geeigneten Netzzonen. Im Mittelpunkt des Interesses stehen dabei Bundesnetzzonen, d.h. gemäss NSP Zonen, deren Inhaber Organisationseinheiten der Bundesverwaltung sind.

1.9 Verweis auf ISO-Standard

Der vorliegende IT-Grundschutz ist ein Tailoring des ISO-Standards 27002:2013, erweitert mit spezifischen BV-Massnahmen. Der Verweis auf die ISO-Nummerierung wird in kursiver Schrift und in Klammern bei der jeweiligen Ziffer aufgeführt. Detaillierte oder weitergehende Ausführungen können zum besseren Verständnis auch dem ISO-Standard 27002:2013 entnommen werden.

1.10 Umsetzung IKT-Grundschutz und Übergangsbestimmungen

Die Verwaltungseinheiten haben den IKT-Grundschutz, sofern sie diesen nicht bereits einhalten, innert einer nützlichen Frist den Vorgaben anzupassen, gemäss WIsB, Ziff. 2.2, Abs. 3. Ist dies nicht möglich, haben sie gemäss Ziff. 1.2 dieses Dokuments eine Ausnahme zu beantragen.

Sie haben periodisch zu prüfen, ob die Umsetzung des IKT-Grundschutzes den aktuellen Weisungen des ISB (vgl. Ziff. 1.4 dieses Dokuments) entspricht und gegebenenfalls Anpassungen innert nützlicher Frist vorzunehmen.

Folgende Massnahmen sind neu oder wurden substantiell verändert. Die Neuerungen sind ab dem Inkrafttreten dieser Vorgabe umzusetzen:

- 1.1.2, 2.1.2, 4.1.1, 4.1.2, 7.1.7, 8.1, 8.5, 9.2, 10.1.3, 10.1.5, 12.1.4, 12.4.4, 12.6.2, 14.1.4, 15.2.1

Folgende Massnahmen wurden in andere Massnahmen integriert:

- 2.1.10 in 2.1.11, 10.1.2 in 10.1.1, 11.1.3 in 13.1.4, 12.6.3 in 12.6.2
-

Für folgende Massnahme gilt eine Umsetzungsübergangsfrist bis Ende 2019:

- 12.4.4

2 Minimale Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf

1 Informationssicherheitsleitlinien (*5*)

1.1 Richtungsvorgabe des Managements zur Informationssicherheit (*5.1*)

Nr.	Anforderung	Umsetzung		
		LB [10]	LE [11]	BE [12]
1.1.1 (*5.1.1, 5.1.2*)	Die Bundeskanzlei, die Departemente und die VE erlassen in Zusammenarbeit mit dem oder der zuständigen ISBO oder ISBD weitergehende oder spezifische Vorgaben[13] zur sicheren Nutzung der IKT-Mittel und halten diese aktuell.	X	X	
1.1.2 *(17.1.3)*	Die Sicherheitsdokumentationen wie Schutzbedarfsanalyse, Massnahmenumsetzung zum IKT-Grundschutz und ISDS-Konzepte haben eine Gültigkeit von max 5 Jahren.	X	X	

2 Organisation der IKT-Sicherheit (*6*)

2.1 Smart Devices (Smartphones und Tablets) (*6.1*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
2.1.1 (*6.2.1*)	Der Anschluss privater Smart Devices an eine Bundesnetzzone ist verboten. Davon ausgenommen sind Geräte • die im Mobile Device Management System (MDM) registriert sind. Das MDM muss über erzwungene Zugangsrichtlinien (enforced policy) verfügen • die via Public Wireless- und Webmaildienste der LE sowie andere im Standarddienst Datenkommunikation geregelte Netzwerkzugänge angeschlossen werden.	X	X	X
2.1.2 (*6.2.1*)	Auf Smart Devices ist die Bearbeitung und Speicherung von klassifizierten Informationen der Stufe VERTRAULICH oder GEHEIM, sowie von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen verboten. Sofern das Smart Device in den MDM-Service integriert ist, müssen die sonstigen Geschäftsdaten mit Anwendungen in der Sandbox gesendet, gelesen, bearbeitet und gespeichert werden. Geschäftliche Fotos dürfen mit der Foto-App erstellt werden, jedoch müssen diese anschliessend in die Sandbox kopiert und ausserhalb gelöscht werden. Ausnahmen zu dieser Massnahme (z.B. spezielle Geräte zur verschlüsselten Kommunikation) müssen in einem ISDS-Konzept beschrieben werden.	X	X	X
2.1.3 (*6.2.1*)	Die Datensynchronisation von Kalender, Mail, Aufgaben und Kontakte mit der zentralen Informatik der Bundesverwaltung erfolgt		X	

[10] LB: Leistungsbezüger

[11] LE: Leistungserbringer

[12] BE: Benutzer / Mitarbeitende

[13] Weisungen, Verordnungen etc.

