Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
Informatiksicherheit Bund SEC

Version 4.6

Si001 - IKT-Grundschutz in der Bundesverwaltung

vom 19. Dezember 2013 (Stand 1. April 2021)

Der Delegierte für Cybersicherheit erlässt gestützt auf Artikel 11, Absatz 1, Buchstabe e der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) vom 27. Mai 2020 nachfolgende Vorgabe. Diese stellt eine Vorgabe für den Grundschutz gemäss Artikel 14*c* CyRV dar.

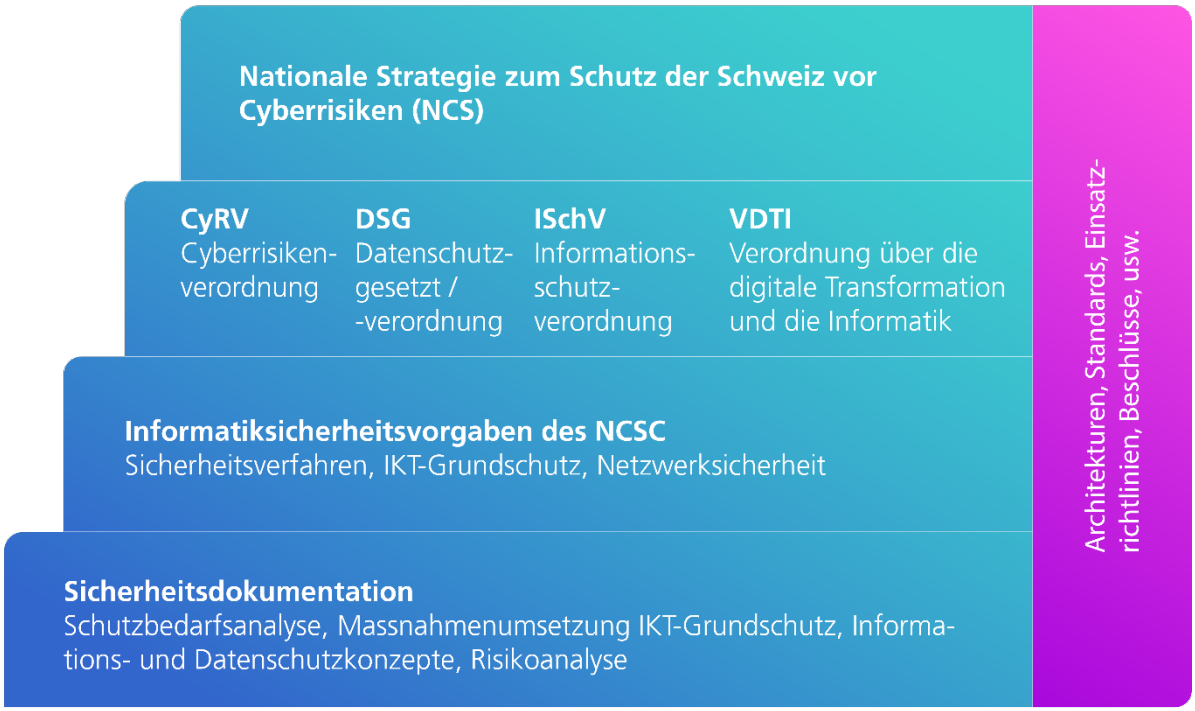

Abbildung 1: Zusammenfassung Informatiksicherheitsgrundlagen

Inhaltsverzeichnis

1 Allgemeine Bestimmungen zum IKT-Grundschutz

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

Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verpflichteten Verwaltungseinheiten (VE) zu dokumentieren und zu überprüfen (CyRV, Art.14 Abs. 3 und Art.14*c*).
Die Sicherheitsanforderungen sind mit den Leistungserbringern sowohl für die Entwicklung und den Betrieb als auch für die Ausserbetriebnahme von Informatikmitteln schriftlich zu vereinbaren. Die Verwaltungseinheiten dokumentieren und überprüfen die Umsetzung der Sicherheitsmassnahmen.

Die Dokumentation der Umsetzung des IKT-Grundschutzes ist mindestens von der oder dem Informatiksicherheitsbeauftragten der Verwaltungseinheit (ISBO) zu prüfen[1]. Sie ist von der Auftraggeberin oder dem Auftraggeber und dem oder der Geschäftsprozessverantwortlichen zu genehmigen.

Weiter ist zu beachten das Dokumentationen wie bspw. Betriebshandbücher, Berechtigungslisten revisionsgerecht geführt werden.

1.1 Geltungsbereich

Der Geltungsbereich dieser Vorgaben richtet sich nach Artikel 2 CyRV.

1.2 Ausnahmen zu den Vorgaben des IKT-Grundschutzes

Das NCSC kann Ausnahmen bewilligen (CyRV, Art. 11, Abs. 1, Bst. f) 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 (CyRV, Art. 11, Abs. 1, Bst. f).
Die VE hat die dadurch entstehenden Risiken identifiziert, quantifiziert und in einem detaillierten Antrag dem NCSC 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 oder die ISBD entsprechend im Ausnahme-Prozess miteinbezogen wird, damit er seine Verantwortung jederzeit wahrnehmen kann.

