



Version 5.0

Si001 – IT-Grundschutz in der Bundesverwaltung

vom 1. März 2022

Gestützt auf Artikel 11, Absatz 1, Buchstabe e der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) vom 27. Mai 2020 [CyRV] erlässt der Delegierte für Cybersicherheit nachfolgende Vorgabe zum IT-Grundschutz in der Bundesverwaltung.

Die Si003 – Netzwerksicherheit in der Bundesverwaltung, Version 3.1 vom 19. Dezember 2013 (Stand 1. April 2021) wird mit dem Inkrafttreten dieser Vorgabe ausser Kraft gesetzt.



Abbildung 1: Zusammenfassung Informatiksicherheitsgrundlagen

Inhaltsverzeichnis

1	Allgemeine Bestimmungen	3
1.1	Gegenstand	3
1.2	Geltungsbereich und rechtliche Rahmenbedingungen	3
1.3	Ausnahmen	3
2	Begriffe	4
3	Grundsätze und Prinzipien	6
4	Sicherheitsanforderungen.....	8
5	Inkraftsetzung und Übergangsbestimmungen	18
	Abkürzungen	19
	Referenzen.....	21
	Anhang A: Zonenmodell Bund.....	22
	Anhang B: Sicherheitsstufen für Authentifikations- und Identitätsnachweismittel.....	24
	Anhang C: Zonenpolicy «Netzdomäne blau»	26
	Anhang D: Zugriffsmatrix blaue Netzdomäne und SSZ.....	27
	Anhang E: Änderungen gegenüber Version 4.6 (Stand 1. Januar 2021)	28

1 Allgemeine Bestimmungen

1.1 Gegenstand

¹ Diese Vorgabe legt die minimalen organisatorischen, personellen und technischen Anforderungen an die Informatiksicherheit der Bundesverwaltung bzw. deren Informatikschutzobjekte (Schutzobjekte) gemäss Artikel 14 Absatz 2 CyRV fest.

² Jede Verwaltungseinheit (VE) ist für ihre Schutzobjekte selbst verantwortlich und muss für sie diese Vorgabe umsetzen und einhalten, bzw. deren Umsetzung und Einhaltung kontrollieren.

³ Die Umsetzung und Einhaltung dieser Vorgabe muss von der verantwortlichen VE nachvollziehbar dokumentiert sein (z.B. auf der Basis von [Si001-Hi01]). Dabei muss die Dokumentation mindestens von

- a) der oder dem Schutzobjektverantwortlichen (gemäss Kapitel 2 Absatz 1),
- b) der oder dem Informatiksicherheitsbeauftragten der verantwortlichen VE (ISBO),
- c) der Auftraggeberin oder dem Auftraggeber (bei einem Projekt) und
- d) der oder dem Geschäftsprozessverantwortlichen

überprüft und unterzeichnet sein. Die Unterzeichnenden bestätigen auch, dass gemäss ihrer Einschätzung alle am Betrieb des Schutzobjektes beteiligten Leistungserbringer (LE) die sie betreffenden Anforderungen erfüllen.

⁴ Die Kontrolle der Umsetzung und Einhaltung dieser Vorgabe muss von der verantwortlichen VE ebenfalls nachvollziehbar dokumentiert sein. Die Art und Weise, wie diese Kontrolle zu erfolgen hat, hängt auch vom Informatikschutzobjekt und dessen Schutzbedarf ab, und muss mit dem ISBO abgesprochen und mitdokumentiert sein. Für ein Schutzobjekt, das von einem oder mehreren internen LE im Auftrag der verantwortlichen VE betrieben wird, gilt die Kontrolle als erfüllt, wenn das Dokument «Massnahmenumsetzung zum IKT-Grundschutz» von den entsprechenden LE mitunterzeichnet ist.

1.2 Geltungsbereich und rechtliche Rahmenbedingungen

¹ Der Geltungsbereich dieser Vorgabe richtet sich nach Artikel 2 CyRV.

² Weitere rechtliche Rahmenbedingungen ergeben sich aus

- a) der Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) [ISchV] und den Weisungen über die detaillierten Bearbeitungsvorschriften zum Informationsschutz (Bearbeitungsweisung),
- b) der Bundesgesetzgebung über den Datenschutz für den Umgang mit Personendaten, sowie
- c) der Bundesgesetzgebung über die Archivierung für die Archivierung von Daten.

1.3 Ausnahmen

¹ Kann eine VE für ein Informatikschutzobjekt eine oder mehrere Anforderungen dieser Vorgabe nicht erfüllen, braucht sie gemäss Art. 11 Absatz 1 Buchstabe f der CyRV eine Ausnahmegewilligung. Diese kann auf eine der in den folgenden drei Absätzen 2 – 4 aufgeführten Arten erlangt werden.

² Die Anforderungen, die in Kapitel 4 mit einem Stern (*) markiert sind, sind aus der Sicht der Informatiksicherheit für die Bundesverwaltung weniger risikobehaftet. Für sie sind Abweichungen möglich, wenn sie im Dokument «Massnahmenumsetzung zum IKT-Grundschatz» oder im ISDS-Konzept begründet und dokumentiert sind. Die Ausnahme gilt dann als durch die gemäss Kapitel 1.1 Absatz 3 verantwortlichen Stellen bewilligt.

³ Ein ISBD kann einen formalen Ausnahmeantrag bewilligen oder die Kompetenz zur Ausnahmebewilligung an den ISBO der verantwortlichen VE delegieren, wenn die folgenden Voraussetzungen (kumulativ) erfüllt sind:

- a) Der ISBD ist in den Ausnahmebewilligungsprozess so eingebunden, dass er seine Verantwortung wahrnehmen kann.
- b) Bei der Ausnahme geht es ausschliesslich um die Verwendung von Informationen der verantwortlichen VE oder andere Schutzobjekte, die entweder keinen erhöhten Schutzbedarf haben oder einen erhöhten Schutzbedarf haben, der sich alleine auf Datenschutzanforderungen begründet.
- c) Die Ausnahme betrifft weder die IKT-Standarddienste noch eine andere VE.
- e) Alle in Kapitel 1.1 Absatz 3 aufgeführten Personen und die Leiterin oder der Leiter bzw. ein Geschäftsleitungsmitglied der verantwortlichen VE sind nachweislich mit der Ausnahme einverstanden.
- d) Der ISBD führt ein aktuelles Verzeichnis der erteilten Ausnahmebewilligungen und bringt diese auf Anfrage dem NCSC zur Kenntnis.

⁴ Alle anderen Ausnahmeanträge können über das IKT-Anforderungs- und Vorgabenmanagement Bund (P035) zuhanden des NCSC eingereicht werden. Im entsprechenden Antrag müssen die Unterschreitungen des IT-Grundschatzes begründet und mögliche sowie geplante Massnahmen zur Risikoreduktion aufgezeigt und diskutiert sein.

⁵ Ausnahmebewilligungen gemäss Absatz 4 sind immer zeitlich befristet (in der Regel auf zwei Jahre).

2 Begriffe

¹ Der Begriff **Informatikschutzobjekt (Schutzobjekt)** ist in der CyRV definiert. Ein Schutzobjekt wird in oder im Auftrag der Bundesverwaltung eingesetzt bzw. genutzt, muss gemäss seinem Schutzbedarf geschützt sein und ist Gegenstand dieser Vorgabe¹. Für jedes Schutzobjekt muss eine Schutzobjektverantwortliche oder ein Schutzobjektverantwortlicher definiert sein. Für Anwendungen ist das die oder der Anwendungs-Verantwortliche gemäss der Rollenbeschreibung der Informatikprozesse der Bundesverwaltung². Der Begriff «Schutzobjektverantwortliche» bezieht sich aber auf alle Schutzobjekte und stellt in diesem Sinne eine Verallgemeinerung dar.

² In dieser Vorgabe bedeuten zudem:

- a) **Schutzbedarfsanalyse:** Strukturierte Methode zur Erhebung des Schutzbedarfs eines Informatikschutzobjekts. Dabei wird zwischen Grundschatz und erhöhtem Schutzbedarf unterschieden.

¹ Mehrere Informatikmittel können zu einem Schutzobjekt zusammengefasst werden, wenn sie inhaltlich zusammengehören und den gleichen Schutzbedarf aufweisen.

² https://intranet.dti.bk.admin.ch/isb_kp/de/home/ikt-vorgaben/prozesse-methoden/p000-informatikprozesse_in_der_bundesverwaltung.html

- b) **Informationssicherheits- und Datenschutz (ISDS) Konzept:** Strukturierte Beschreibung der Sicherheitsanforderungen eines Schutzobjekts, der geplanten und umgesetzten Sicherheitsmassnahmen, sowie der verbleibenden Restrisiken.
- c) **Informationen:** Elektronisch gespeicherte, verarbeitete und/oder übertragene Daten³. Beziehen sich die Daten auf eine bestimmte oder bestimmbare Person, dann handelt es sich um **Personendaten** im Sinne der Datenschutzgesetzgebung.
- d) **IT-System (System):** Ein informationstechnisches System, welches als (System-) Software auf einer dedizierten Hardware oder auf einer virtualisierten Hardware bzw. virtuellen Maschine betrieben wird⁴. Im zweiten Fall kann das IT-System als virtualisiert bezeichnet werden.
- e) Ein IT-System gilt als⁵
- **Server-System**, wenn es mehrheitlich IT-Leistungen erbringt.
 - **Client-System**, wenn es mehrheitlich IT-Leistungen bezieht.
 - **Bundesclient**, wenn es ein Client-System ist, das im IKT-SD BA geführt wird. Dabei kann es sich entweder um ein Arbeitsplatzsystem (APS) oder ein virtualisiertes, auf einem «Smart Device» in einer Sandbox mit einem Mobile Device Management (MDM) gemäss [E021] betriebenes Client-System handeln (MDM-System).
 - **Peripheriegerät**, wenn es andere IT-Systeme funktional erweitert, und dazu integriert oder installiert (Treiber) werden muss, wie z.B. Drucker, Multifunktionsgeräte oder Präsentationssysteme für Konferenzräume.
 - **Messgerät**, wenn seine primäre Aufgabe darin besteht, Messwerte⁶ eines am Messort befindlichen Messfühlers (Sensor) über eine dedizierte und nicht für andere Zwecke nutzbare Verbindung zu einem geografisch abgesetzten IT-System zu übertragen. Das empfangende IT-System kann die Messwerte entweder nur sammeln und aufzeichnen oder diese auch auswerten und weiterverarbeiten. Die Kommunikation kann bilateral erfolgen und z.B. auch die Übertragung von Steuerungsinformation an das Messgerät beinhalten. Messgeräte werden vor allem in Internet of Things (IoT) Anwendungen eingesetzt.
 - **Netzwerkkomponente**, wenn es primär dem Datentransport zwischen IT-Systemen dient, wie z.B. Switches, Router und einfache statische Paketfilter (IP-Firewalls). Im OSI-Referenzmodell arbeiten Netzwerkkomponenten bis und mit Schicht 5 (Sitzungsschicht).
 - **Policy Enforcement Point (PEP)**, wenn es primär der Durchsetzung von Regeln (von Policies) dient, wie z.B. dynamische Paketfilter, Applikationsprotokoll-Gateways, Proxy Server und Reverse Proxy Server. Im OSI-Referenzmodell arbeitet ein PEP bis und mit Schicht 7 (Anwendungsschicht), und kontrolliert in diesem Sinne auch das (die) vermittelte(n) Kommunikationsprotokoll(e).