	verschlüsselt über das Mobilfunknetz oder ein anderes geeignetes Drahtlosnetz (over the air, OTA).			
2.1.4 (*6.2.1*)	Die Synchronisierung geschäftlicher Daten auf private IKT-Mittel ist verboten. Davon ausgenommen sind Smart Devices die über das Mobile Device Management System (MDM) des LE angeschlossen sind. Ausnahmen zu dieser Vorgabe sind in einem ISDS-Konzept zu beschreiben.	X	X	X
2.1.5 (*6.2.1*)	Der Benutzer hat den Verlust eines Gerätes unverzüglich dem Servicedesk des LE zu melden.			X
2.1.6 (*6.2.1*)	Der LE implementiert einen Prozess der den Umgang mit verlorenen oder gestohlenen Geräten regelt. Diese Regelung muss den VE in geeigneter Form zur Kenntnis gebracht werden. Der Prozess muss mindestens das Zurücksetzen des Geräts (auf die Grundeinstellung = Verlust sämtlicher Daten) beinhalten.	x	X	
2.1.7 (*6.2.1*)	Der nachfolgend beschriebene Zugriffsschutz auf Smart Devices wird, soweit technisch möglich, durchgesetzt. Davon ausgenommen sind reine Telefoniefunktionen, wie die Entgegennahme von Anrufen oder die Ziffern-/Kurznummernwahl.		X	
2.1.8 (*6.2.1*)	*Symbol-/Musterpasswörter* müssen mindestens 6 Zeichen enthalten oder vier Punkte verbinden. Bei Symbolpasswörtern müssen mindestens drei verschiedene Zeichen vorhanden sein. *Passwörter* müssen mindestens vier Zeichen enthalten und aus Buchstaben und Zahlen bestehen. *PIN* müssen mindestens 6 Zeichen enthalten. Trivial-Kombinationen wie Benutzer-ID, Name, Vorname, Geburtsdatum oder Ziffernfolgen wie 1111, 1234 sind verboten. Spätestens nach drei Minuten Inaktivität ist das Gerät zu sperren und das Passwort oder der PIN neu einzugeben. Biometrische Merkmale (Touch ID, usw.) dürfen alternativ zu Passwörtern eingesetzt werden.		X	
2.1.9 (*6.2.1*)	Es dürfen nur Smart Devices zum Einsatz gebracht werden, welche vom LE zentral gemanagt werden, die Steuerung der Sicherheitseinstellungen unterstützt und deren Veränderung durch den Benutzer verhindern (MDM).	X	X	
2.1.10	Massnahme ist mit der Überarbeitung 2016 weggefallen.			
2.1.11 (*6.2.1*)	Der LE setzt ein Sicherheits- und Device Management System unter anderem für folgende Zwecke ein: • Verwaltung der SIM-Karten und der Smart Devices, • zur Sicherstellung der Inventarisierung, • zur Inbetriebnahme, • zur Rücksetzung des Geräts, • zwecks Einsatz spezieller Sicherheitsverfahren, • Sperren von sicherheitskritischen Anwendungen, • Erkennung und Abweisung nicht autorisierter Geräte.		X	
2.1.12 (*6.2.1*)	Die geschäftlichen Daten auf Smart Devices müssen durch Verschlüsselung des Speichers oder eines Teiles davon gegen Daten-/Informationsabfluss (Diebstahlschutz) geschützt werden.		X	

3 Personalsicherheit und Führungsverantwortung (*7*)

3.1 Verantwortung des Managements (*7.2.1*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
3.1.1 (*7.2.2*)	Die VE schulen und sensibilisieren die Mitarbeitenden stufen- und funktionsgerecht bezüglich den Vorgaben und Empfehlungen im Bereich IKT-Sicherheit und stellen dabei sicher, dass die Mitarbeitenden ihre Verantwortlichkeiten kennen.	X	X	
3.1.2 (*7.3.1*)	Die Benutzerrechte der Mitarbeitenden auf Zutritt, Zugang und Zugriff zu IKT-Schutzobjekten müssen aktuell gehalten werden. Sie müssen umgehend an veränderte Verhältnisse angepasst werden, wenn die Anstellung, der Auftrag oder eine entsprechende Nutzungs-vereinbarung der Mitarbeitenden geändert oder beendet wird.	X	X	
3.1.3 (*7.1*)	Gestützt auf das Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) und die Verordnung über die Personensicherheitsprüfung (PSPV) muss bei Bediensteten des Bundes eine Personensicherheitsprüfung durchgeführt werden, wenn dies für die Funktion erforderlich ist.	X	X	

3.2 Verantwortung der Mitarbeiterinnen und Mitarbeiter aller Stufen (*7.3.1*)

3.2.1 (*13.2.4*)	Es dürfen keine Informationen an Unberechtigte weitergegeben werden.	X	X	X