- Das Informatikschutzobjekthat keinen erhöhten Schutzbedarf.
- Die IKT-Grundschutz-Unterschreitung betrifft nicht die Standarddienste und gefährdet ausschliesslich die eigene Verwaltungseinheit (VE).
- Der oder die Informatiksicherheitsbeauftragte hat geprüft, ob keine amtsinternen, departementsinternen oder gesetzlichen Regelungen eine Abweichung vom IKT-Grundschutz verhindern/verbieten.

[1] Bei den Standarddiensten ist sie von der oder dem Informatiksicherheitsbeauftragten für die Standarddienste zu prüfen.

- 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.
- Die Risiken, die sich durch die IKT-Grundschutz Unterschreitung ergeben, müssen, wenn immer möglich mit ergänzenden/alternativen Massnahmen reduziert werden. Die bekannten Restrisiken[2] sind, ähnlich wie in der CyRV Art.14*d* Abs.2 beschrieben, auszuweisen und den Auftraggeberinnen und Auftraggebern, den Geschäftsprozessverantwortlichen und der Leitung der Verwaltungseinheit schriftlich zur Kenntnis zu bringen.
- Der Leiter oder die Leiterin der Verwaltungseinheit entscheidet ob die bekannten Restrisiken in Kauf genommen werden. (CyRV Art.14d Abs.3).
- Der ISBD führt ein aktuelles Verzeichnis und bringt Entscheide über Abweichungen auf Anfrage dem NCSC zur Kenntnis.

Es werden in der Regel nur zeitlich befristete Ausnahmen bewilligt.

1.3 Ausführungsbestimmungen zum IKT-Grundschutz

Das NCSC erlässt mit der "Si003 - Netzwerksicherheit in der Bundesverwaltung" verbindliche Ausführungsbestimmungen zum IKT-Grundschutz.
Daneben publiziert es Empfehlungen zum IKT-Grundschutz. Diese Unterlagen finden sich auf der Homepage des NCSC[3] unter der entsprechenden Rubrik.

1.4 Verweis auf ISO-Standard

Die Sicherheitsmassnahmen orientieren sich an aktuellen internationalen Standards, insbesondere an den ISO-Standards die Informatiksicherheitsverfahren betreffend.
Der Verweis auf die ISO/IEC 27002:2013[4] Nummerierung wird in kursiver Schrift und in Klammern bei der jeweiligen Ziffer aufgeführt. Detaillierte oder weitergehende Ausführungen können zum besseren Verständnis auch dem Standard ISO/IEC 27002:2013 entnommen werden.

1.5 Einsatz von neuen Informations- und Kommunikationstechnologien

Will eine Verwaltungseinheit neue Informations- und Kommunikationstechnologien (Hard- und Software) oder bestehende Technologien in einem neuen Einsatzgebiet einsetzen, so muss sie die Technologien vor dem Einsatz einer Risikobeurteilung unterziehen. Das Ergebnis der Risikobeurteilung ist der oder dem zuständigen Informatiksicherheitsbeauftragten und dem NCSC vorzulegen.

[2] Risiken, die nicht oder nur ungenügend reduziert werden können.

[3] intranet.ncsc.admin.ch

[4] intranet.ncsc.admin.ch, Dokumentation > Sicherheitsrelevante Dokumente von Partnern > ISO-Normen

2 Minimale Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf

1 Informationssicherheitsleitlinien (*5*)

1.1 Richtungsvorgabe des Managements zur Informationssicherheit (*5.1*)

Nr.	Anforderung	Verantwortlich Umsetzung[5]	Art[6]
1.1.1	Anforderung ist mit der Überarbeitung 2019 weggefallen.	-	-
1.1.2	Anforderung ist mit der Überarbeitung 2019 weggefallen.	-	-
1.1.3	Anforderung ist mit der Überarbeitung 2019 weggefallen.	-	-

2 Organisation der Informatiksicherheit (*6*)

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

Nr.	Anforderung	Verantwortlich Umsetzung	Art
2.1.1 (*6.2.1*)	Nur Smart Devices, welche über ein Mobile Device Management (MDM)[7] verwaltet werden, dürfen mit Systemen der Bundesverwaltung kommunizieren. Ausgenommen davon sind anonyme und personalisierte Zugriffsmöglichkeiten zu E-Government-Anwendungen oder öffentliche Web-Auftritte der Bundesverwaltung.	LB	O
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. Ausgenommen davon sind die dafür bewilligten Anwendungen (z.B. Anwendungen zur verschlüsselten Kommunikation[8]).	BE	O
2.1.3	Anforderung ist mit der Überarbeitung 2018 weggefallen.	-	-
2.1.4	Anforderung ist mit der Überarbeitung 2018 weggefallen.	-	-
2.1.5	Anforderung ist mit der Überarbeitung 2018 weggefallen. Sie ist in der Anforderung 6.2 enthalten.	-	-

[5] Verantwortlich für die Umsetzung: Leistungsbezüger (LB), Leistungserbinger (LE), Benutzer (BE). Diese Zuteilung gilt als Indikation. Wenn anders geregelt, muss es zwischen die Beteiligten schriftlich vereinbart werden.