³ Der Botschaft zum neuen ISG folgend wird der Begriff «Informationen» generisch für «Informationen und Daten» verwendet und nur dann von Daten gesprochen, wenn es sich um Personendaten im Sinne des Datenschutzes handelt.

⁴ Das IT-System, das die virtualisierte Hardware bzw. die virtuelle Maschine zur Verfügung stellt (Hypervisor), ist selbst wiederum eine Software und stellt daher ein eigenständiges IT-System dar.

⁵ Die Unterscheidung zwischen einem Client- und Server-System ist nicht präzise, und ein IT-System kann gleichzeitig sowohl als Client-System als auch als Server-System auftreten.

⁶ Dabei kann es sich bei den Messwerten auch um akustische und/oder optische Signale handeln.

- f) **Anwendung:** Anwendungssoftware, die auf IT-Systemen von einer oder mehreren VE zur Abwicklung von Geschäftsprozessen eingesetzt wird. IoT-Anwendungen unterscheiden sich von anderen Anwendungen vor allem dadurch, dass die verwendeten Informationen primär von Messgeräten erzeugt sind.
- g) **Netzwerk:** Technische Vorrichtung (primär bestehend aus Netzwerkkomponenten und Verbindungen) zum Datenaustausch zwischen IT-Systemen.
- h) **Netzwerksegment (Segment):** Teil eines Netzwerkes, das – aus Lastausgleichs- und/oder Sicherheitsgründen – typischerweise mit Netzwerkkomponenten von den restlichen Teilen des Netzwerkes getrennt ist.
- i) **Zone:** Logischer Verbund von IT-Systemen, die sich durch ähnliche Sicherheitsanforderungen auszeichnen und der gleichen Zonenpolicy unterliegen. Insbesondere ist eine Zone nicht auf einen bestimmten Ort (z.B. Rechenzentrum) beschränkt. Die netzwerk-mässige Erschliessung einer Zone erfolgt über Netzwerkkomponenten, während die Durchsetzung der Regeln der Zonenpolicy über PEPs erfolgt.
- j) **Unterzone:** Eine Zone kann in Unterzonen unterteilt sein, wenn die entsprechende Policy dies vorsieht. Jede Unterzone stellt selbst wiederum eine Zone dar. Insbesondere muss jede Unterzone über eine Policy verfügen, die die Policy der übergeordneten Zone nur verschärfen darf, d.h. sie darf nur zusätzliche Anforderungen und Vorgaben enthalten (Abschwächungen sind unzulässig). Die Unterzonierung einer Unterzone ist erlaubt, sollte aber nur in zwingenden Fällen angewendet werden.
- k) **Zonenpolicy:** Strukturierte Beschreibung von Anforderungen und Vorgaben an eine Zone, d.h.
- die in der Zone betriebenen IT-Systeme,
 - die Zone selbst, wie z.B. ob und wenn ja wie die Zone netzwerk-mässig segmentiert werden kann,
 - die Authentifikation der Personen und automatisierten Prozesse, die auf in der Zone betriebenen IT-Systeme und Anwendungen zugreifen, sowie
 - die für die Zone zulässige interne (auch Segment-übergreifende) und externe (auch PEZ-übergreifende) Kommunikation, d.h. die zulässigen aus- und eingehenden Kommunikationsbeziehungen⁷. Eine Kommunikation zwischen zwei oder mehr gleichen Zonen⁸ gilt als intern, wenn die Konformität der Zonenübergänge mit den Policies in der gleichen PEZ sichergestellt wird.
- l) **Zonenmodell Bund:** Generisches Modell für die Zonenbildung in der Bundesverwaltung (vgl. Anhang A).

3 Grundsätze und Prinzipien

¹ **Form der Leistungserbringung:** Der IT-Grundschutz gilt für alle Schutzobjekte unabhängig von der Form der Leistungserbringung, d.h. die LE betreffenden

⁷ Eine Kommunikationsbeziehung ist ausgehend, wenn der entsprechende Datenaustausch von einem IT-System der zur Diskussion stehenden Zone angestossen wird. Demgegenüber ist sie eingehend, wenn der Datenaustausch zwar von einem IT-System ausserhalb der Zone angestossen wird, sich aber an ein IT-System in der Zone richtet. In beiden Fällen kann der eigentliche Datenaustausch bidirektional erfolgen.

⁸ Diese Zonen können auch über unterschiedliche Inhaber verfügen.

Sicherheitsanforderungen und -massnahmen müssen sowohl von internen als auch von externen LE umgesetzt werden. Bei externen LE muss insbesondere sichergestellt sein, dass die Informatiksicherheitsvorgaben eingehalten⁹ und die entsprechende Einwilligung der vorgesetzten Behörde gemäss den amts- bzw. departementsspezifischen Prozessen eingeholt sind (vgl. [Si001-Hi04]).

² **Virtualisierung:** Der IT-Grundschatz gilt unabhängig von der Frage, ob ein Schutzobjekt auf dedizierter Hardware oder virtualisiert auf gemeinsam genutzter Hardware betrieben wird. Im Bereich des erhöhten Schutzbedarfs muss der Einsatz von allfälligen Virtualisierungstechnologien und -lösungen im ISDS-Konzept begründet und dokumentiert sein.

³ **«Zero Trust»-Prinzip:** Das Sicherheitsdispositiv eines Schutzobjektes sollte wenn möglich so gestaltet sein, dass die Sicherheitsanforderungen aus Kapitel 4 autonom erfüllt werden können und das Objekt so von seiner Umgebung isoliert und abgeschottet ist, dass minimale Annahmen über die Sicherheit der Umgebung gemacht werden müssen. Vom «Zero Trust»-Prinzip ausgenommen sind Dienste mit übergreifendem Charakter, wie z.B. Single Sign-On (SSO) Dienste im Rahmen des IKT-SD IAM. Allerdings müssen in diesen Fällen die Risiken ausgewiesen und im Rahmen eines umfassenden Risikomanagements behandelt sein.

⁴ **«Defense-in-Depth»-Prinzip:** Wenn möglich und wirtschaftlich vertretbar muss ein Schutzobjekt mit verschiedenen, sich gegenseitig ergänzenden, komplementären Sicherheitsmassnahmen geschützt sein, um in Bezug auf die Erfüllung der Sicherheitsanforderungen Redundanz zu erwirken. Die Sicherheitsmassnahmen müssen insgesamt eine präventive, detektive und reaktive Wirkung haben.

⁵ **Stand der Technik:** Alle eingesetzten (präventiv, detektiv und/oder reaktiv wirkenden) Sicherheitsmassnahmen müssen dem Stand der Technik entsprechen¹⁰, idealerweise standardisiert und im operativen Betrieb erprobt sein. Massnahmen, die veraltet sind oder für die relevante Verwundbarkeiten oder Schwachstellen bekannt sind, müssen zeitnah und unabhängig vom «Life Cycle» nachgebessert oder ersetzt werden.

⁶ **«Least Privilege»- bzw. «Need-to-Know»-Prinzip:** Die Vergabe von Zugriffsrechten und Privilegien muss minimal erfolgen. Dies gilt beispielsweise für die Benutzerinnen und Benutzer von IT-Systemen und Anwendungen¹¹, die aktivierten Dienste und Zusatzfunktionalitäten («Features») von IT-Systemen und Anwendungen, sowie die zulässigen Kommunikationsbeziehungen im Rahmen von Zonenpolicies¹².

⁸ **«Security by Design»-Prinzip:** Bei der Entwicklung von Hard- und Softwarekomponenten bzw. deren Einsatz in IT-Systemen und Anwendungen muss die Sicherheit von Anfang an mitberücksichtigt und aktuell gehalten werden, so dass diese möglichst frei von Schwachstellen und Verwundbarkeiten sind und entsprechende Angriffsmöglichkeiten klein gehalten werden.

⁹ **«Security by Default»-Prinzip:** Schutzobjekte müssen so entwickelt, konfiguriert und betrieben werden, dass alle in einem spezifischen Umfeld sinnvollen

⁹ Die Einhaltung der Informatiksicherheitsvorgaben kann z.B. vertraglich geregelt und/oder aufgrund von entsprechenden Prüfungen und Zertifikaten sichergestellt sein.

¹⁰ Im Bereich der Kryptografie gibt die Technologiebetrachtung «IKT-Sicherheitsempfehlungen für den Grundschatz - Kryptografische Verfahren: Algorithmen und Protokolle» der FUB ZEO KRYPT Auskunft über den Stand der Technik.

¹¹ Für die Erteilung von Zugriffsrechten an Benutzerinnen und Benutzer ist idealerweise ein Rollenkonzept vorzusehen (im Rahmen einer Rollen-basierten Zugriffskontrolle).

¹² Kommunikationsprotokolle sind grundsätzlich nur dann zulässig, wenn sie betrieblich erforderlich sind.

Sicherheitsmassnahmen standardmässig aktiviert sind und ihre Wirkung entfalten können, ohne dass sich die Benutzerinnen und Benutzer darum kümmern müssen.

¹⁰ **Produkteneutralität:** Die Vorgaben und Empfehlungen des NCSC sind grundsätzlich produkteneutral. Aussagen für oder gegen den Einsatz bestimmter Produkte werden nur abgegeben, wenn sie entweder einen IKT-SD betreffen¹³ oder es andere gewichtige Gründe aus der Sicht der Informatiksicherheit gibt.

4 Sicherheitsanforderungen

¹ Für jedes Schutzobjekt müssen die Grundsätze und Prinzipien aus Kapitel 3 berücksichtigt und die Sicherheitsanforderungen aus Absatz 2 erfüllt sein. Die Anforderungen sind teilweise aus ISO/IEC 27002:2013 übernommen und in Anlehnung an ISO/IEC DIS 27002 strukturiert¹⁴.

² Die Sicherheitsanforderungen, die die Organisation (O), das Personal (P), die Technik (T) und die Informationen (I) betreffen, müssen immer erfüllt sein, während die Anforderungen für IT-Systeme (S), Anwendungen (A) und Zonen (Z) nur dann erfüllt sein müssen, wenn entsprechende Schutzobjekte auch eingesetzt werden.

Organisation	
O1	<p>Verantwortlichkeit</p> <p>Für das Schutzobjekt muss eine verantwortliche Person (innerhalb der verantwortlichen VE) als Schutzobjektverantwortliche/r definiert sein. Diese Person ist für die Umsetzung dieser Vorgabe zuständig. Sie muss sich ihrer Verantwortung bewusst und fachtechnisch in der Lage sein, die Verantwortung auch wahrzunehmen.</p>
O2	<p>Dokumentation</p> <p>O2.1 Für das Schutzobjekt muss eine aktuelle und mit den beteiligten LE abgeglichene Dokumentation vorliegen. Dabei muss die Dokumentation die gesamte Lebensdauer («Life Cycle») des Objekts abdecken und insbesondere auch</p> <ul style="list-style-type: none"> a) die Lieferkette («Supply Chain»), b) die physischen Schutzmassnahmen, wobei die Notwendigkeit von baulichen und technischen Massnahmen zum physischen Schutz von IT-Systemen dort wo erforderlich mit dem BBL, der armasuisse bzw. dem Bundessicherheitsdienst abgeklärt sein muss, c) die sicherheitsrelevanten Komponenten, Funktionen und Einstellungen,

¹³ So sind z.B. im Bereich der asymmetrischen Kryptografie vorzugsweise Zertifikate einzusetzen, die von der Swiss Government PKI (SG-PKI) ausgestellt sind, und für die Verschlüsselung von als VERTRAULICH klassifizierten Dateien ist auf APS die Verschlüsselungssoftware der Bundesverwaltung (Schale 1) einzusetzen.