4 Management von organisationseigenen Werten (*8*)

4.1 Verantwortung für organisationseigene Werte (*8.1*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
4.1.1 (*8.1.1*) *(8.2.1)*	Für jedes IKT-Schutzobjekt muss eine Schutzbedarfsanalyse gemäss WIsB Ziffer 3.2 durchgeführt werden. [14]	X	X	
4.1.2 (*8.1.3*)	Die Verwendung privater IKT-Mittel (bspw. USB-Speichermedien, Firewire- und Bluetooth-Geräte, Headset etc.), privat beschaffter Software (bspw. Buchhaltungs-, Architektur-SW etc.) zu geschäftlichen Zwecken, ist verboten. Davon ausgenommen ist der Anschluss über das Mobile Device Management System (MDM) oder an die Public Wireless- und Webmaildienste des Leistungserbringers sowie andere besonders geregelte Einsatzformen.[15] Ausnahmen sind durch die Departemente zu regeln.	X		X
4.1.3 (*11.2.6 13.2.4*)	Die Bearbeitung von geschäftlichen Informationen auf nicht bundeseigenen IKT-Systemen ist nur aufgrund einer vertraglichen Regelung[16] zulässig, welche die sicherheitsrelevanten Belange regelt.	X	X	X

[14] Vorlage unter intranet.isb.admin.ch / IKT-Vorgaben / Sicherheit

[15] z.B. Formen der Telearbeit, siehe dazu die Richtlinien zur Telearbeit in der Bundesverwaltung des EPA

[16] z.B. Homeoffice, Verträge mit Externen

5 Handhabung von Speicher- und Aufzeichnungsmedien (*8.3*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
5.1 (*8.3.1, 8.3.2, 8.3.3*)	Die LB und LE erstellen ein Konzept für den Umgang mit datenhaltenden IKT-Schutzobjekten (Datenträgern), insbesondere für deren Reparatur und Vernichtung bzw. Entsorgung. Datenträger sind so zu entsorgen, dass keine Rückschlüsse auf den Inhalt oder die gespeicherten Daten möglich sind. Reparaturen sind grundsätzlich in Zusammenarbeit mit dem zuständigen ISBO oder ISBD zu regeln	X	X	

6 Arbeitsplatzsysteme (Notebooks, Desktops etc.) (*8.3*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
6.1 (*8.3.3, 18.1.5*)	Arbeitsplatzsysteme (Notebooks, Desktops) müssen durch eine vollständige Diskverschlüsselung gegen Daten-/Informationsabfluss (Diebstahlschutz) geschützt sein.		X	
6.2 (*16.1.2*)	Der Benutzer hat den Verlust eines Gerätes unverzüglich dem Servicedesk des LE zu melden. (siehe auch Massnahme 2.1.5)			X

7 Zugriffskontrolle (*9*)

7.1 Anforderungen an die Zugriffskontrolle (*9.1*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
7.1.1 (*9.1.1, 9.3.1, 9.4.2*)	Sämtliche Zugriffe auf IKT-Mittel müssen mit einer dem Schutzbedarf entsprechenden Authentifikation geschützt werden. Die Details sind in den Ausführungsbestimmungen "Zugriffsmatrix" geregelt.		X	
7.1.2 (*9.1.1, 9.4.3*)	Mittels Passwort geschützte IKT-Mittel müssen einen automatischen, periodischen Passwortwechsel erzwingen. Ist dies technisch nicht machbar, müssen die Benutzer in geeigneter Weise auf das regelmässige Ändern des Passworts aufmerksam gemacht werden.		X	
7.1.3 (*9.1.1, 9.4.2*)	Die VE setzen technische und organisatorische Massnahmen[17] zur Durchsetzung und Überprüfung der Authentifikationsanforderungen ein.	X	X	
7.1.4 (*9.4.1*)	Den Benutzern sind auf IKT-Mitteln nur die Rechte einzuräumen, die sie zwingend benötigen.	X	X	
7.1.5 (*9.2.3, 12.4.3*)	Lokale Administratorenrechte auf Arbeitsplatzsystemen sind nicht erlaubt. Wo unumgänglich, ist die Nutzung von administrativen Rechten nachvollziehbar (Logging) zu gewährleisten. Ein entsprechendes ISDS-Konzept ist zu erstellen.	X	X	

[17] Technisch: z.B. Durchsetzung der Passwortregelung (Massnahme 8.1); Organisatorisch: z.B. keine Weitergabe des Passworts bzw. der Smartcard (Massnahme 8.1)

7.1.6 (*6.1.2*)	Die Gewaltentrennung zwischen Bewilligung und Vergabe von Zugriffsrechten ist zu berücksichtigen und zu dokumentieren.	X	X	
7.1.7 (*9.2.3*)	Der Zugang zu Arbeitsplatz- und Serversystemen der BV darf nur über eine 2-Faktor-Authentisierung möglich sein. Ausnahmen siehe Kapitel „Funktions- Accounts“ im Dokument „Zugriffsmatrix“. Kann dies nicht gewährleistet werden, ist die Ausweichlösung in einem ISDS-Konzept zu beschreiben.	X	X	
7.1.8 (9.1.2, *9.2.3, 12.4.3*)	Für die Fernwartung müssen spezielle Benutzerkonten eingerichtet werden. Diese sind zu überwachen und die Verwendung muss nachvollziehbar sein (Logging).		X	
7.1.9 (*9.1.2*)	Der volle Zugriff via Remote-Access auf das BV-Netz darf nur verschlüsselt und mittels einer 2-Faktor-Authentifikation vorgenommen werden.		X	
7.1.10 *(9.1.2, 9.2.3*)	Ein Remote Zugriff zu Supportzwecken auf das Arbeitsplatzsystem ist nur mit einer vorgängigen, expliziten Einwilligung des Benutzers erlaubt.		X	