[6] Art: Organisatorisch (O), Technisch (T), Hinweis (H)

[7] Siehe dazu die IKT-Vorgabe «E021 - Einsatzrichtlinie Smartphone / Smarttablet Sync» auf intranet.isb.admin.ch, IKT-Vorgaben > Einsatzrichtlinien > E021 - Einsatzrichtlinie Smartphone/Smarttablet Sync

[8] Siehe dazu die IKT-Vorgabe «E027 – Einsatzrichtlinie Verschlüsselte Sprachkommunikation (VSK)» auf intranet.isb.admin.ch, IKT-Vorgaben > Einsatzrichtlinien > E027 - Einsatzrichtlinie Verschlüsselte Sprachkommunikation (VSK)

2.1.6 (*6.2.1*)	Der LE implementiert einen Prozess, der den Umgang mit zu reparierenden, verlorenen oder gestohlenen Smart Devices regelt. Diese Regelung muss den Verwaltungseinheiten in geeigneter Form zur Kenntnis gebracht werden. Der Prozess muss mindestens das Zurücksetzen des Smart Devices (auf die Grundeinstellung = Verlust sämtlicher Daten) beinhalten.	LE	O
2.1.7	Anforderung ist mit der Überarbeitung 2018 weggefallen.	-	-
2.1.8 (*6.2.1*)	Der Zugang zu Smart Devices muss mittels Passwort, PIN oder biometrischen Merkmalen (Touch ID, usw.) geschützt werden. *Passwörter* und/oder *PIN* müssen mindestens 6 Zeichen enthalten. Trivial-Kombinationen wie Benutzer-ID, Name, Vorname, Geburtsdatum oder Ziffernfolgen wie 111111, 123456 sind verboten. Spätestens nach drei Minuten Inaktivität ist das Smart Device zu sperren und das Passwort, der PIN oder die biometrischen Merkmale neu einzugeben.	LE BE	T O
2.1.9	Anforderung ist mit der Überarbeitung 2018 weggefallen. Sie ist in der Anforderung 2.1.1 enthalten.	-	-
2.1.10	Anforderung ist mit der Überarbeitung 2016 weggefallen.	-	-
2.1.11	Anforderung ist mit der Überarbeitung 2018 weggefallen. Sie ist in der IKT-Teilstrategie für das mobile Arbeiten in der Bundesverwaltung enthalten.	-	-
2.1.12	Anforderung ist mit der Überarbeitung 2018 weggefallen.	-	-

3 Personalsicherheit und Führungsverantwortung (*7*)

3.1 Verantwortung des Managements (*7.2.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
3.1.1 (*7.2.2*)	Die Mitarbeitenden müssen in Bezug auf das Informatikschutzobjekt stufen- und funktionsgerecht im Bereich Informatiksicherheit geschult und sensibilisiert werden. Sie kennen dabei ihre Verantwortlichkeiten.	LB	O
3.1.2 (*7.3.1, 9.2.1*)	Die Benutzerrechte der Mitarbeitenden auf Zutritt, Zugang und Zugriff zu Informatikschutzobjekten müssen aktuell gehalten werden. Sie müssen umgehend an veränderte Verhältnisse angepasst werden, wenn die Anstellung, der Auftrag oder eine entsprechende Nutzungsvereinbarung der Mitarbeitenden geändert oder beendet wird. Ein Prozess für die Behandlung unbenutzter Konten muss eingerichtet werden.	LB	O
3.1.3 (*7.1*)	Die Notwendigkeit einer Personensicherheitsprüfung muss, in Bezug auf den Zugriff auf das Informatikschutzobjekt, geprüft werden.[9]	LB	O

[9] Siehe Verordnung über die Personensicherheitsprüfung (PSPV)

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

Nr.	Anforderung	Verantwortlich Umsetzung	Art
3.2.1	Anforderung ist mit der Überarbeitung 2018 weggefallen.	-	-

4 Management von organisationseigenen Werten (*8*)

4.1 Verantwortung für organisationseigene Werte (*8.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
4.1.1	Anforderung ist mit der Überarbeitung 2018 weggefallen.	-	-
4.1.2 (*11.2.6*)	Bei der Verwendung privater IKT-Mittel, inkl. privat beschaffter Software zu geschäftlichen Zwecken, ist der Schutzbedarf der entsprechenden Informationen und Daten zu gewährleisten.	BE	O
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[10] zulässig, welche die sicherheitsrelevanten Belange regelt.	LB	O

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

Nr.	Anforderung	Verantwortlich Umsetzung	Art
5.1 (*8.3.1, 8.3.2, 8.3.3*)	Die LB und LE erstellen ein Konzept für den Umgang mit datenhaltenden Informatikschutzobjekten (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 der oder dem zuständigen ISBO oder ISBD zu regeln.	LB	O

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

Nr.	Anforderung	Verantwortlich Umsetzung	Art
6.1 (*8.3.3, 18.1.5*)	Arbeitsplatzsysteme (Notebooks, Desktops) müssen durch eine vollständige Diskverschlüsselung gegen Daten-/Informationsabfluss (Diebstahlschutz) geschützt sein.	LE	T
6.2 (*16.1.2*)	Der Benutzer hat den Verlust eines Gerätes (Arbeitsplatzsysteme, Smart Devices, usw.) unverzüglich dem Servicedesk des LE zu melden.	BE	O