¹⁴ Im Gegensatz zu ISO/IEC 27002:2013 werden in diesem Entwurf organisatorische (Abschnitt 5), personelle (Abschnitt 6), physische (Abschnitt 7) und technische Kontrollen (Abschnitt 8) unterschieden. Das Mapping der Kontrollen aus ISO/IEC DIS 27002 auf die Kontrollen aus ISO/IEC 27002:2013 ist in Anhang B von ISO/IEC DIS 27002 zusammengestellt.

	<p>d) die Schlüsselverwaltung beim Einsatz kryptografischer Verfahren,</p> <p>e) die Modalitäten und Prozesse bei Änderung (im Rahmen des «Change Managements»), Reparatur, Entsorgung und Verlust,</p> <p>f) die vertraglichen Vereinbarungen, sowie</p> <p>g) die Audit-Prozesse und -Aktivitäten¹⁵ zur Kontrolle der Umsetzung und Einhaltung dieser Vorgabe mit einschliessen.</p> <p>O2.2 Wird das Schutzobjekt (IT-System oder Anwendung) nicht in einer Zone der Bundesverwaltung betrieben (z.B. in einer Public Cloud), muss in der Dokumentation beschrieben sein,</p> <p>a) wie in dieser Umgebung dem Schutzbedarf des Objekts entsprochen werden kann, und</p> <p>b) mit welchen komplementären Sicherheitsmassnahmen sichergestellt wird, dass sich für andere Schutzobjekte der Bundesverwaltung keine zusätzlichen Bedrohungen und Risiken ergeben.</p>
O3	<p>Geschäftskontinuität</p> <p>Für das Schutzobjekt muss die Geschäftskontinuität im Rahmen eines IT Service Continuity Management (ITSCM) bzw. eines Business Continuity Management (BCM) Prozesses gemäss ausgewiesenem Bedarf in der Schutzbedarfsanalyse (Schuban) sichergestellt und dokumentiert sein.</p>
O4	<p>Cybervorfälle</p> <p>Das Schutzobjekt muss in den Prozess zur Bewältigung von Cybervorfällen¹⁶ eingebunden sein. Bei grösseren Vorfällen werden die Arbeiten vom NCSC koordiniert.</p>
Personal	
P1	<p>Sensibilisierung und Schulung</p> <p>P1.1 Alle Benutzerinnen und Benutzer des Schutzobjekts müssen im Bereich der Informatiksicherheit stufen- bzw. funktionsgerecht sensibilisiert und geschult sein.</p> <p>P1.2 Alle Benutzerinnen und Benutzer des Schutzobjekts müssen die für das Schutzobjekt relevanten Einsatzrichtlinien kennen und sind zu deren Einhaltung verpflichtet¹⁷.</p>
P2	<p>Meldepflicht</p> <p>Alle Benutzerinnen und Benutzer des Schutzobjekts müssen sicherheitskritische Ereignisse, wie z.B. anormales und verdächtiges Systemverhalten oder</p>

¹⁵ Audit-Prozesse und –Aktivitäten müssen von einer unabhängigen Stelle durchgeführt werden und so gestaltet sein, dass die Verfügbarkeit der Schutzobjekte möglichst wenig beeinträchtigt wird (d.h. Störungen und Unterbrechungen im Betrieb möglichst klein gehalten werden).

¹⁶ https://intranet.ncsc.admin.ch/dam/ncscintra/de/dokumente/partner/20210217-Bewaeltigung_Cybervorfaelle.pdf.download.pdf/20210217-Bewaeltigung_Cybervorfaelle.pdf

¹⁷ Gilt insbesondere für die Nutzung von MDM-Systemen und/oder privaten Peripheriegeräten beim Mobilien Arbeiten. Eine Übersicht über alle Einsatzrichtlinien ist unter https://intranet.dti.bk.admin.ch/isb_kp/de/home/ikt-vorgaben/einsatzrichtlinien.html verfügbar.

	physischer Verlust, möglichst zeitnah der dafür zuständigen Stelle melden (z.B. Servicedesk des LE).
Technik	
T1	<p>Betrieb</p> <p>Das Schutzobjekt muss dem Stand der Technik entsprechend und unter Berücksichtigung von branchenüblichen Sicherheitsvorgaben und -empfehlungen («Best Practices») betrieben werden.</p>
T2	<p>Konfiguration und Einstellung</p> <p>T2.1 Das Schutzobjekt muss vor der ersten Inbetriebnahme so konfiguriert und eingestellt sein, dass</p> <ol style="list-style-type: none"> es vor unberechtigtem Zugriff geschützt ist, es soweit technisch möglich gehärtet ist und in einer zur Aufgabenerfüllung erforderlichen und vom Benutzer nicht veränderbaren Minimalkonfiguration betrieben wird (d.h. nicht genutzte Schnittstellen, Module und Funktionen müssen deaktiviert sein), und wichtige sicherheitsrelevante Aktivitäten und Ereignisse (mit Zeitangaben) aufgezeichnet und zeitnah ausgewertet werden. <p>T2.2 Sicherheitskonfigurationen und -einstellungen dürfen nur autorisiert aktiviert, geändert, deaktiviert und deinstalliert werden.</p>
T3	<p>Produktive Umgebung</p> <p>Die produktive Umgebung des Schutzobjekts muss von allenfalls vorhandenen nicht produktiven Umgebungen (z.B. für Entwicklung und/oder Test) getrennt sein. Erfolgt die Trennung logisch, müssen die entsprechenden Sicherheitsvorkehrungen und -massnahmen begründet und dokumentiert sein.</p>
T4	<p>Schwachstellen und Verwundbarkeiten</p> <p>Das Schutzobjekt muss im Hinblick auf Schwachstellen und Verwundbarkeiten vor seiner Inbetriebnahme und in Abhängigkeit seines Schutzbedarfs und Exposition gegenüber dem Internet auch während des laufenden Betriebs regelmässig und vorzugsweise automatisiert überprüft werden (z.B. mit einem Security Scanner). Für kritische Schwachstellen und Verwundbarkeiten ist das NCSC beizuziehen.</p>
T5	<p>Authentifikation und Autorisation</p> <p>T5.1 Jeder Zugriff auf ein Schutzobjekt muss seinem Schutzbedarf entsprechend authentifiziert¹⁸ und gemäss dem «Least Privilege»- bzw. «Need-to-Know»-Prinzip autorisiert sein.</p> <p>T5.2 Alle Zugriffsrechte auf das Schutzobjekt müssen im Rahmen eines definierten und dokumentierten Prozesses¹⁹ verwaltet und stets aktuell</p>

¹⁸ Die Authentifikation kann lokal oder über eine oder mehrere Netzwerkverbindungen erfolgen. Im zweiten Fall wird die Authentifikation in ihrer Gesamtheit betrachtet (d.h. lokale Authentifikation auf einem Endgerät und allfällige Authentifikationen auf Proxy Servern).

¹⁹ Im Rahmen dieses Prozesses muss die Gewaltentrennung zwischen Bewilligung und Vergabe von Zugriffsrechten wenn möglich und sinnvoll berücksichtigt und mit dokumentiert sein.

	<p>gehalten werden. Insbesondere müssen die Rechte mindestens jährlich in Bezug auf Notwendigkeit und Richtigkeit überprüft und nicht mehr benötigte Rechte (bzw. Konti) entfernt werden.</p> <p>T5.3 Für das Schutzobjekt dürfen nur Authentifikations- und Identitätsnachweismittel eingesetzt werden, die im Rahmen eines definierten und dokumentierten Prozesses verwaltet werden, der den gesamten Life Cycle des Mittels (inkl. Zugriffsmöglichkeiten für Notfälle, Sperrung, Zurücksetzung, Revozierung und Entsorgung) mit abdeckt.</p>
T6	<p>Benutzerauthentifikation</p> <p>T6.1 Die Benutzerauthentifikation gegenüber einem APS oder einem Server-System muss auf der Basis eines Authentifikations- und Identitätsnachweismittels mindestens der Sicherheitsstufe «mittel» gemäss Anhang B bzw. einer 2-Faktoren-Authentifikation erfolgen²⁰.</p> <p>T6.2 Die Benutzerauthentifikation gegenüber einem MDM-System muss auf der Basis der vom jeweiligen Betriebssystem unterstützten Verfahren erfolgen, wie z.B. PIN²¹ oder biometrische Authentifikation (z.B. Touch ID oder Face ID für iOS-Geräte). Ein PIN muss mindestens 6 Zeichen enthalten und darf nicht trivial sein.</p> <p>T6.3 Die Benutzerauthentifikation gegenüber einer Netzwerkkomponente muss auf der Basis eines Authentifikations- und Identitätsnachweismittels mindestens der Sicherheitsstufe «hoch» gemäss Anhang B erfolgen.</p>
T7	<p>Passwörter</p> <p>Für die Benutzerauthentifikation mittels Passwort gelten die folgenden Anforderungen.</p> <p>T7.1* Das Passwort</p> <ol style="list-style-type: none"> a) muss persönlich²² sein b) muss einmalig²³ sein c) darf nicht weitergegeben werden d) darf nicht aufgeschrieben bzw. muss geschützt abgelegt oder mit einem Passwort-Verschlüsselungsprogramm verwaltet werden²⁴ e) muss mindestens 10 Zeichen lang sein (bei Benutzern mit erhöhten Rechten 18 Zeichen), wobei die Zeichen aus mindestens drei der vier Kategorien Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen stammen müssen

²⁰ Die Notwendigkeit einer 2-Faktoren-Authentisierung ergibt sich aus dem BRB vom 04. Juni 2010. Für die Angestellten des Bundes werden dabei Klasse-B-Zertifikate der SG-PKI eingesetzt. Bei einem Server-System bezieht sich die Benutzerauthentifikation auf die Betriebssystemebene.

²¹ Die konzeptionellen Unterschiede zwischen einem Passwort und einer PIN sind in der Technologiebetrachtung «Passwörter vs. PINs» vom 29. Juni 2012 ausgeführt. Entsprechend gelten die hier aufgeführten Mindestanforderungen für PINs nur beschränkt.

²² Unpersönliche Funktionsaccounts dürfen nur in begründeten Einzelfällen vergeben werden (vgl. [Si002-Hi01]) und dürfen nur für Zugriffe auf Schutzobjekte mit nicht erhöhtem Schutzbedarf (Grundschutz) verwendet werden.

²³ Insbesondere ist es unzulässig, ein Passwort für die Authentifikation gegenüber mehreren IT-Systemen und Anwendungen zu verwenden.

²⁴ Auf APS ist die Persönliche Passwortverwaltung (Schale 1) einzusetzen.