8 Benutzerverwaltung (*9.4*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
8.1 (*9.4.3*)	Passwortregeln für die Personenauthentifikation: • Länge: – Benutzerpasswort mind. 8 Stellen, – Administratorenpasswort mind. 12 • Zusammensetzung: – Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen – mindestens drei dieser Elemente müssen enthalten sein – Trivialpasswörter wie Benutzer-ID, Name, VornameGeburtsdatum etc. dürfen nicht verwendet werden – Das Auf- oder Abzählen von Passwörtern ist verboten • Passwortwiederholung – Initialpasswort = keine Wiederholung – Benutzer- und Administratorenpasswort = Wiederholung nach 10 erfolgten Wechseln • Gültigkeit: – Benutzerpasswort: max. 360 Tage – Administratorenpasswort: max. 90 Tage • Fehlversuche – max. 5, anschliessend muss die Benutzer-ID gesperrt werden • Weitergabe – Das Passwort oder die PIN ist persönlich und darf nicht weitergegeben werden • Bei Verdacht, dass Unberechtigte ein Passwort oder eine PIN kennen, ist das jeweilige umgehend zu ändern Ausnahmen zur Gültigkeit und zur Zusammensetzung müssen schriftlich, entweder im Dokument «Massnahmenumsetzung zum IKT-Grundschutz» oder in einem ISDS-Konzept, festgehalten werden.	X	X	X

8.2 (*9.4.3*)	Passwortanforderungen für unpersönliche Personenidentifikation[18]: • Unpersönliche Benutzer-ID oder Passwörter sind so wenig wie möglich zu vergeben. • Von den Passwortanforderungen gemäss Massnahme 8.1 darf nur abgewichen werden (zum Beispiel von der Gültigkeit) wenn – mit dieser Benutzer-ID/Passwort ausschliesslich auf Anwendungen mit generellem Schutzbedarf (Grundschutz) zugegriffen wird oder – ein genehmigtes Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) und eine Bewilligung des oder der ISBD vorliegt.	X	X	
8.3 (*9.4.2*)	Technische Benutzer-ID / funktionsbezogene- resp. Batch-User müssen sich mit einem PKI-Verfahren authentisieren. Der private Schlüssel (*private key)* muss auf dem System mit den notwendigen Zugriffsrechten sicher geschützt sein. Falls vorgenannte Regelung nicht möglich ist, müssen folgende Regeln eingehalten werden: • Länge: – mindestens 12 Zeichen (sofern technisch machbar). • Zusammensetzung: – Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen, – mindestens drei dieser Elemente müssen enthalten sein. • Gültigkeit: – Bei einem Haupt-Release Wechsel ist das Passwort zu ändern. • Verwendung: – Es ist nur eine statische Verwendung erlaubt. Das Passwort darf nicht durch Personen für Arbeiten auf IKT-Systemen oder Anwendungen verwendet werden. • Aufbewahrung / Dokumentation: – Das Passwort muss für Notfälle und/oder Wartungsarbeiten schriftlich, in sicherer Form (z.B. einem Safe), hinterlegt sein. – Der Umgang mit Passwortänderungen muss im ISDS-Konzept oder Betriebskonzept des Systems resp. der Anwendung beschrieben sein. • Ausnahme: – Die vorerwähnte Regelung gilt nicht für die Authentifikation an Netzwerkgrenzen (z.B. an einem Firewallsystem).	X	X	
8.4 (*9.2.2,9.4.3*)	Die VE verfügen über einen umgesetzten, dokumentierten und seitens des zuständigen ISBD genehmigten Prozess zur Rücksetzung vergessener, abgelaufener oder gesperrter Mittel zur Authentifizierung.	X	X	
8.5 (*9.2.5*)	Die Verantwortlichen von Anwendungen, Systemen und Datensammlungen prüfen jährlich die Richtigkeit und Notwendigkeit der erteilten Benutzerrechte.	X	X	