7 Zugriffskontrolle (*9*)

7.1 Anforderungen an die Zugriffskontrolle (*9.1*)

[10] z.B. Verträge mit Externen, Einsatzrichtlinien zum Mobilen Arbeiten

Nr.	Anforderung	Verantwortlich Umsetzung	Art
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. Für den Zugriff in eine Zone gelten die Bestimmungen aus "Si003 - Netzwerksicherheit in der Bundesverwaltung"[11].	LE	T
7.1.2 (*9.1.1, 9.4.3*)	Anforderung ist mit der Überarbeitung 2019 weggefallen.	LE	T
7.1.3	Anforderung ist mit der Überarbeitung 2017 weggefallen. Sie ist in der Anforderung 8.1 enthalten.	-	-
7.1.4 (*9.4.1, 9.2.5*)	Den Benutzern sind auf IKT-Mitteln nur die Rechte einzuräumen, die sie zwingend benötigen. Die Verantwortlichen von Anwendungen, Systemen und Datensammlungen prüfen jährlich die Richtigkeit und Notwendigkeit der erteilten Benutzerrechte.	LB	O
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.	LE	T
7.1.6 (*6.1.2*)	Die Gewaltentrennung zwischen Bewilligung und Vergabe von Zugriffsrechten ist zu berücksichtigen und zu dokumentieren. Ausnahmen zu dieser Anforderung müssen im Dokument «Massnahmenumsetzung zum IKT-Grundschutz» oder in einem ISDS-Konzept beschrieben werden.	LB	O
7.1.7 (*9.2.3*)	Der Zugriff von Personen auf Arbeitsplatz- und Serversysteme der Bundesverwaltung darf nur über eine 2-Faktor-Authentisierung möglich sein.[12] Ausnahmen siehe Dokument «Antrag für unpersönlicher Account (E- und F-Accounts)»[13]. Kann dies nicht gewährleistet werden, ist die entsprechende Lösung in einem ISDS-Konzept zu beschreiben.	LE	T
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).	LE	T
7.1.9 (*9.1.2*)	Ein uneingeschränkter Zugriff[14] darf nur verschlüsselt erfolgen.	LE	T

[11] intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Si003 - Netzwerksicherheit in der Bundesverwaltung

[12] BRB vom 04. Juni 2010

[13] intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Grundschutz > Si002-Hi01 - Antrag für unpersönlicher Account (E- und F-Accounts)

[14] Definition gemäss « Si003 – Netzwerksicherheit in der Bundesverwaltung »; intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Si003 - Netzwerksicherheit in der Bundesverwaltung

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.	LE	O
7.1.11	Nicht interaktive Dienst-Accounts (z.B. Service-Accounts): • müssen einzigartig sein (ein Account pro Dienst); • dürfen nur die minimalen Privilegien haben, die sie benötigen.	LE	T

8 Authenfizierungsmittel (*9.4*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
8.1 (*9.4.3*)	Passwortregeln für die Personenauthentifikation: • Länge: – Benutzerpasswort mind. 10 Zeichen – Administratorenpasswort mind. 12 Zeichen – Für den Login mit der PIN-Karte gelten die Vorgaben des Certification Service Providers (CSP). • Zusammensetzung: – Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen – mindestens drei dieser Elemente müssen enthalten sein – Trivialpasswörter wie Benutzer-ID, Name, Vorname, Geburtsdatum 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 • Fehlversuche: – max. 5, anschliessend muss die Benutzer-ID gesperrt werden • Weitergabe und Ablage: – Das Passwort oder die PIN ist persönlich und darf nicht weitergegeben werden. – Passwörter müssen geschützt abgelegt werden.[15] • Einmaligkeit: – Für jedes System und jeden Account muss ein eigenes, einmaliges Passwort benutzt werden. <u>Bei Verdacht, dass Unberechtigte ein Passwort oder eine PIN kennen, ist das jeweilige umgehend zu ändern.</u> Ausnahmen zur Zusammensetzung müssen schriftlich, entweder im Dokument «Massnahmenumsetzung zum IKT-Grundschutz» oder in einem ISDS-Konzept, festgehalten werden.	LE BE	T O
8.2 (*9.4.3*)	Passwortanforderungen für unpersönliche Personenidentifikation[16]: • Unpersönliche Benutzer-ID oder Passwörter sind so wenig wie möglich zu vergeben. • Von den Passwortanforderungen gemäss Anforderung 8.1 darf nur abgewichen werden wenn – mit dieser Benutzer-ID/Passwort ausschliesslich auf Anwendungen mit generellem Schutzbedarf (Grundschutz) zugegriffen wird oder – ein genehmigtes ISDS-Konzeptund eine Bewilligung des oder der ISBD vorliegt.	LB	O

[15] Mit einem Passwort-Verwaltungsprogramm (z.B. KeePass).

[16] Siehe dazu das Hilfsmittel zu den Funktionsaccounts: intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Grundschutz > Si002-Hi01 - Antrag für unpersönlicher Account (E- und F-Accounts)

8.3 (*9.4.2*)	Nicht interaktive Dienst-Accounts 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 für das Passwort eingehalten werden: • Länge: – mindestens 28 Zeichen (sofern technisch machbar). • Zusammensetzung: – Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen, – mindestens drei dieser Elemente müssen enthalten sein. • Automatisierte Erneuerung: – Falls das System eine automatisierte Erneuerung des Passwortes unterstützt, muss diese aktiviert sein und mit einer möglichst kleinen Periodizität eingesetzt werden. • Einmaligkeit: – Für jedes System und jeden Account muss ein eigenes, einmaliges Passwort benutzt werden. • 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.	LE	T
8.4 (*9.2.1, 9.2.2, 9.4.3*)	Die VE verfügen über einen umgesetzten und dokumentierten Prozess zur Rücksetzung vergessener, abgelaufener oder gesperrter Mittel zur Authentifizierung.	LB	O
8.5	Anforderung ist mit der Überarbeitung 2018 weggefallen. Sie ist in der Anforderung 7.1.4 enthalten.	-	-