	<p>f) darf nicht trivial sein und keinen Bezug zum Benutzer haben, d.h. Attribute wie User-ID, Name, Vorname oder Geburtsdatum dürfen nicht enthalten sein.</p> <p>T7.2* Ein administrativ gesetztes Initialpasswort muss bei seinem Erstgebrauch geändert werden.</p> <p>T7.3* Wenn das Passwort geändert wird, muss sichergestellt sein, dass das neue Passwort keinem der 10 zuletzt verwendeten Passwörtern entspricht.</p> <p>T7.4* Nach maximal 5 Fehleingaben muss das Passwort gesperrt und darf nur im Rahmen eines definierten Prozesses wieder freigegeben werden.</p> <p>T7.5 Bei Verdacht auf Kenntnisnahme durch Unberechtigte oder Missbrauch muss das Passwort umgehend geändert werden.</p> <p>T7.6* Server-seitig muss sichergestellt sein, dass das Passwort nicht im Klartext ausgelesen oder im Rahmen eines anderen Angriffs leicht kompromittiert werden kann.</p>
T8	<p>Administrative Zugriffe und Fernzugriffe</p> <p>T8.1 Administrative Zugriffe auf das Schutzobjekt müssen auf eine dokumentierte und kontrollierte Art und Weise erfolgen. Insbesondere müssen solche Zugriffe kryptografisch abgesichert sein und nachvollziehbar aufgezeichnet und ausgewertet werden.</p> <p>T8.2 Die für administrative Zugriffe verwendeten IT-Systeme müssen für diese Aufgabe ausgelegt sein und vorzugsweise in einer Management Zone betrieben werden. Die Nutzung der entsprechenden (privilegierten) Konti muss einer Person zugeordnet werden können. Zudem dürfen die Konti nur über minimal erforderliche und möglichst kurzlebige Zugriffsrechte verfügen²⁵, müssen einer Schicht in einem Schichtenmodell²⁶ zugeordnet sein und dürfen nur zur Administration in dieser Schicht verwendet werden (zwecks Verhinderung einer «Privilege Escalation»). Insbesondere dürfen die Konti nicht für nicht-administrative Internet-Zugriffe genutzt werden.</p> <p>T8.3 Ein direkter Fernzugriff durch einen externen Anbieter ist zulässig, wenn</p> <ol style="list-style-type: none"> der Inhaber des Objekts einverstanden ist und bezüglich möglicher Amtsgeheimnisverletzungen gemäss den amts- bzw. departementsspezifischen Prozessen eingewilligt hat (vgl. [Si001-Hi03, Si001-Hi04), der Zugriff über ein dediziertes Konto erfolgt und die entsprechende Benutzerauthentifikation auf einem Authentifikations- und Identitätsnachweismittel mindestens der Stufe «mittel» gemäss Anhang B basiert, die Nutzung dieses Kontos zeitlich begrenzt ist und überwacht wird, wenn technisch möglich der Zugriff über einen Jumphost erfolgt, die netzwerktechnische Verbindung für den Zugriff kryptografisch abgesichert ist (z.B. mit Hilfe von SSH) und

²⁵ Idealerweise werden die Konti im Rahmen einer Privileged Access Management (PAM) Lösung verwaltet und sind nur für die Dauer einer bestimmten Administrationstätigkeit gültig.

²⁶ Ein solches Schichtenmodell ist z.B. im Rahmen der im Entwurf vorliegenden E033 definiert.

	f) die Auditierbarkeit der externalisierten Prozesse jederzeit sichergestellt ist.
Informationen (Daten)	
I1*	Zulässigkeit von IT-Systemen Geschäftsrelevante Informationen dürfen nur auf IT-Systemen gespeichert und verarbeitet werden, deren Inhaber entweder eine VE der Bundesverwaltung oder für die die Einhaltung der sicherheitstechnischen Anforderungen aus dieser Vorgabe vertraglich geregelt ist (z.B. im Rahmen einer Cloud-Lösung).
I2	Vertraulichkeit und Integrität 12.1 Die Vertraulichkeit und Integrität von geschäftsrelevanten Informationen müssen jederzeit ihrem Schutzbedarf entsprechend und unter Berücksichtigung der physischen Gegebenheiten mit Hilfe kryptografischer Verfahren geschützt sein ²⁷ (gilt auch für Testdaten und zu Testzwecken eingesetzte produktive Daten). Werden Informationen verschlüsselt, dann müssen die dazu verwendeten Schlüssel so verwaltet werden, dass eine Wiederherstellung und damit eine Entschlüsselung der Informationen jederzeit möglich ist. In der Regel bedingt das eine aufwändige Schlüsselverwaltung (mit einem «Key Recovery»-Mechanismus) sowie ein periodisches Austesten der Wiederherstellbarkeit der Informationen. 12.2 Die eingesetzten IT-Systeme müssen geeignet sein, den Schutz der Vertraulichkeit und Integrität der Informationen zu gewähren ²⁸ .
I3	Verfügbarkeit 13.1 Die Verfügbarkeit von geschäftsrelevanten Informationen muss jederzeit dem Schutzbedarf entsprechend sichergestellt sein. 13.2 Die für Informationen verantwortliche VE muss über eine Backup-Strategie verfügen ²⁹ und diese auch umsetzen. Diese Strategie muss ein Mehrgenerationen-Prinzip und eine offline Speicherung wichtiger Datenbestände vorsehen, so dass Daten auch im Falle von datenverschlüsselnder Malware («Ransomware») wiederhergestellt werden können.
I4	Datenträger Die Datenträger, auf denen geschäftsrelevante Informationen gespeichert sind, müssen jederzeit dem Schutzbedarf der Informationen entsprechend geschützt

²⁷ Insbesondere müssen Informationen mit erhöhtem Schutzbedarf, die auf Festplatten von physisch nicht speziell geschützten Server-Systemen gespeichert sind, mit einer Festplattenverschlüsselung geschützt sein.

²⁸ So ist z.B. auf MDM-Systemen die Speicherung und Verarbeitung von als VERTRAULICH klassifizierten Informationen bzw. besonders schützenswerten Personendaten oder Persönlichkeitsprofilen grundsätzlich nicht bzw. nur im Rahmen von verschlüsselter Sprachkommunikation zulässig [E027].

²⁹ Ist die verantwortliche VE ein LB, kann die Backup-Strategie auch vom LE stammen. Allerdings muss die Strategie dann vom LB geprüft und als angemessen akzeptiert sein. Der regelmässigen Beübung der Strategie kommt in diesem Fall eine zentrale Bedeutung zu, wobei die Wiederherstellbarkeit von Daten nach einem Verlust regelmässig kontrolliert und vom LB bestätigt werden muss.

	sein. Namentlich für die Reparatur und Entsorgung von Datenträgern ³⁰ müssen geeignete Prozesse definiert und umgesetzt sein.
IT-Systeme	
S1	<p>Zonenzugehörigkeit</p> <p>Das IT-System muss einer Zone zugehören und gemäss der entsprechenden Zonenpolicy betrieben werden³¹.</p>
S2	<p>Updates und Fehlerkorrekturen</p> <p>Für das IT-System muss entweder sichergestellt sein, dass der oder die Hersteller während der ganzen Lebensdauer Updates und Fehlerkorrekturen (Patches) bereitstellen, die zeitnah geprüft und eingespielt werden³², oder das IT-System in einer dedizierten und möglichst stark abgeschotteten Zone betrieben wird (z.B. Technik Zone) und mit Hilfe welchen komplementären Sicherheitsmassnahmen sichergestellt wird, dass sich für andere Schutzobjekte der Bundesverwaltung keine zusätzlichen Bedrohungen und Risiken ergeben. Falls ein Ersatz geplant ist, darf das IT-System während maximal zwei Jahren weiter betrieben werden, sofern der Weiterbetrieb in einem ISDS-Konzept beschrieben ist.</p>
S3	<p>Dienstkonti</p> <p>S3.1 Von Systemdiensten benutzte Konti (Dienstkonti) müssen spezifisch³³ und nur mit den für die Diensterbringung minimal erforderlichen Rechten ausgerüstet sein.</p> <p>S3.2* Die Dienstkonti müssen automatisiert verwaltet werden und eine kryptografisch starke Authentifikation erfordern. Im Idealfall basiert diese Authentifikation auf dem Einsatz asymmetrischer Kryptografie, wobei die dazu verwendeten privaten Schlüssel sicher hinterlegt werden müssen. Basiert die Authentifikation auf Passwörtern, müssen diese deutlich stärker (und länger) sein als bei der Benutzerauthentifikation.</p>
S4	<p>Integritäts- und Malwareschutz</p> <p>S4.1 Die Integrität der auf dem IT-System eingesetzten Softwarekomponenten muss sichergestellt sein (z.B. mit Hilfe von digitalen Signaturen). Insbesondere muss jedes Server-System mit erhöhtem Schutzbedarf regelmässig einer Integritätsprüfung unterzogen werden³⁴.</p> <p>S4.2 Wird ein Integritätsverlust festgestellt, muss das IT-System unmittelbar vom Netzwerk getrennt, gesichert und untersucht werden. Im Falle einer</p>

³⁰ Bei der Entsorgung von Datenträgern ist insbesondere darauf zu achten, dass keine Rückschlüsse auf den Inhalt oder die gespeicherten Daten möglich sind.

³¹ Ein IT-System, das keiner anderen Zone zugeordnet werden kann, gehört zum Internet. In diesem Fall gibt es keine Zonenpolicy. Zudem kann es Netzwerkkomponenten geben, die weder einer Zone noch dem Internet angehören. Diese Komponenten müssen dokumentiert sein.

³² Für APS, die nicht permanent mit dem Netzwerk verbunden sind, muss sichergestellt sein, dass diese mindestens einmal pro Monat mit Updates und Patches aktualisiert werden.

³³ Ein Dienstkonto ist spezifisch, wenn es für nur einen Dienst verwendet wird.

³⁴ BRB vom 16. Dezember 2009

	<p>bestätigten Kompromittierung muss das IT-System vollständig gelöscht und neu aufgesetzt werden.</p> <p>S4.3 Das IT-System muss in ein auf [SB003] aufbauendes Malwareschutzkonzept eingebunden sein, das insbesondere auch regelt, wie bei einem Malwarebefall vorzugehen ist und welche Stellen wie informiert werden müssen.</p>
S5	<p>Bundesclients</p> <p>S5.1 Auf dem Bundesclient müssen interne nicht-flüchtige Datenspeicher (z.B. Festplatten) transparent verschlüsselt sein. Für ein MDM-System muss zudem eine Möglichkeit vorgesehen sein, das System entfernt auf seine Grundeinstellungen zurückzusetzen und sämtliche lokal gespeicherten Informationen zu löschen.</p> <p>S5.2 Bei fehlender Benutzeraktivität muss der Zugriff auf den Bundesclient automatisch gesperrt werden (auf APS nach maximal 15 Minuten und auf MDM-Systemen nach maximal 3 Minuten). Eine manuelle Aktivierung der Systemzugriffssperre muss ebenfalls möglich sein. Ist eine Sperrung aus technischen Gründen nicht möglich, muss der Zugang zu unbeaufsichtigten aber freigeschalteten Bundesclients physisch geschützt sein (z.B. durch Abschliessen des Raumes).</p> <p>S5.3 Auf dem Bundesclient darf keine Autorun-Funktion beim Anschluss externer Datenträger (z.B. USB-Sticks) aktiviert sein.</p> <p>S5.4 Die Benutzerinnen und Benutzer des APS dürfen über keine lokalen Administratorenrechte verfügen.</p> <p>S5.5 Ein administrativer Zugriff zu Supportzwecken auf das APS ist nur mit einer vorgängigen, expliziten Einwilligung der Benutzenden erlaubt.</p>
S6	<p>Peripheriegeräte</p> <p>S6.1 Das Peripheriegerät darf eingesetzt werden, wenn</p> <ol style="list-style-type: none"> a) es durch eine Beschaffungstelle des Bundes beschafft worden ist und b) seine Integrierbarkeit³⁵ und grundsätzliche Sicherheit vom LE nachweislich bestätigt worden ist. <p>S6.2 Das Peripheriegerät muss vom LE minimal konfiguriert und vor nicht berechtigten Änderungen (der Konfiguration) geschützt sein.</p> <p>S6.3 Wird das Gerät zum Drucken klassifizierter Dokumente benutzt, muss</p> <ol style="list-style-type: none"> a) das Gerät lokal betrieben werden oder eine Möglichkeit zur Personenauthentifizierung am Gerät bestehen, und b) interne nicht-flüchtige Datenspeicher (z.B. Festplatten) müssen gemäss einschlägigen Empfehlungen³⁶ überschrieben werden können, wobei die Überschreibung entweder manuell vom Benutzer oder automatisiert ausgelöst werden kann. <p>S6.4 Für die Nutzung von privaten Peripheriegeräten beim Mobilten Arbeiten muss die Einsatzrichtlinie [E026] eingehalten werden.</p>