[18] Siehe dazu den Anhang zu den Funktionsaccounts in der Zugriffsmatrix

9 Zugangskontrolle für IKT-Systeme und Anwendungen (*9.4*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
9.1 (*9.4.1, 9.4.4*)	Administrative Aufgaben in Anwendungen, welche lokale Administratorenrechte benötigen, werden von dedizierten IKT-Systemen aus erledigt. Für Anwendungen mit erhöhtem Schutzbedarf muss im ISDS-Konzept festgehalten werden ob - und wenn ja - welche administrativen Tätigkeiten von dedizierten IKT-Systemen erledigt werden müssen.	X	X	
9.2 (*9.4.4*)	Administrative Aufgaben erfordern die Nutzung gesonderter personengebundener administrativer Benutzerkonten. Diese Benutzerkonten bzw. die Systeme dürfen keinen Zugang zum Internet und zur Bürokommunikation (i.e.Mailbox) besitzen. Der Nutzung dieser Konten auf Bürokommunikations-Endgeräten ist zu unterbinden. Die Administration ist über dedizierte und gesondert abgesicherte IKT-Systeme auszuführen. Für den Zugriff auf diese administrative Managementebene bzw. auf die zu administrierenden Zielsysteme ist eine 2-Faktor-Authentifizierung umzusetzen. Die Administration erfolgt auf einem (logischen) getrennten Administrationsnetz. Wenn technisch nicht umsetzbar, muss die Art und Weise des Administrationszugangs in einem ISDS-Konzept beschrieben werden.		X	
9.3 (*9.4.2*)	Die für den Authentifikationsprozess zur Verfügung stehende Zeit muss, soweit technisch möglich, begrenzt werden.		X	
9.4 (*9.4.2*)	Systemzugriffssperren müssen nach maximal 15 Minuten automatisch aktiviert werden. Eine manuelle Aktivierung muss ebenfalls möglich sein. Ist eine entsprechende Sperrung aus technischen Gründen nicht möglich, muss der Zugang zu unbeaufsichtigten Arbeitsplätzen mit aktiven Sessionen geschützt werden (z.B. Abschliessen des Raumes). Ausnahmen zu dieser Massnahme müssen in einem ISDS-Konzept beschrieben werden.	X	X	

10 Kryptographie (*10*)

10.1 Kryptographische Massnahmen (*10.1*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
10.1.1 (*10.1.1*)	Die eingesetzten kryptografischen Verfahren und Methoden müssen dem Stand der Technik[19] entsprechen.	X	X	
10.1.2	Massnahme ist mit der Überarbeitung 2016 weggefallen.			
10.1.3 (*10.1.1, 13.1.2*)	Beim Einsatz asymmetrischer Kryptosysteme müssen die Zertifikate von der Swiss Government PKI oder von einer vom jeweiligen LE akzeptierten CA ausgestellt sein. Wo technisch nicht umsetzbar, dürfen Zertifikate anderer anerkannten Zertifikatsaussteller verwendet werden. Dies ist in einem ISDS-Konzept zu beschreiben.		X	

[19] Link: https://intranet.isb.admin.ch/dam/isb_kp/de/dokumente/ikt-vorgaben/sicherheit/KryptografieGrundschutz_V1-0.pdf.download.pdf/KryptografieGrundschutz_V1-0.pdf

10.1.4 *(10.1.1)*	Die Verwaltung kryptographischer Schlüssel, einschliesslich Methoden zur Handhabung des Schutzes kryptographischer Schlüssel und der Wiederherstellung verschlüsselter Daten im Falle verlorener, kompromittierter oder beschädigter Schlüssel sind zu Dokumentieren und periodisch auf ihre Zuverlässigkeit hin zu testen.		X	
10.1.5	Die Zertifikatsstores müssen durch den LE verwaltet werden. Wo nicht umsetzbar, dürfen Zertifikatsstores anderer anerkannten Zertifikatsaussteller (z.B. bei Multifunktionsgeräten) verwendet werden. Dies ist in einem ISDS-Konzept zu beschreiben.		X	
10.1.6	Die Liste der vertrauenswürdigen CAs, muss durch den LE verwaltet werden.		X	

11 Physische und umgebungsbezogene Sicherheit (*11*)

11.1 Sicherheitsbereiche (*11.1*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
11.1.1 (*11.1*)	Für den physischen Schutz der IKT sind bei baulichen Vorhaben die Vorgaben des BBL und des Bundessicherheitsdienstes einzuhalten. Die Beurteilung und die Festlegung der erforderlichen Sicherheitsmassnahmen erfolgt risikobasiert und objektspezifisch individuell. Dafür ist eine enge Zusammenarbeit zwischen den beteiligten Stellen notwendig. Die physischen Sicherheitsmassnahmen sind dabei ergänzend zu den organisatorischen und technischen Sicherheitsmassnahmen zu verstehen.	X	X	
11.1.2 (*11.2.1*)	Netzwerkkomponenten müssen soweit als möglich vor dem physischen Zugriff durch Unbefugte geschützt werden.	X	X	
11.1.3 (*13.1*)	Massnahme ist mit der Überarbeitung 2016 weggefallen. Der Kontext ist in Massnahme 13.1.4 geregelt.			

12 Betriebssicherheit (*12*)

12.1 Betriebsverfahren und Verantwortlichkeiten (*12.1*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
12.1.1 (*12.1.1*)	IKT-Mittel müssen in Bezug auf Installation, Betrieb, Wartung und Benutzung mindestens in folgenden Punkten stets aktuell dokumentiert sein: • System-Hardware, • Betriebssystem und systemnahe Software, • Anwendungskomponenten (Programme, Datenstrukturen, Modifikationen, Parametrisierung, usw.), • Sicherheitsrelevante Einstellungen und Funktionen. • Lebenszyklus (Lifecycle)	X	X	
12.1.2 (*12.1.2*)	Im Rahmen des Änderungsmanagements (Changemanagements) von Hardware und Software müssen die geschäftskritischen und sicherheitstechnisch wichtigen Funktionen auf ihre Funktionstüchtigkeit überprüft und gegebenenfalls angepasst werden.	X	X	
12.1.3 (*12.1.2*)	Änderungsaufträge (Change request) an den Betrieb müssen nachvollziehbar erfolgen.	X	X	