9 Zugriffskontrolle auf IKT-Systeme und Anwendungen (*9.4*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
9.1 (*9.4.1, 9.4.4*)	Administrative Aufgaben • welche lokale Administratorenrechte benötigen, sind von dedizierten IKT-Systemen (z.B. Privileged Access Workstation) aus zu erledigen. • sind mit gesonderten, personengebundenen administrativen Konten zu erledigen. 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.	LE LB	T
9.2 (*9.4.4*)	Die Administration von Serversystemen erfolgt auf einem (logischen) getrennten Administrationsnetz und ist über dedizierte und gesondert abgesicherte IKT-Systeme auszuführen. Dieses Netz darf keinen Zugriff zum Internet und zur Bürokommunikation (i.e. Mailbox) haben. Wenn technisch nicht umsetzbar, muss die Art und Weise des Administrationszugangs in einem ISDS-Konzept beschrieben werden. Für den Zugriff auf diese administrative Managementebene bzw. auf die zu administrierenden Zielsysteme ist eine 2-Faktor-Authentifizierung umzusetzen.	LE	T
9.3 (*9.4.2*)	Die für den Authentifikationsprozess zur Verfügung stehende Zeit[17] muss, soweit technisch möglich, begrenzt werden.	LE	T
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 Anforderung müssen im Dokument «Massnahmenumsetzung zum IKT-Grundschutz» oder in einem ISDS-Konzept beschrieben werden.	LE	T

10 Kryptographie (*10*)

10.1 Kryptographische Anforderungen (*10.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
10.1.1 (*10.1.1*)	Die eingesetzten kryptografischen Verfahren und Methoden müssen dem Stand der Technik[18] entsprechen.	LE	T
10.1.2	Anforderung ist mit der Überarbeitung 2016 weggefallen.	-	-

[17] Ab Beginn des Sessionaufbaus

[18] Empfohlene kryptografische Verfahren für die Bundesverwaltung findet man auf: https://intranet.ncsc.admin.ch > Dokumentation > Empfehlungen & Technologiebetrachtungen

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.	LE	T
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.	LE	T
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.	LE	T
10.1.6	Die Liste der vertrauenswürdigen CAs, muss durch den LE verwaltet werden.	LE	O

11 Physische und umgebungsbezogene Sicherheit (*11*)

11.1 Sicherheitsbereiche (*11.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
11.1.1 (*11.1*)	Die Notwendigkeit von baulichen und technischen Massnahmen zum physischen Schutz sind mit dem BBL, der armasuisse und dem Bundessicherheitsdienst zu klären.	LB	O
11.1.2 (*11.2.1, 11.2.3*)	IKT-Systeme müssen soweit als möglich vor dem physischen Zugriff durch Unbefugte geschützt werden.	LE	O
11.1.3	Anforderung ist mit der Überarbeitung 2016 weggefallen. Der Kontext ist in der Anforderung 13.1.4 geregelt.	-	-

12 Betriebssicherheit (*12*)

12.1 Betriebsverfahren und Verantwortlichkeiten (*12.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
12.1.1 (*8.1.1, 8.1.2, 12.1.1*)	Informatikschutzobjekte müssen in Bezug auf Installation, Betrieb, Wartung und Benutzung mindestens in folgenden Punkten stets aktuell dokumentiert sein: • System-Hardware, • Betriebssystem und systemnahe Software, • Anwendungskomponenten (z.B. Programme, Modifikationen, Parametrisierung), • Sicherheitsrelevante Einstellungen und Funktionen, • Lebenszyklus (Lifecycle), • Verantwortlicher.	LE LB	O

12.1.2 (*12.1.2, 14.2.4*)	Im Rahmen des Änderungsmanagements (Changemanagements) von Hardware und Software müssen die geschäftskritischen und sicherheitstechnisch wichtigen Funktionen auf ihre Funktionstüchtigkeit überprüft und gegebenenfalls angepasst werden.	LB	O
12.1.3 (*12.1.2*)	Änderungsaufträge (Change request) an den Betrieb müssen nachvollziehbar erfolgen.	LB	O
12.1.4 (*12.1.2*)	Entwicklungs-, Integrations-, Schulungs- und Testumgebungen etc. müssen von produktiven Umgebungen[19] logisch getrennt und selbst adäquat geschützt sein[20]. Ausnahmen sind im Dokument «Massnahmenumsetzung zum IKT-Grundschutz» oder in einem ISDS-Konzept zu beschreiben.	LE	T

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

Nr.	Anforderung	Verantwortlich Umsetzung	Art
12.2.1 (*12.2.1*)	Die gesamte IKT muss durch aktuell gehaltene Software vor Schadsoftware-Befall geschützt werden[21]. Basierend auf der Malwareschutzstrategie[22] 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.	LE	T
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.	BE LB	O
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.	BE	O
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.	LE	T

12.3 Backup (*12.3*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
12.3.1 (*12.3.1*)	Die Rekonstruktion und Wiederverwendbarkeit von Daten nach einem Datenverlust muss durch den verantwortlichen LE beschrieben und sichergestellt sein.	LE	O

[19] Systeme, Anwendungen, Daten

[20] z.B. Internet-Zugang nur durch virtualisierte Browser und E-Mail Client für Entwicklungsumgebungen

[21] Siehe "Malwareschutz Strategie für die Bundesverwaltung"