³⁵ Die Integrierbarkeit bedeutet z.B. auch, dass das Gerät für Funktionen wie ScanToMail an die Mitarbeiterverzeichnisse der Bundesverwaltung angebunden werden kann

³⁶ B.B. DoD 5220.22-M oder NIST SP 800-88

Anwendungen	
A1	<p>Beschaffung / Entwicklung</p> <p>A1.1 Die Anwendung muss im Rahmen eines methodischen Vorgehens (vorzugsweise nach HERMES³⁷) und unter frühzeitiger Berücksichtigung von einschlägigen Sicherheitsvorgaben und -empfehlungen³⁸ («Best Practices») beschafft bzw. entwickelt werden.</p> <p>A1.2 Bei der Entwicklung der Anwendungssoftware muss insbesondere sichergestellt sein, dass</p> <ol style="list-style-type: none"> a) der Quellcode sicher aufbewahrt wird, b) der Zugriff auf die entsprechenden Repositories klar geregelt und nachvollziehbar kontrolliert wird, c) die Build Prozesse überwacht werden und Änderungen an der Build Pipeline nur kontrolliert erfolgen können, d) die Software regelmässig getestet wird und e) die Integrität der Software jederzeit sichergestellt ist (z.B. mit Hilfe von digitalen Signaturen).
A2	<p>Wartung und Pflege</p> <p>Für die Anwendung und ihre Komponenten (z.B. Software-Bibliotheken) müssen während der ganzen Lebensdauer eine professionelle Wartung und Pflege sichergestellt sein. Darunter fallen insbesondere auch die Einspielung von regelmässigen und betrieblich oder sicherheitstechnisch notwendigen Updates und Fehlerkorrekturen (Patches).</p>
Zonen	
Z1	<p>Konformität</p> <p>Z1.1 Die Zone muss konform zum Zonenmodell Bund sein und über einen Inhaber, einen eindeutigen Namen³⁹, eine Zonenpolicy und einen Betreiber⁴⁰ verfügen (gilt nicht für das Internet bzw. die Zone Internet). . Umfasst die Zone IT-Systeme und Anwendungen, die ausserhalb der Bundesverwaltung (z.B. in einer Public Cloud) betrieben werden, dann muss die netzwerk-mässige Erschliessung in der Zonenpolicy beschrieben sein.</p> <p>Z1.2 Der Betreiber muss sicherstellen, dass nur gemäss Zonenpolicy zulässige Kommunikation von und zu der Zone stattfinden kann, und dass mit Hilfe geeigneter komplementärer Sicherheitsmassnahmen (z.B. Isolierung und Segmentierung) von dieser Kommunikation keine</p>

³⁷ <https://www.hermes.admin.ch>

³⁸ Für die Entwicklung von Web-Anwendungen sind z.B. die Vorgaben und Empfehlungen der Open Web Application Security Project (OWASP) mit zu berücksichtigen. Diese decken auch die sichere Verwaltung von Programmcode mit ab.

³⁹ Die Eindeutigkeit kann z.B. dadurch erreicht werden, dass der Inhaber als Suffix dem Namen angehängt wird (z.B. SZ-FUB für eine von der FUB betriebene Server Zone). Falls ein Inhaber eine Zone mehrfach umsetzen lässt, müssen die entsprechenden Namen unterscheidbar sein.

⁴⁰ Der Betreiber ist ein LE, der die Zone im Auftrag des Inhabers netzwerktechnisch betreibt. Falls der Inhaber der Zone ein LE ist, können der Inhaber und der Betreiber auch identisch sein. Falls der Inhaber einer (Unter-)Zone die Policy ändert, muss dem Betreiber eine angemessene Frist für die Umsetzung eingeräumt werden.

	<p>zusätzlichen Bedrohungen und Risiken für andere IT-Systeme und Anwendungen in- und ausserhalb der Zone ausgeht.</p> <p>Z1.3 Die Zone muss in das Verzeichnis integriert sein, das vom zuständigen ISBD geführt und dem NCSC zur Verfügung gestellt wird. Ein ISBD ist zuständig, wenn eine Verwaltungseinheit des Departementes entweder als Inhaber oder Betreiber der Zone auftritt.</p>
Z2	<p>Zugriffe</p> <p>Z2.1 Ein eingeschränkter⁴¹ Zugriff in die Zone ist nur für Personen und automatisierte Prozesse zulässig, die mit einem Authentifikations- und Identitätsnachweismittel mindestens der Stufe «mittel» authentifiziert worden sind (für Messgeräte reicht die Stufe «tief»). Die folgenden Ausnahmen sind erlaubt:</p> <ul style="list-style-type: none"> a) Anonyme und personalisierte Zugriffe im Rahmen von E-Government-Anwendungen, die einer breiten Bevölkerungsschicht in einer SZ zugänglich gemacht werden. Die entsprechenden Webseiten müssen mit TLS (HTTPS) abgesichert und Formulare vor automatisierten Angriffen geschützt werden (z.B. mit Hilfe von CAPTCHAs). b) Zeitlich befristete Zugriffe zum Hochladen von Daten auf ein Server-System⁴². c) Automatisierte und im Einverständnis mit dem Zoneninhaber durchgeführte Zugriffe im Rahmen von Sicherheitsüberprüfungen von Web-Auftritten (Scans). <p>Erfolgt der Zugriff in eine Zone mit erhöhtem Schutzbedarf (z.B. SZ+) muss das Authentifikations- und Identitätsnachweismittel mindestens der Stufe «hoch» gemäss Anhang B sein und die oben aufgeführten Ausnahmen a) und b) sind dann nicht zulässig.</p> <p>Z2.2 Ein uneingeschränkter Zugriff in die Zone ist nur für Personen zulässig, die sich über einen Bundesclient verbinden, mit einem Authentifikations- und Identitätsnachweismittel mindestens der Stufe «hoch» gemäss Anhang B authentifiziert sind und die Verbindung kryptografisch abgesichert ist (z.B. mit Hilfe von SSH).</p>
Z3	<p>Zonenübergreifende Kommunikation</p> <p>Jede zonenübergreifende Kommunikation muss über eine PEZ erfolgen⁴³. Diese hat sicherzustellen, dass die Kommunikation konform zu den betroffenen Zonenpolicies ist. Dazu müssen die erlaubten Kommunikationsmuster und -beziehungen in den Policies so präzise wie möglich (idealerweise auf der Anwendungsschicht und in Form einer «Allow List») spezifiziert sein. Ist eine Konformitätsprüfung in einer PEZ nicht möglich (z.B. im Falle End-zu-End</p>

⁴¹ Ein Zugriff ist eingeschränkt, wenn er mit Hilfe technischer Vorkehrungen (z.B. IP-Paketfilterung) auf ein oder ein paar wenige definierte IT-Systeme oder Anwendungen und auf die für den Zugriff zwingend erforderlichen Protokolle eingeschränkt ist. Anderenfalls heisst der Zugriff uneingeschränkt.

⁴² Die Abgrenzung der entsprechenden Server-Systeme gegenüber den anderen IT-Systemen in der gleichen Zone muss in diesem Fall entweder in der Zonenpolicy oder – zusammen mit allen komplementären Sicherheitsmassnahmen zur Minimierung der Risiken – in der Sicherheitsdokumentation der Anwendung dokumentiert sein. Selbstverständlich muss auch der Zoneninhaber mit dem Betrieb der Server-Systeme einverstanden sein.

⁴³ Obwohl das grundsätzlich auch für die Kommunikation von einer Unterzone in die darüber liegende Zone gilt, kann in begründeten und in den Policies der entsprechenden Unterzonen dokumentierten Fällen darauf verzichtet werden.

	<p>verschlüsselter Kommunikation), kann die Prüfung auch durch die IT-Systeme in den Zonen selbst durchgeführt werden (im Sinne eines PEP). Allerdings ist dann der Einsatz von komplementären und risikomildernden Massnahmen vorzusehen und zu dokumentieren.</p>
Z4	<p>PEZ</p> <p>Z4.1 Die in einer PEZ betriebenen PEPs dürfen nur zonenintern virtualisiert betrieben werden, d.h. auf der gemeinsam genutzten Hardware dürfen keine IT-Systeme aus anderen Zonen betrieben werden.</p> <p>Z4.2 Der Inhaber einer PEZ bzw. einer Web-Proxy-Infrastruktur muss regeln, wie der Zugriff auf Ressourcen im Internet erfolgt und welche Zugriffe zulässig sind. Diese Regelung kann entweder in der Zonenpolicy der PEZ oder in einer separaten Vorgabe erfolgen. Das NCSC kann Einträge in den entsprechenden Regelsätzen erlassen. Im Einsatzgebiet des IKT-SD Datenkommunikation (DAKO) erfolgt die Regelung im Rahmen von [Si004].</p> <p>Z4.3 Die Anbindung einer PEZ an das Internet muss hochverfügbar und allenfalls redundant ausgelegt sein. Darüber hinaus muss der Betreiber mit Hilfe geeigneter Massnahmen sicherstellen, dass die durch die PEZ vom Internet getrennten IT-Systeme adäquat vor (D)DoS-Angriffen geschützt sind.</p>
Z5	<p>Überwachung</p> <p>Z5.1 Innerhalb einer Zone muss die Kommunikation dahingehend überwacht werden, dass Angriffe möglichst zuverlässig erkannt werden können (z.B. mit Hilfe von IDS/IPS) und der Betreiber im Bedarfsfall zeitnah und adäquat reagieren kann.</p> <p>Z5.2 Die bei der Überwachung anfallenden Informationen müssen gemäss den rechtlichen Vorgaben (insbesondere Datenschutzgesetzgebung und «Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen» vom 22. Februar 2012) aufbewahrt und vor nachträglichen Manipulationen geschützt werden. Im Bedarfsfall müssen die Informationen dem NCSC zur Verfügung gestellt werden.</p>

5 Inkraftsetzung und Übergangsbestimmungen

¹ Die Vorgabe tritt am 1. März 2022 in Kraft.

² Für Schutzobjekte, die vor der Inkraftsetzung dieser Vorgabe in Betrieb genommen worden sind, gelten die zu diesem Zeitpunkt geltenden Vorgaben (d.h. mindestens Si001 Version 4.4 und Si003 Version 3.1). Allerdings müssen diese Schutzobjekte im Rahmen ihres Life Cycles aber spätestens innerhalb von 5 Jahren seit Genehmigung der Sicherheitsdokumentation an die neuen Vorgaben angepasst werden.

³ Für Ausnahmen gilt Kapitel 1.3. Alle bisherigen Ausnahmegenehmigungen behalten ihre Gültigkeit.