12.1.4 (*12.1.2*)	Entwicklungs-, Integrations-, Schulungs- und Testumgebungen etc. müssen von produktiven Umgebungen[20] logisch getrennt sein. Ausnahmen sind in einem ISDS-Konzept zu beschreiben.		X	

12.2 Schutz vor Schadsoftware (Malware) (*12.2*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
12.2.1 (*12.2.1*)	Die gesamte IKT muss durch aktuell gehaltene Software vor Schadsoftware-Befall geschützt werden[21]. Basierend auf der Malwareschutzstrategie erstellen die LE ein Malwareschutzkonzept, in welchem mindestens geregelt ist: • Prozesse und Verantwortlichkeiten, • Aktualisierung der Software zum Malwareschutz, • Festlegung der Schwerpunkte und Periodizität des Scannings (z. B. Clients, Server, Datenspeicher), • Technische Umsetzung.	X	X	X
12.2.2 (*12.2.1, 16.1.2*)	Bei Verdacht auf Malwarebefall ist der Servicedesk umgehend zu informieren. Das detaillierte Vorgehen (inkl. dem Trennen von Systemen vom Netz) ist in den entsprechenden Prozessen zu regeln.	X	X	X
12.2.3 (*12.2.1*)	Bei Arbeitsplatzsystemen (z.B. Laptops), die nicht permanent vernetzt sind, müssen mindestens einmal pro Monat, die Sicherheits-Updates eingespielt werden.	X	X	X
12.2.4 (*12.2.1 14.1.1*)	Die Autorun-Funktion beim Anschluss von externen Datenträgern ist bei allen Betriebssystemen (Arbeitsplatzsysteme und Server) zu deaktivieren.		X	

12.3 Backup (*12.3*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
12.3.1 (*12.3.1*)	Die Rekonstruktion und Wiederverwendbarkeit von Daten nach einem Datenverlust muss durch den verantwortlichen LE in einem Datensicherungskonzept beschrieben werden.		X	
12.3.2 (*12.3.1*)	Die Wiederherstellung von Daten muss periodisch geübt werden. Die Verwendbarkeit der Daten muss vom LB bestätigt werden.	X	X	

12.4 Aufzeichnung und Überwachung (*12.4*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
12.4.1 (*12.4.1 12.4.3*)	Folgende Aktivitäten sind (möglichst in pseudonymer Form) für IKT-Systeme und Anwendungen zweckgebunden und nachvollziehbar aufzuzeichnen, zu überwachen und zeitnah auszuwerten: • System-Boot und -Shutdown, • Gescheiterte Authentifikationsversuche (inklusive eindeutiger Identifikation der Herkunft), • Gescheiterte Objektzugriffe, • Vergabe und Änderung von Privilegien, • Alle Aktionen, die erhöhte Privilegien benötigen.	X	X	

[20] Systeme, Anwendungen, Daten

[21] Siehe "Malware Strategie für die Bundesverwaltung"

12.4.2 (*12.4.4*)	Die Systemzeit muss grundsätzlich zentral synchronisiert werden und darf nur autorisiert verändert werden.		X	
12.4.3 *(12.4.1)*	Die LE sind für die technische System- und Netzüberwachung verantwortlich.		X	
12.4.4 *(11.2.4)*	Serversysteme mit hohem Schutzbedarf sind periodisch einer Integritätsprüfung[22] zu unterziehen damit unberechtigte Veränderungen festgestellt werden. Unerwartete Veränderungen müssen in der Folge von System- und Sicherheitsspezialisten genau analysiert werden. Unrechtmässig veränderte Systeme müssen in jedem Fall sofort vom Netzwerk getrennt und gesichert werden. Nach einer allfälligen forensischen Analyse müssen verseuchte Systeme in jedem Fall vollständig gelöscht und neu installiert werden.		X	

12.5 Kontrolle von Software im Betrieb (*12.5*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
12.5.1 (*12.5.1*)	Die Authentizität der Software ist zu prüfen. Nicht autorisierte Veränderungen sind zu analysieren und zu bereinigen.	X	X	

12.6 Schwachstellenmanagement (*12.6*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
12.6.1 (*12.6.1*)	Fehlerkorrekturen (Patches) sind geprüft und schnellstmöglich zu installieren. Es sind Prozesse zu implementieren die eine zeitgerechte Fehlerkorrektur sicherstellen. Besonders zu berücksichtigen sind Systemkomponenten, Programme der Büroautomationsumgebung, Internet-Browser und deren Zusatzprogramme.	X	X	
12.6.2 (*12.6.1*)	Alle Anwendungen und IKT-Systeme sind • vor der Inbetriebnahme und • im laufenden Betrieb, periodisch, insbesondere bei substantiellen Anpassungen auf Schwachstellen zu prüfen. Die Ergebnisse müssen dokumentiert sein. Entdeckte Schwachstellen müssen vor Inbetriebnahme beurteilt und entsprechend behoben werden. Insbesondere Anwendungen und IKT-Systeme mit Zugang zum Internet dürfen in der Produktion keine kritischen Schwachstellen aufweisen. Verwundbarkeiten betreffend Web-Anwendungen müssen nach den aktuellen Top 10 Risiken nach OWASP (Open Web Application Security Project) geprüft und entsprechend beseitigt werden.	X	X	
12.6.3	Massnahme mit der Überarbeitung 2016 weggefallen. Sie wurde in Massnahme 12.6.2 integriert.			