[22] intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > SB003 - IKT-Teilstrategie Malwareschutz

12.3.2 (*12.3.1*)	Im Auftrag des LB muss die Wiederherstellung von Daten geprobt werden. Die Verwendbarkeit der Daten muss vom LB bestätigt werden.	LE	T

12.4 Aufzeichnung und Überwachung (*12.4*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
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.	LE	T
12.4.2 (*12.4.4*)	Die Systemzeit muss zentral synchronisiert werden und darf nur autorisiert verändert werden.	LE	T
12.4.3 *(12.4.1)*	Eine angemessene technische System- und Netzüberwachung muss gewährleistet sein.	LE	O
12.4.4 *(12.5)*	Serversysteme mit hohem Schutzbedarf sind periodisch einer Integritätsprüfung[23] zu unterziehen damit unberechtigte Veränderungen festgestellt werden.[24] 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.	LE	T

12.5 Kontrolle von Software im Betrieb (*12.5*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
12.5.1 (*12.5.1*)	Die Authentizität der Software ist zu prüfen (z.B. Signaturen). Nicht autorisierte, festgestellte Veränderungen sind zu analysieren und zu bereinigen.	LE	T

[23] Siehe die Technologiebetrachtung «Integritätsprüfung von Systemen» für weitere Informationen an wie diese Anforderung zu verstehen ist, wie ihr heute entsprochen werden kann, welche Werkzeuge dafür existieren und wie diese Werkzeuge in der Bundesverwaltung einzusetzen sind: intranet.ncsc.admin.ch > Dokumentation > Empfehlungen und Technologiebetrachtungen

[24] BRB vom 16. Dezember 2009

12.6 Schwachstellenmanagement (*12.6*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
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, Software der Büroautomationsumgebung, Webanwendungen, Internet-Browser und deren Zusatzsoftware. Sind Fehlerkorrekturen aufgrund veralteter Systeme nicht mehr möglich, müssen Massnahmen zum Ersatz dieser Systeme getroffen werden (Lifecycle Management). Ist dieser Ersatz nicht möglich, ist der Weiterbetrieb (max. zwei Jahren) in einem ISDS-Konzept zu beschreiben.	LE LB	T O
12.6.2 (*12.6.1, 14.2.8, 14.2.9*)	Alle Anwendungen und IKT-Systeme (inkl. eigebundene Software-Komponenten) sind • während der Entwicklung • 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.	LE	T
12.6.3	Anforderung mit der Überarbeitung 2016 weggefallen. Sie wurde in der Anforderung 12.6.2 integriert.	-	-

12.7 Auswirkungen von Audits auf Informationssysteme (*12.7*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
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.	LB	O
12.7.2 *(18.2)*	Audits sind von einer unabhängigen Stelle durchzuführen.	LB	O

13 Kommunikationssicherheit (*13*)

13.1 Management der Netzsicherheit (*13.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
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.	LE	O
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 zu 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).	LE	O
13.1.3 (*13.1.2)*	Die Netzwerkkomponenten müssen vor Angriffen geschützt werden. Die getroffenen Schutzmassnahmen sind zu dokumentieren.	LE	T
13.1.4 (*13.1.2)*	Alle konfigurierbaren, aktiven Netzwerkkomponenten müssen vor unberechtigtem Zugriff geschützt werden. Es gelten folgende Anforderungen: • Der administrative 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.	LE	T

13.1.5 (*13.1.2)*	Sämtliche Netzkommunikationen unterliegen der "Si003 - Netzwerksicherheit in der Bundesverwaltung"[25], insbesondere die Kommunikationsbeziehungen mit dem Internet.	LE	T
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.[26] Die Logs sind von nachträglichen Manipulationen zu schützen.	LE	O
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.	LE	T
13.1.8	Anforderung ist mit der Überarbeitung 2015 weggefallen. Sie wurde in der Anforderung 7.1.7 integriert.		
13.1.9	Anforderung ist mit der Überarbeitung 2018 weggefallen.	-	-
13.1.10 (*13.2.1*)	Öffentlich zugängliche Webseiten des Bundes sind mittels SSL/TLS (HTTPS) abzusichern. Die Zertifikate sind gemäss der Anforderung 10.1.3 zu beziehen. Formulare auf diesen Webseiten sind vor automatisierten Angriffen zu schützen (z.B. mittels CAPTCHAs).	LE	T

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

14.1 Sicherheitsanforderungen an Informationssysteme (*14.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
14.1.1 (*14.1.1*)	Peripherie-Geräte (z.B. Tastaturen, Drucker, Präsentations-Systeme), welche integriert oder installiert (Treiber) werden müssen, sind durch die Beschaffungstellen des Bundes zu beschaffen.[27] Die Integrierbarkeit und die Sicherheit ist vorgängig durch die Beschaffungstelle bei den LE abklären zu lassen. Für die Nutzung von privaten Peripherie-Geräten beim Mobilen Arbeiten, gelten die entsprechenden Einsatzrichtlinien.	LE	T
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.	LE	T

[25] intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Si003 - Netzwerksicherheit in der Bundesverwaltung

[26] Siehe dazu die SR 172.010.442 «Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen»

[27] Siehe dazu auch den A-IS-Beschluss 66.10: Minimale Sicherheitsanforderungen an Geräte für die Ein- / Ausgabe von Dokumenten in der Büroautomation (Scanner, Drucker, Fax, Kopierer bzw. Kombinationen davon, oft auch als Multifunktionsgeräte bezeichnet)