⁴ Bis die Inhaberschaft der Netzdomäne blau geklärt und entsprechende Vorgaben erlassen

sind, gelten sowohl die Zonenpolicy aus Anhang C mit allen Abweichungsbewilligungen (Ausnahmen) und Vereinbarungen⁴⁴ als auch die Zugriffsmatrix aus Anhang D⁴⁵.

⁵ Das NCSC prüft die Vorgabe periodisch auf ihre Aktualität.

Abkürzungen

APS	Arbeitsplatzsystem
BA	Büroautomation
BBL	Bundesamt für Bauten und Logistik
BC	Bundesclient
BCM	Business Continuity Management
BK	Bundeskanzlei
BRB	Bundesratsbeschluss
CA	Certification Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CC	Common Criteria
CyRV	Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung
CZ	Client Zone
DAKO	Datenkommunikation
DDoS	Distributed DoS
DIS	Draft International Standard
DNS	Domain Name System
DoS	Denial of Service
DTI	Digitale Transformation und IKT-Lenkung (Bereich der BK)
EAL	Evaluation Assurance Level
EFK	Eidgenössische Finanzkontrolle
FIDO	Fast ID Online
FT	Fremdterminal
FUB	Führungsunterstützungsbasis
IAM	Identity and Access Management
ID	Identifikator
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
IKT	Informations- und Kommunikationstechnologie
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	IP security
ISBD	Informatiksicherheitsbeauftragter Departement
ISBO	Informatiksicherheitsbeauftragter Verwaltungseinheit
ISchV	Informationsschutzverordnung
ISDS	Informationssicherheits- und Datenschutz
ISG	Informationssicherheitsgesetz
ISO	International Organization for Standardization
IT	Informationstechnik
ITSCM	IT Service Continuity Management

⁴⁴ Dabei handelt es sich um eine Vereinbarung mit den Parlamentsdiensten.

⁴⁵ Allfällige Entscheidungen diesbezüglich wird DTI dem NCSC vorlegen.

JSON	JavaScript Object Notation
JWT	JSON Web Token
LB	Leistungsbezüger
LE	Leistungserbringer
LoA	Level of Assurance
MDM	Mobile Device Management
NCSC	Nationales Zentrum für Cybersicherheit
NW	Network Full Access (uneingeschränkter Netzzugriff)
OSI	Open Systems Interconnection
OTP	One-Time Passwort
OWASP	Open Web Application Security Project
PAM	Privileged Access Management
PEP	Policy Enforcement Point
PEZ	Policy Enforcement Zone
PIN	Persönliche Identifikatio
PKI	Public Key Infrastruktur
RA	Restricted Access (eingeschränkter Netzzugriff)
SAML	Security Assertion Markup Language
Schuban	Schutzbedarfsanalyse
SD	Standarddienst
SG-PKI	Swiss Government PKI
SMS	Short Message Service
SSH	Secure Shell
SSO	Single Sign-On
SZ	Server Zone
SZ+	Server Zone mit erhöhtem Schutzbedarf
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
VE	Verwaltungseinheit
VSK	verschlüsselte Sprachkommunikation

Referenzen

- [CyRV] Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) vom 27. Mai 2020
- [E021] DTI, E021 - Einsatzrichtlinie Smartphone/Smarttablet Sync, Version 2.1 vom 9. Juni 2020
- [E026] DTI, E026 - Einsatzrichtlinie Arbeitsplatzsystem, Version 1.0 vom 11. Juni 2019 (wird im Hinblick auf das Mobile Arbeiten überarbeitet)
- [E027] DTI, E027 - Einsatzrichtlinie Verschlüsselte Sprachkommunikation (VSK), Version 1.1 vom 1. Oktober 2021
- [ISchV] Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007
- [SB003] NCSC, Malwareschutz Strategie in der Bundesverwaltung, 2021
- [Si001-Hi01] Massnahmenumsetzung zum IKT-Grundschatz in der Bundesverwaltung, Version 4.6 vom 31. März 2021
- [Si001-Hi03] Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung, Version 1.4 vom 31. März 2021
- [Si001-Hi04] Handlungsempfehlung zur operativen Umsetzung von Einwilligungsverfahren, 15. Dezember 2020
- [Si002-Hi01] Antrag für unpersönlicher Account (E- und F-Accounts), 15. Dezember 2020
- [Si004] Regelung der Zugriffe auf Ressourcen im Internet, Web Proxy Richtlinie BV, Version 1.3 vom 4. Oktober 2016 (Stand 1. April 2019)

Anhang A: Zonenmodell Bund

Das Zonenmodell Bund (vgl. Abbildung A.1) ist ein generisches Modell für die Zonenbildung in der Bundesverwaltung. Es legt fest, wie die IT-Systeme bzw. Netzwerke der Bundesverwaltung in Zonen und Unterzonen organisiert und betrieben werden müssen.

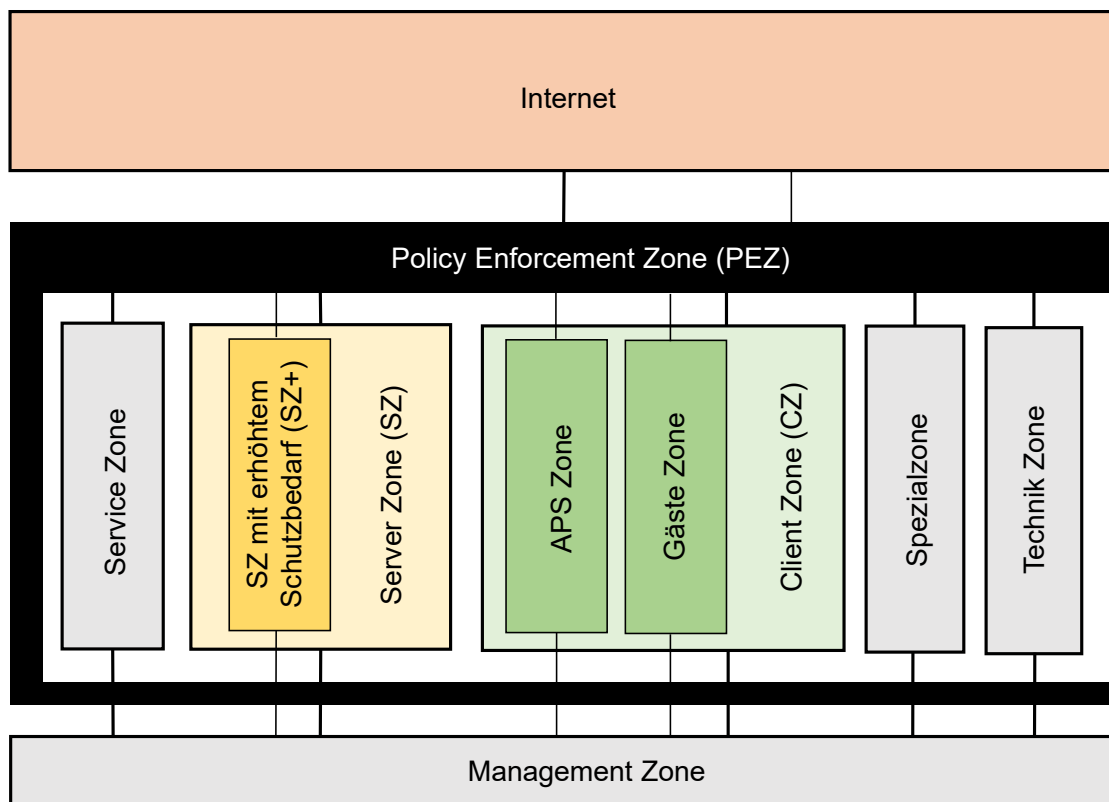


Abbildung A.1: Zonenmodell Bund

Im Zonenmodell Bund werden die folgenden Zonen und Unterzonen unterschieden:

- Internet:** Zone, welche keine der Kriterien für die übrigen Zonen entspricht und an welche keine (Sicherheits-) Anforderungen gestellt werden können.
- Policy Enforcement Zone (PEZ):** Zone für PEPs, die zur Durchsetzung der Regeln für die externe Kommunikation anderer Zonen erforderlich sind.
- Service Zone:** Zone für Server-Systeme, die für die Erbringung von Infrastrukturdiensten erforderlich sind (z.B. DNS- und Zeitserver).
- Server Zone (SZ):** Zone für Server-Systeme, auf denen Anwendungen mit nicht erhöhtem Schutzbedarf gemäss Schutzbedarfsanalyse (Schuban) betrieben werden.
- Server Zone mit erhöhtem Schutzbedarf (SZ+):** Unterzone der SZ für Server-Systeme, auf denen Anwendungen mit erhöhtem Schutzbedarf gemäss Schutzbedarfsanalyse (Schuban) betrieben werden⁴⁶.

⁴⁶ Falls für den Betrieb einer Anwendung mit erhöhtem Schutzbedarf mehrere Server-Systeme erforderlich sind, dann muss die Verteilung der verschiedenen Systeme auf die SZ und SZ+ im ISDS-Konzept dokumentiert und begründet sein.

- f) **Client Zone (CZ):** Zone für Client-Systeme. Der Betrieb von Server-Systemen in der CZ oder einer Unterzone ist zulässig, wenn dies in der Policy vorgesehen ist und die Server-Systeme primär von Client-Systemen der gleichen (Unter-) Zone benutzt werden (z.B. lokale Büroautomations- oder Printserver).
- g) **APS Zone:** Unterzone der CZ für Client-Systeme, die als Arbeitsplatzsysteme (APS) ausgelegt sind und ausschliesslich für den IKT-Standarddienst BA / UCC eingesetzt werden.
- h) **Gäste Zone:** Unterzone der CZ für Client-Systeme, die nicht von einer Verwaltungseinheit des Bundes betrieben werden, wie z.B. Geräte, die von externen Mitarbeiterinnen und Mitarbeitern oder Angestellten der Bundesverwaltung im Rahmen von „Bring Your Own Device“ genutzt werden.
- i) **Spezialzone:** Zone für IT-Systeme der Bundesverwaltung, die sich durch spezielle Eigenschaften und entsprechende Anforderungen auszeichnet, wie z.B. autarke Betriebbarkeit oder schmalbandige Netzwerkanbindung, und die aus der Management Zone heraus verwaltet und administriert werden kann (z.B. Transportnetz mit spezifischen Anforderungen).
- j) **Technik Zone:** Spezielle Zone für IT- und IoT-Systeme, wie z.B. Systeme für die Gebäudetechnik bzw. Facility Management, Zeiterfassungssysteme, Messsysteme und Systeme zur Ferndiagnose.
- k) **Management Zone:** Spezielle Zone für IT-Systeme, die ausschliesslich für die Verwaltung und Administration von IT-Systemen in anderen Zonen verwendet werden.

Jede (Unter-)Zone des Zonenmodells kann in der Bundesverwaltung auch mehrfach umgesetzt werden.