[22] Z.B. mittels Anwendung von Hash-Funktionen über Server

12.7 Auswirkungen von Audits auf Informationssysteme (*12.7*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
12.7.1 (*12.7.1*)	Audit-Anforderungen und -Aktivitäten im Zusammenhang mit betriebsrelevanten IKT-Systemen müssen sorgfältig geplant, dokumentiert und vertraglich vereinbart werden, um Unterbrechungen der Geschäftsabläufe zu minimieren.	X	X	
12.7.2 *(18.2)*	Audits sind von einer unabhängigen Stelle durchzuführen.	X	X	

13 Kommunikationssicherheit (*13*)

13.1 Management der Netzsicherheit (*13.1*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
13.1.1 (*13.1.1*)	Für Netze sind folgende Dokumentationen stets aktuell zu halten: • Eigner und Betreiber des Netzes, • Netztopologie inklusive ihrer aktiven Komponenten und deren Konfigurationen, • Administrationsvorgaben für aktive Netzwerkwerkkomponenten.		X	
13.1.2 (*13.1.2, 13.1.3)*	Wenn auf einer physischen Einheit eine oder mehrere Virtualisierungen (z.B. Systeme, Anwendungen, Netze, Speicher der IKT) betrieben werden und diese nicht der gleichen Netzzone angehören, muss mittels eines durch den LE genehmigten ISDS-Konzept nachgewiesen werden, dass die Risiken mindestens gleich tragbar zur einer physisch getrennten Lösung sind. Der LE informiert den LB im Voraus über Änderungen welche Auswirkungen auf das genehmigte ISDS-Konzept haben (z.B. durch Änderungen an einer virtualisierten Plattform).	X	X	
13.1.3 (*13.1.2)*	Die Netzwerkkomponenten müssen vor Angriffen geschützt werden. Die getroffenen Schutzmassnahmen sind zu dokumentieren.		X	
13.1.4 (*13.1.2)*	Alle konfigurierbaren, aktiven Netzwerkkomponenten müssen vor unberechtigtem Zugriff geschützt werden. Es gelten folgende Anforderungen: • Der Zugriff auf aktive Netzwerkkomponenten ist mittels geeigneter Authentifizierung- und Autorisierungsmassnahmen sicherzustellen. Nach Möglichkeit werden 2-Faktor-Authentifizierungen mittels Klasse B Zertifikaten verwendet. Falls dies nicht möglich sind andere starke Authentifikationsverfahren (bspw. One Time Password) zu verwenden. • Der Fernzugriff erfolgt über eine verschlüsselte Verbindung aus einem dedizierten Management-Netz heraus (Analog zu 9.2). Der Zugang zum Management-Netzwerk ist mittels Verschlüsselung und 2-Faktor-Authentifizierung zu schützen. • Änderungen an den Konfigurationen aktiver Netzwerkkomponenten müssen entsprechend dem Konfigurations- bzw. Änderungsmanagement vorgenommen werden. • Konfigurationen dürfen nur geschützt übertragen werden. • Allfällige Zugangsdaten müssen in Konfigurationen geschützt gespeichert werden. • Alle Komponenten müssen über Mechanismen zur Deaktivierung ungenutzter Schnittstellen, Modulen und Funktionen verfügen.		X	

13.1.5 (*13.1.2)*	Die LE setzen Proxy-Sperrlisten ein. Der gesamte Internet-Verkehr der Netzdomäne Blau ist über einen Proxy Array des Bundes zu lenken. Des Weiteren gilt die Web Proxy Policy des ISB[23].		X	
13.1.6 (*13.1.2, 12.4.1)*	Sämtliche Verkehrsprotokolle (Logfiles und Proxy-Logs) von Netzübergängen (Firewalls und Gateways) müssen 2 Jahre aufbewahrt und regelkonform ausgewertet werden.		X	
13.1.7 (*13.1.2, 13.2)*	Die Vertraulichkeit und Integrität von schützenswerten Daten (z.B. Authentifikationsdaten) muss bei der Übertragung über Netzwerke geschützt werden.		X	
13.1.8	Massnahme ist mit der Überarbeitung 2015 weggefallen. Sie wurde in Massnahme 7.1.7 integriert.			
13.1.9 (*13.1.2)*	Authentisierungsvorgänge für den Zugriff auf nicht öffentliche Ressourcen des Bundes (OWA, RAS, etc.) dürfen nicht via Anonymisierungsdienste (wie z.B. das Tor-Netzwerk, private VPN-Services oder öffentliche Web-Proxies) erfolgen. Wo technisch nicht möglich, ist dies organisatorisch zu regeln (siehe auch Massnahme 1.1.1).	X	X	X
13.1.10 (*13.2.1*)	Öffentlich zugängliche Web-Seiten des Bundes sind mittels SSL/TLS (HTTPS) abzusichern. Die Zertifikate sind gemäss Massnahme 10.1.3 zu beziehen.		X	