14.1.3 (*14.1.1*)	Die Informatiksicherheitseinstellungen dürfen nur autorisiert umkonfiguriert, deinstalliert oder deaktiviert werden können.	LE	T
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. Dies 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 die oder den ISBO des LE und des LB zu genehmigen.	LE	T

14.2 Testdaten (*14.3*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
14.2.1 (*14.3.1*)	Testdaten sind entsprechend ihrer Einstufung zu schützen. Ist es unumgänglich, dass produktive Daten zu Testzwecken verwendet werden, sind diese gemäss ihrer Einstufung zu schützen.	LE	T

15 Beziehungen mit Lieferanten (*15*)

15.1 Regelung der Dienstleistungserbringung durch Dritte (*15.2*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
15.1.1 (*15.1, 15.2, 18.1.1, 18.1.2*)	Bei Dienstleistungen durch Dritte sind die Informatiksicherheitsvorgaben des Bundes verbindlich und vertraglich zu regeln. Die entsprechende Einwilligung der vorgesetzten Behörde ist gemäss den amts- bzw. departementsspezifischen Prozessen einzuholen.[28]	LB	O

[28] Eine Basis für die umzusetzenden organisationsspezifischen Einwilligungsprozesse ist im Dokument «Handlungsempfehlung zur operativen Umsetzung von Einwilligungsverfahren im Zusammenhang mit Art. 320 StGB» zu finden. Siehe intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Grundschutz > Si001 - Hi04 - Handlungsempfehlung zur operativen Umsetzung von Einwilligungsverfahren

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

Nr.	Anforderung	Verantwortlich Umsetzung	Art
15.2.1 *(15.2, 7.1.1)*	Die Offenbarung von Amtsgeheimnissen an externe IKT-Anbieter ist zu minimieren. Folgende Massnahmen sind zu treffen: • Der Remote Support auf IKT-Systeme erfolgt wenn möglich via Jumphost. Er muss bei Bedarf manuell und nur so lange wie nötig freigegeben werden; • Der Remote Support ist zu überwachen (Aufzeichnen oder/und Vier-Augen-Prinzip); • Remote Support Verbindungen sind zu verschlüsseln; • Daten dürfen nur mit dem Einwilligungsverfahren oder nur via Inhaber der Daten herausgegeben werden; • Die Auditierbarkeit der externalisierten Prozesse ist sicherzustellen. Die entsprechende Einwilligung der vorgesetzten Behörde und nach Möglichkeit der Inhaber der Daten ist gemäss den amts- bzw. departementsspezifischen Prozessen einzuholen.[29] Weitere Anforderungen sind im Dokument «Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung»[30] beschrieben.	LB	O

16 Umgang mit Informationssicherheitsvorfällen (*16*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
16.1 (*16.1*)	Es müssen Pläne entwickelt werden, um bei einem Sicherheitsvorfall, im Bezug auf das Informatikschutzobjekt, entsprechend reagieren zu können.[31]	LB	O
16.2 (*15.2, 16.1*)	Der Leistungserbringer muss bei Sicherheitsvorfällen oder Sicherheitslücken, die ihn selber betreffen, umgehend seine Leistungsbezüger darüber informieren. Entsprechende Log-Dateien sollen den Leistungsbezügern für Analysen zur Verfügung gestellt werden.	LE	O

[29] Eine Basis für die umzusetzenden organisationsspezifischen Einwilligungsprozesse ist im Dokument «Handlungsempfehlung zur operativen Umsetzung von Einwilligungsverfahren im Zusammenhang mit Art. 320 StGB» zu finden. Siehe intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Grundschutz > Si001 - Hi04 - Handlungsempfehlung zur operativen Umsetzung von Einwilligungsverfahren

[30] Siehe intranet.ncsc.admin.ch, Vorgaben & Hilfsmittel > Sicherheitsverfahren > Grundschutz > Si001-Hi03 - Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung

[31] Muss mit dem Sicherheitsvorfallbearbeitungsprozess (SVBP) der VE abgestimmt sein

17 Sicherstellung des Geschäftsbetriebs (*17*)

17.1 Fortbestand der Informationssicherheit (*17.1*)

Nr.	Anforderung	Verantwortlich Umsetzung	Art
17.1.1 (*11.2.2, 17.1, 17.2*)	Adaptiert an das Bedürfnis des Informatikschutzobjekts müssen Pläne entwickelt, dokumentiert und umgesetzt werden, um bei Störfällen, Notfällen und Katastrophenfällen den Betrieb des Informatikschutzobjekts aufrechtzuerhalten und wiederherzustellen (ITSCM). Massnahmen für die Sicherstellung von kritischen Geschäftsprozessen müssen definiert werden (BCM).[32]	LB	O

3 Weitere Aspekte zum IKT-Grundschutz

3.1 Übergeordnete Rahmenbedingungen

3.1.1 Archivierung

Die Anforderungen an die Archivierung von elektronischen Informationen richten sich nach den Vorgaben des Bundesarchives (Archivierungsgesetz, BGA[33]). Es koordiniert die Aktenführung und unterstützt die Organisationseinheiten bei deren Umsetzung.

3.1.2 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[34]) und in der Verordnung zum Bundesgesetz über den Datenschutz (VDSG[35]) geregelt.