Anhang B: Sicherheitsstufen für Authentifikations- und Identitätsnachweismittel

Die heute zur Verfügung bzw. im Einsatz stehenden Authentifikations- und Identitätsnachweismittel mit entsprechenden Föderationsverfahren werden in die folgenden vier Sicherheitsstufen (tief, mittel, hoch und hoch+) eingeteilt⁴⁷:

- a) **Tief:** Die Authentifikationsinformation, die netzwerktechnisch übertragen wird, ist statisch und bei jeder Authentifikation identisch, d.h. sie kann von einem Angreifer abgegriffen und z.B. für einen «Replay»-Angriff und eine anschliessende Identitätstauschung missbraucht werden. Typisches Beispiel ist Benutzername und Passwort. Wird die Authentifikationsinformation als Föderationstoken im Sinne von I050 eingesetzt, dann muss diese nur schwach gegen Integritätsangriffe geschützt und an den Anwenderkontext gebunden sein. Beispiele sind verschiedene «Bearer-Token» wie Cookies.
- b) **Mittel:** Die Authentifikationsinformation ändert sich bei jeder Authentifikation dynamisch und kann entsprechend nicht für einen «Replay»-Angriff und eine anschliessende Identitätstauschung missbraucht werden. Beispiele sind Username und Passwort mit SMS-Verifikationscode oder Gerätebindung, OTP-Softwarelösungen (z.B. Google Authenticator) und von der SG-PKI ausgegebene Software-Zertifikate (Klassen C, D oder E). Wird die Authentifikationsinformation als Föderationstoken eingesetzt, dann muss diese gegen Integritätsangriffe geschützt und auf eine dem Stand der Technik entsprechende Art an den Anwenderkontext gebunden sein. Beispiele sind Kerberos-Tickets der Ressourcen-Forests des IKT-SD BA, sowie per SAML oder OIDC/OAuth übertragene «Bearer-Token» wie JWT.
- c) **Hoch:** Die Authentifikationsinformation ist dynamisch und hängt von einem kryptografischen Schlüssel ab, der in einem dedizierten Hardware-Modul gespeichert ist und von dort (mit vertretbarem Aufwand) nicht ausgelesen werden kann. Falls das Authentifikations- und Identitätsnachweismittel persönlich ist, muss die Registrierung der Person oder die Übergabe des Nachweismittels an die Person auf der Basis eines amtlichen Identitätsausweises (z.B. Reisepass oder Identitätskarte) erfolgen. Erfolgt die Identitätsüberprüfung der Person bei deren Registrierung, so muss die Übergabe des Nachweismittels per eingeschriebener Post erfolgen. Die Übergabe darf auch mit einem Geheimnis (z.B. Passwort/PIN) oder mit biometrischen Merkmalen (z.B. Touch ID oder Face ID im Falle von Apple oder Hello im Falle von Windows) geschützt erfolgen. Beispiele sind OTP-Token, OTP-Lösungen auf der Basis eines TPM, FIDO2-Token, Swisscom Mobile ID und SuisseID. Wird die Authentifikationsinformation als Föderationstoken eingesetzt, dann muss diese gegen Integritätsangriffe geschützt und auf eine dem Stand der Technik entsprechende Art an den Anwenderkontext gebunden sein. Insgesamt muss das Föderationsverfahren einem mit CC EAL4+-vergleichbaren Schutzprofil entsprechen. Beispiele sind SSO-Identity/SSO-Federation des SSO-Portals und Kerberos-Tickets der User-Forests, wenn diese auf der Basis einer Benutzerauthentifizierung mit einem von der SG-PKI ausgegebenen Klasse-B-Zertifikat ausgestellt worden sind.

⁴⁷ Der IKT-Standard I050 definiert vier Verlässlichkeitsstufen (Level of Assurance, LoA) 1 – 4, die zur Spezifikation der minimalen Sicherheitsanforderungen an die einzusetzenden Authentifikations- und Identitätsnachweismittel herangezogen werden könnten. Weil die LoA-Einstufung der heute verfügbaren und im Einsatz stehenden Authentifikations- und Identitätsnachweismittel aber noch nicht vorliegt, wird hier im Sinne einer Übergangslösung eine einfache und auf ein paar wenige technische Sicherheitsaspekte der Authentifikations- und Identitätsnachweismittel selbst fokussierende Einstufung verwendet.

- d) **Hoch+**: Das Authentifikations- und Identitätsnachweismittel erfüllt die Anforderungen der Stufe «hoch» (inkl. Anforderungen an das Föderationsverfahren). Zudem müssen sowohl das Hardware-Modul als auch der dahinterliegende Registrationsprozess vom NCSC für die Bundesverwaltung anerkannt sein. Einziges Beispiel sind von der SG-PKI ausgegebene Zertifikate auf Smartcards (Klasse B).

Die genannten Beispiele sind nicht abschliessend zu verstehen und in Tabelle B.1 summarisch zusammengestellt.

Sicherheitsstufe	Beispiele von Authentifikations- und Identitätsnachweismitteln
tief	<ul style="list-style-type: none"> • Benutzername und Passwort • «Bearer-Token» (z.B. Cookies)
mittel	<ul style="list-style-type: none"> • Benutzername und Passwort mit SMS-Verifikationscode⁴⁸ • Benutzername und Passwort mit Gerätebindung • OTP-Softwarelösung (z.B. Google Authenticator) • Von der SG-PKI ausgegebenes Software-Zertifikat (Klasse C, D oder E) • Kerberos-Tickets der Ressourcen-Forests des IKT-SD BA • Per SAML oder OIDC/OAuth übertragene «Bearer-Token» wie JWT
hoch	<ul style="list-style-type: none"> • OTP-Token (z.B. RSA, Vasco, ...) • OTP-Lösung auf der Basis eines TPM • FIDO2-Token • Swisscom Mobile ID • SuisseID (solange offiziell angeboten) • SSO-Identity/SSO-Federation des SSO-Portals • Im Rahmen von eIAM ausgegebene SAML-Token • Kerberos-Tickets der User-Forests (SG-PKI)
hoch+	<ul style="list-style-type: none"> • Von der SG-PKI ausgegebenes Zertifikat auf Smartcard (Klasse B)

Tabelle B.1: Sicherheitsstufen einiger Authentifikations- und Identitätsnachweismittel

Grundsätzlich kann durch das Kumulieren von mehreren Authentifikations- und Identitätsnachweismitteln einer Sicherheitsstufe diese Stufe nicht erhöht werden, d.h. ein der SG-PKI ausgegebenes Software-Zertifikat bleibt z.B. in der Sicherheitsstufe «mittel», auch wenn es mit Benutzername und Passwort mit SMS-Verifikationscode kombiniert wird.

⁴⁸ Grundsätzlich sollten SMS-basierte Authentifikationsverfahren nur noch eingesetzt werden, wenn es keine bessere Alternative gibt.

Anhang C: Zonenpolicy «Netzdomäne blau»

C.1 Anforderungen und Vorgaben an die IKT-Systeme

¹ Ein IKT-System darf in der Netzdomäne blau betrieben werden, wenn es die Anforderungen aus Kapitel 3a der CyRV namentlich in Bezug auf Schutzbedarfsanalyse (Schuban), IKT- bzw. IT-Grundschatz und ISDS-Konzept erfüllt.

C.2 Anforderungen und Vorgaben an die Netzdomäne blau

¹ Die Netzdomäne blau kann netzwerkmissig segmentiert sein.

² Eine Unterzonierung im Sinne von Kapitel 2 Absatz 2 Buchstabe j) ist m3glich.

C.3 Anforderungen und Vorgaben an die zulässige Kommunikation

C.3.1 Interne Kommunikation

¹ Die interne Kommunikation kann direkt erfolgen und unterliegt keinen über eine Netzwerksegmentierung hinausgehenden Einschränkungen.

C.3.2 Externe Kommunikation

¹ Die externe Kommunikation darf nicht direkt und muss über einen oder mehrere PEPs (z.B. in einer PEZ) erfolgen.

² Es muss sichergestellt sein, dass ein IKT-System in der Netzdomäne blau nicht gleichzeitig mehrere externe Kommunikationsbeziehungen mit IKT-Systemen in anderen Zonen unterhalten kann.

³ Für eingehende Kommunikationsbeziehungen gelten die folgenden Anforderungen und Vorgaben:

- a) Als Protokolle werden ausschliesslich Protokolle verwendet, die offengelegt und standardisiert sind oder für die es einen vertrauenswürdigen Reverse Proxy Server gibt. Für Webservices müssen die Protokolle/Datenformate SOAP/XML, REST/XML und/oder REST/JSON verwendet werden.
- b) Die Kommunikation wird über einen Reverse Proxy Server geführt, der (i) die die Kommunikationsbeziehung anstossende Person authentifiziert, (ii) den Datenverkehr absichert und (iii) die Randdaten der Kommunikation aufzeichnet und zeitnah auswertet. Im Falle von Webservices ist eine Authentifizierung der Prozesse (Webservice Consumer und Webservice Provider) auf der Basis von anerkannten SSL/TLS-Zertifikaten ausreichend, und die Absicherung des Datenverkehrs muss durch eine Überprüfung der Nachrichteninhalte⁴⁹ und eine transparente Datenverschlüsselung und -authentifizierung auf der Basis von HTTPS erfolgen.
- c) Ein unbeschränkter Netzwerkzugriff ist nur von einem IKT-System aus möglich, das von einer Organisationseinheit der Bundesverwaltung betrieben wird.

⁴ Für ausgehende Kommunikationsbeziehungen gilt die Web Proxy Richtlinie BV [Si004].

⁴⁹ Falls eine End-zu-End-Verschlüsselung zwischen Webservice Consumer und Webservice Provider erforderlich ist und der Webservice Firewall die Nachrichteninhalte entsprechend nicht direkt überprüfen kann, sind komplementäre Massnahmen einzusetzen, damit die Nachrichteninhalte wenigstens indirekt überprüft werden können.

Anhang D: Zugriffsmatrix blaue Netzdomäne und SSZ

Die folgenden Tabellen sind der Version 4.0 der Zugriffsmatrix (ehemals Si002) entnommen und gelten für die Authentifizierung von Personen an der blauen Netzdomäne und der SSZ (Tabelle D.1), bzw. für die Authentifizierung von Partnersystemen und Prozessen (Tabelle D.2). Die Ausnahmebestimmungen für E-Government-Anwendungen (Anforderung Z2.1 a)) gelten nach wie vor.

	Schutzniveau	Basis (SN0)				1 (SN1)				2 (SN2)			
	Benutzerterminal	BC	BC	FT	FT	BC	BC	FT	FT	BC	BC	FT	FT
	Zugriffsmethode	NW	RA	NW	RA	NW	RA	NW	RA	NW	RA	NW	RA
Blaue Netzdomäne	Hard Crypto Token	j	j	n	j	j	j	n	j	j	j	n	j
	OTP	j	j	n	j	j	j	n	j	j	j	n	j
	OTP ohne Device	n	j	n	j	n	j	n	j	n	n	n	n
	Soft Crypto Token	n	n	n	n	n	n	n	n	n	n	n	n
	Password or PIN token	n	n	n	n	n	n	n	n	n	n	n	n
SSZ	Hard Crypto Token	j ⁵⁰⁾	j	n	j	j ⁵⁰⁾	j	n	j	j ⁵⁰⁾	j	n	j
	OTP	j ⁵⁰⁾	j	n	j	j ⁵⁰⁾	j	n	j	j ⁵⁰⁾	j ⁵⁰⁾	n	j
	OTP ohne Device	n	j	n	j	n	j	n	j	n	n	n	n
	Soft Crypto Token	n	j	n	j	n	j	n	j	n	n	n	n
	Password or PIN token	n	j	n	j	n	j	n	j	n	n	n	n

Tabelle D.1: Authentifizierung von Personen an der blauen Netzdomäne bzw. der SSZ

	Schutzniveau	Basis (SN0)		1 (SN1)		2 (SN2)	
	Zugriffsmethode	NW	RA	NW	RA	NW	RA
Blaue Netzdomäne / SSZ	Hard Crypto Token	n	j	n	j	n	j
	OTP / OTP ohne Device	Keine praktischen Anwendungen					
	Soft Crypto Token	n	j	n	j	n	j ⁵¹⁾
	Password or PIN token	n	j ⁵²⁾	n	n	n	n

Tabelle D.2: Authentifizierung von Partnersystemen und entsprechenden Prozessen

⁵⁰ Der einzige Anwendungsfall ist die Administration von Systemen via Admin-LAN (Management Zone LE).