14 Beschaffung, Entwicklung und Wartung von Informationssystemen (*14*)

14.1 Sicherheitsanforderungen an Informationssysteme (*14.1*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
14.1.1 (*14.1.1*)	Es dürfen nur homologierte drahtlose und drahtgebundene Peripherie-Geräte (z.B. Tastaturen, Drucker, Kopierer) eingesetzt werden. Diese sind durch den LE zu installieren. Risiken und Schutzmassnahmen werden in einem ISDS-Konzept ausgewiesen.	X	X	X
14.1.2 (*9.2.4*)	Bei der Auslieferung und Erstinstallation von Anwendungs- oder Systemkomponenten müssen vordefinierte Konten, Initialpasswörter, Privilegien oder Zugriffsrechte sofort kontrolliert und allenfalls angepasst oder gelöscht werden.	X	X	X
14.1.3 (*14.1.1*)	Grundschutzeinstellungen dürfen nur autorisiert umkonfiguriert, deinstalliert oder deaktiviert werden können.	X	X	
14.1.4 (*14.1.1*)	Jedes System darf nur die zu seiner Aufgabenerfüllung erforderliche Minimalkonfiguration (in Bezug auf installierte Software, Dienste, Konten, Administrationsoberfläche usw.) aufweisen. Dieses erfolgt mit dem Ziel, die Angriffsfläche zu reduzieren. Je nach Schutzbedarf und Umgebung sind gesonderte Härtungsmassnahmen angezeigt. Es ist ein zentrales Konfigurationsmanagement vorzusehen. Ausnahmen sind schriftlich zu dokumentieren und durch den ISBO des LE und des LB zu genehmigen.	X	X	

[23] Fundort: intranet.isb.admin.ch / IKT-Vorgaben / https://intranet.isb.admin.ch/dam/isb_kp/de/dokumente/ikt-vorgaben/sicherheit/Si004_Web_Proxy_Richtlinie_BV_V1-0_2016-10-04.pdf.download.pdf/Si004_Web_Proxy_Richtlinie_BV_V1-0_2016-10-04.pdf

14.2 Testdaten (*14.3*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
14.2.1 (*14.3.1*)	Testdaten sind entsprechend ihrer Einstufung zu schützen.	X	X	

15 Beziehungen mit Lieferanten (*15*)

15.1 Regelung der Dienstleistungserbringung durch Dritte (*15.2*)

Nr.	Anforderung	Umsetzung		
		LB	LE	BE
15.1.1 (*15.1, 15.2*)	Bei Dienstleistungen durch Dritte sind die IKT-Sicherheitsvorgaben des Bundes verbindlich und vertraglich zu regeln.	X	X	

15.2 Anforderungen angesichts des Risikos der Amtsgeheimnisverletzung (*15.2*)

		LB	LE	BE
15.2.1 *(15.2, 7.1.1)*	Die Offenbarung von Amtsgeheimnissen an externe IKT-Anbieter ist zu minimieren. Folgende Massnahmen sind zu berücksichtigen: • Der Remote Support darf nur über Verbindungen erfolgen die aus dem eigenen RZ (Bundesverwaltung) geöffnet werden • Der Remote Support ist zu überwachen (Aufzeichnen oder/und Vier-Augen-Prinzip) • Remote Support Verbindungen sind zu verschlüsseln • Daten nur mit dem Einwilligungsverfahren herausgeben oder nur via Inhaber der Daten • Auditierbarkeit der externalisierten Prozesse sicherstellen Weitere Anforderungen sind im Dokument «Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung»[24] beschrieben.	X	X	

[24] Siehe intranet.isb.admin.ch / IKT-Vorgaben Bund / Sicherheit https://intranet.isb.admin.ch/dam/isb_kp/de/dokumente/ikt-vorgaben/sicherheit/Si001-Anforderungen_zur_Reduktion_von_Amtsgeheimnisverletzungen.pdf.download.pdf/Si001-Anforderungen_zur_Reduktion_von_Amtsgeheimnisverletzungen.pdf

16 Umgang mit Informationssicherheitsvorfällen (*16*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
16.1 (*16.1*)	Die VE implementieren einen Sicherheitsvorfallbearbeitungsprozess[25] (Incident Management Prozess).	X	X	

17 Sicherstellung des Geschäftsbetriebs (*17*)

17.1 Fortbestand der Informationssicherheit (*17.1*)

Nr.	Anforderung	Umsetzung		
		LB	**LE**	**BE**
17.1.1 (*17.1, 17.2*)	Es müssen Pläne entwickelt, dokumentiert und umgesetzt werden, um • bei Störfällen, Notfällen und Katastrophenfällen den Betrieb aufrechtzuerhalten oder wieder herzustellen und • die Verfügbarkeit von IKT-Mitteln nach Unterbrechungen oder Ausfällen von kritischen Geschäftsprozessen im erforderlichen Mass und im erforderlichen Zeitraum sicherzustellen.	X	X	

[25] Siehe auch Sicherheitsvorfallbearbeitungsprozess (SVBP) des ISB