Für eine korrekte Grundlage eines IKT-Vorhabens sind die Artikel 4, Absatz 1 und Artikel 14, Absatz 3 der CyRV ein wesentlicher Bestandteil.

3.1.3 Finanzkontrolle

Die Eidgenössische Finanzkontrolle ist das oberste Finanzaufsichtsorgan des Bundes. Sie richtet ihre Prüfungstätigkeit nach dem Finanzkontrollgesetz (FKG[36]).

3.1.4 BBL, armasuisse

Eine der Hauptaufgaben des Bundesamtes für Bauten und Logistik BBL ist die

[32] Muss mit dem Business Continuity Management (BCM) der VE abgestimmt sein

[33] SR 152.1

[34] SR 235.1

[35] SR 235.11

[36] SR 614.0

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.

3.1.5 Fachstelle PSP[37] 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.

3.2 Inkraftsetzung und kontinuierliche Überarbeitung

Die Vorgaben des NCSC zum IKT-Grundschutz, treten auf den 1. April 2021 in Kraft.
Das NCSC prüft diese sowie die Ausführungsbestimmungen periodisch auf ihre Aktualität.
Die aktuellste Version befindet sich der Homepage des NCSC.

3.3 Begriff Informatikschutzobjekte

Informatikschutzobjekte sind Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der Informatik, die in der Bundesverwaltung eingesetzt und somit geschützt werden müssen und entsprechend auch Gegenstand der Weisungen sind. (Art.3 Bst.h CyRV)

Bei der Definition und Abgrenzung eines Informatikschutzobjektes sind die betrieblichen und organisatorischen Aspekte zu berücksichtigen. Wenn notwendig sind mehrere Informatikschutzobjekte zu definieren, so dass mit der Übergabe von Projekt an den Betrieb die Verantwortlichkeiten, eindeutig und vollumfänglich den zuständigen Betriebsorganisationen, übertragen werden können. Es können auch mehrere Objekte zu einem Informatikschutzobjekt zusammengefasst werden, sofern sie zusammengehören und den gleichen Schutzbedarf aufweisen.

3.4 IKT-Portfolio

Die Sicherheitsdokumentation der Anwendungen muss zentral geführt werden. Im IKT-Portfolio (Cockpit IKT)[38] sind für die dort aufgeführten Anwendungen zumindest die Links zur jeweiligen Ablage zu dokumentieren.

[37] PSPV Art. 3

[38] W007 - Weisungen des Bundesrates zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes, vom 16. März 2018, Ziffer 2.2, Abs. 5

3.5 Verwendete Abkürzungen und Begriffe

Abkürzungen	***Bezeichnung***
BBL	Bundesamt für Bauten und Logistik
BE	Benutzer
CA	Certification Authority
CyRV	Cyberrisikenverordnung
https	Hypertext Transfer Protocol Secure
ID	Identifikator
IKT	Informations- und Kommunikationstechnologie
ISBD	Informatiksicherheitsbeauftragter Departement
ISBO	Informatiksicherheitsbeauftragter Verwaltungseinheit
ISDS	Informationssicherheits- und Datenschutz
LB	Leistungsbezüger
LE	Leistungserbringer
MDM	Mobile Device Management
NCSC	Nationales Zentrum für Cybersicherheit
OWASP	Open Web Application Security Project
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PSP	Personensicherheitsprüfung
PSPV	Verordnung über die Personensicherheitsprüfung
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VE	Verwaltungseinheit

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 personenbezogener Daten etc. Wo sich eine Vorschrift ausschliesslich auf Personendaten bezieht, wird dieser Terminus gewählt.
Schutzbedarfsanalyse	Erhebung der Anforderungen an die Sicherheit der Informatikschutzobjekte.
Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept)	Beschreibung der Sicherheitsmassnahmen und ihrer Umsetzung für die Informatikschutzobjekte sowie der Restrisiken.
Netzwerk	Einrichtung, welche die Kommunikation verschiedener IT-Systeme untereinander ermöglicht.
Zone	Logischer Verbund von IT-Systemen, die sich durch ähnliche Sicherheitsanforderungen auszeichnen und der gleichen Zonenpolicy unterliegen.
Zonenpolicy	Vom Inhaber einer Zone erstellte Beschreibung von Anforderungen und Vorgaben an die IT-Systeme der Zone, an die Zone selbst sowie an die für die Zone zulässige interne und externe Kommunikation.
Zonenmodell Bund	Generisches Modell für die Zonenbildung in der Bundesverwaltung.

3.6 Umsetzung IKT-Grundschutz und Übergangsbestimmungen

Die Verwaltungseinheiten haben den IKT-Grundschutz, sofern sie diesen nicht bereits einhalten, innert einer nützlichen Frist, spätestens innerhalb von 2 Jahren den Vorgaben anzupassen. Ist dies nicht möglich, haben sie gemäss Kap. 1.2 dieses Dokuments eine Ausnahme zu beantragen.

Weiter haben sie periodisch zu prüfen, ob die Umsetzung des IKT-Grundschutzes den aktuellen Weisungen des NCSC (vgl. Kap. 2 dieses Dokuments) entspricht. Folgende Anforderungen sind neu oder wurden verändert. Die Neuerungen sind ab dem Inkrafttreten dieser Vorgabe umzusetzen:

- 4.1.3*, 7.1.1, 12.3.1, 12.3.2, 12.6.2, 13.1.5, 13.1.10, 14.1.1* wurden verändert. (* per 01.04.2021 verändert)