⁵¹ Nur zulässig für den Zugriff auf Sedex und andere Anwendungen, über die nur standardisierte Nachrichten ausgetauscht und/oder definierte Abläufe verfolgt werden können.

⁵² Nur zulässig für Telemetriedaten (Messgeräte).

Anhang E: Änderungen gegenüber Version 4.6 (Stand 1. Januar 2021)

Im folgenden ist erläutert, wie die Anforderungen der Si001 Version 4.6 (linke Spalte) in der Version 5.0 eingepflegt sind. Die Erläuterungen beschränken sich auf die Anforderungen, die in Version 4.6 noch nicht weggefallen und explizit aufgeführt sind.

- Zu 2.1.1: Die Einschränkung, dass nur MDM-Systeme mit Systemen der Bundesverwaltung kommunizieren dürfen, erscheint aus heutiger Sicht zu einschränkend, zumal es im Zonenmodell auch Spezialzonen und eine Gäste Zone gibt. Inhaltlich wird ein Unterschied zwischen MDM-Systemen (die auch Bundesclients sind) und anderen Smart Devices gemacht. Gemäss I1* und I2.2 bzw. der dazugehörigen Fussnote ist die Speicherung und Verarbeitung von geschäftsrelevanten Daten (bis und mit Klassifikationsstufe INTERN) nur auf MDM-Systemen zulässig. Insofern wird diesem Punkt Rechnung getragen. Die erwähnten Ausnahmen sind sinngemäss in Z2.1 a) übernommen (zusammen mit anderen Ausnahmesituationen).
- Zu 2.1.2: Folgt aus I2.2 und der dazugehörigen Fussnote. Die Bearbeitung von als GEHEIM klassifizierten Informationen ist auf allen Arten von Smart Devices unzulässig.
- Zu 2.1.6: Diese Anforderung ist in verallgemeinerter Form in O2.1 Buchstabe e) und für MDM-Systeme in S5.1 übernommen. Auf die zusätzliche Anforderung, dass die «Regelung den Verwaltungseinheiten in geeigneter Form zur Kenntnis gebracht werden» muss, wird verzichtet. Diese Anforderung gilt grundsätzlich für alle Regelungen.
- Zu 2.1.8: Diese Anforderung ist in T6.2 und S5.2 übernommen.
- Zu 3.1.1: Diese Anforderung ist in P1.1 übernommen.
- Zu 3.1.2: Diese Anforderung ist bezogen auf Zugriffsrechte in T5.1 und T5.2 übernommen. Die Zutritts- und Zugangsrechte sind Gegenstand der physischen Schutzmassen und mit O2.1 b) abgedeckt.
- Zu 3.1.3: Diese Anforderung gilt unabhängig vom Grundschutz und muss nicht in diesem geregelt werden (betrifft das ISG und dessen Umsetzung).
- Zu 4.1.2 / 4.1.3: Diese Anforderungen sind sinngemäss in I1* übernommen. Dem Schutzbedarf ist dabei grundsätzlich immer Rechnung zu tragen (nicht nur bei privaten IKT-Mitteln).
- Zu 5.1: Diese Anforderung ist inhaltlich in I4 übernommen.
- Zu 6.1: Diese Anforderung ist in S5.1 übernommen.
- Zu 6.2: Diese Anforderung ist als Beispiel in P2 übernommen (zusammen mit anderen sicherheitskritischen Ereignissen).
- Zu 7.1.1: Diese Anforderung ist in T5.1 bzw. Z2 (für Zonen) übernommen.
- Zu 7.1.4: Diese Anforderung ist in T5.1 und T5.2 übernommen.
- Zu 7.1.5: Diese Anforderung ist in S5.4 übernommen und in T8.2 im Sinne einer PAM-Lösung erweitert (bzw. T8.1 für das Logging).
- Zu 7.1.6: Diese Anforderung ist in abgeschwächter Form in T5.2 bzw. der entsprechenden Fussnote übernommen. Die Abschwächung betrifft die

«Gewaltentrennung zwischen Bewilligung und Vergabe von Zugriffsrechten», die nur wenn möglich und sinnvoll einzuhalten ist. Dokumentiert werden muss sie in jedem Fall.

- Zu 7.1.7: Diese Anforderung ist in T6.1 übernommen (2FA). Die Möglichkeit für unpersönliche E- und F-Accounts bleibt in T7.1* bzw. der entsprechenden Fussnote weiterhin bestehen. Diese können gemäss [Si002-Hi01] beantragt werden.
- Zu 7.1.8: Diese Anforderung ist in T8.3 übernommen und präzisiert.
- Zu 7.1.9: Diese Anforderung ist in Z2.2 (letzter Punkt) übernommen.
- Zu 7.1.10: Diese Anforderung ist in S5.5 übernommen.
- Zu 7.1.11: Diese Anforderung ist in S3.1 übernommen.
- Zu 8.1: Diese Anforderung ist in zwar vereinfachter Form aber um Server-seitige Anforderungen an die Passwortverwaltung in T7 übernommen.
- Zu 8.2: Diese Anforderung ist T7.1* a) bzw. der entsprechenden Fussnote übernommen.
- Zu 8.3: Diese Anforderung ist sinngemäss aber in stark vereinfachter Form in S3.2* übernommen.
- Zu 8.4: Diese Anforderung ist in T5.3 übernommen. Die Argumentation erfolgt aber über die Zulässigkeit der einzusetzenden Authentifikations- und Identitätsnachweismittel.
- Zu 9.1: Diese Anforderung ist T8.1 und T8.2 übernommen.
- Zu 9.2: Diese Anforderung ist im Zonenmodell Bund mit dem Konstrukt einer Management Zone übernommen. Allerdings erscheint das grundsätzliche Verbot des Zugangs zum Internet und zur Büroautomation als zu einschränkend und nicht praktikabel. Diese Zugriffsmöglichkeiten müssen in der Policy der Management Zone geklärt sein. Die Forderung nach einer 2-Faktoren-Authentifizierung ist in T6.1 übernommen. Weitere Anforderungen an die Administration ergeben sich aus T8.1 und T8.2.
- Zu 9.3: Diese Anforderung scheint nicht mehr sinnvoll. Jedes im Einsatz stehende Authentifikationsverfahren beschränkt die zur Verfügung stehende Zeit sowieso.
- Zu 9.4: Diese Anforderung ist auf Bundesclients eingeschränkt in S5.2 übernommen. Für Server und Anwendungen erscheint die Anforderung zu einschneidend und benutzerunfreundlich. Im Einzelfall kann natürlich eine zeitliche Schranke sinnvoll sein und entsprechend definiert werden.
- Zu 10.1.1: Diese Anforderung ist in verallgemeinerter Form als Grundsatz und Prinzip 5 (Stand der Technik) übernommen. Dabei wird auf das gleiche Dokument verwiesen.
- Zu 10.1.3: Im Zusammenhang mit der 2-Faktoren-Authentifikation auf der Basis von Zertifikaten (Fussnote zu T6.1) wird weiterhin auf die SG-PKI verwiesen. Dass jeder LE nur Zertifikate einer von ihm akzeptierten CA einsetzt, braucht nicht speziell erwähnt zu werden.
- Zu 10.1.4: Diese Anforderung ist in I2.1 übernommen
- Zu 10.1.5/6: Diese Anforderungen sind in der Vergangenheit nicht wirklich umgesetzt worden und haben wahrscheinlich auch nur begrenzten Nutzen. Insofern

sind sie nicht übernommen bzw. in den Punkten zu den Schutzmassnahmen, die dem Stand der Technik entsprechen müssen, und der Dokumentationspflicht zur Schlüsselverwaltung subsummiert.

- Zu 11.1.1/2: Diese Anforderungen sind in O2.1 b) übernommen.
- Zu 12.1.1: Die Dokumentationspflicht ist in etwas anderer Form in O2 übernommen.
- Zu 12.1.2/3: Diese Anforderungen sind in dieser Form nicht direkt umsetzbar bzw. ergeben sich aus dem laufenden Betrieb. Sie sind entsprechend nicht übernommen und sind eher Gegenstand eines Betriebskonzeptes.
- Zu 12.1.4: Diese Anforderung ist in T3 übernommen. Allerdings haben nicht alle Schutzobjekte nicht produktive Umgebungen (insbesondere im Bereich der agilen Entwicklung).
- Zu 12.2.1/2: Diese Anforderungen sind in S4.3 übernommen (Informationspflicht ergibt sich aus P2).
- Zu 12.2.3: Diese Anforderung ist in S2 bzw. einer entsprechenden Fussnote übernommen.
- Zu 12.2.4: Diese Anforderung ist in S5.3 übernommen.
- Zu 12.3.1/2: Diese Anforderungen sind sinngemäss in I3 übernommen.
- Zu 12.4.1: Diese Anforderung ist in vereinfachter und summarischer Form in T2.1 c) und Z5 (für Zonen) übernommen.
- Zu 12.4.2: Diese Anforderung ist in dieser Form nicht mehr erforderlich (eine Zeitsynchronisation findet fast überall statt).
- Zu 12.4.3: Ergibt sich aus den Bemerkungen zu 12.4.1.
- Zu 12.4.4: Diese Anforderung ist sinngemäss in S4 (insbesondere S4.1 und S4.2) übernommen.
- Zu 12.5.1: Diese Anforderung ist in S4.1 (für IT-Systeme) und A1.2 e) (für Anwendungen) übernommen.
- Zu 12.6.1: Diese Anforderung ist in S2 (für IT-Systeme) bzw. A2 (für Anwendungen) übernommen.
- Zu 12.6.2: Diese Anforderung ist in T4 übernommen. Der Verweis auf OWASP ist in A1.1 bzw. der entsprechenden Fussnote mit übernommen.
- Zu 12.7.1/2: Diese Anforderung ist in O2.1 g) bzw. der entsprechenden Fussnote mit übernommen.
- Zu 13.1.1: Für Netze gilt die Dokumentationspflicht gemäss O2. Zudem sind sie Teil einer Zone und müssen den Vorgaben des Zonenmodells gemäss Z1 entsprechen. Diese Vorgaben umfassen eine Dokumentationspflicht.
- Zu 13.1.2: Die Frage der Virtualisierung ist in Grundsatz und Prinzip 2 (Virtualisierung) geklärt.
- Zu 13.1.3: Netzwerkkomponenten stellen auch IT-Systeme dar. Insofern ist diese Anforderung implizit mit übernommen.
- Zu 13.1.4: Die wichtigsten Punkte dieser Anforderung sind in T6.3 (Benutzerauthentifikation) und T8.3 (Fernzugriff) übernommen. Die anderen Punkte sind in anderen Anforderungen implizit enthalten.
- Zu 13.1.5: Diese Anforderung ist durch die Integration der Si003 implizit übernommen.

- Zu 13.1.6: Diese Anforderung ist Z5.2 übernommen und präzisiert.
- Zu 13.1.7: Diese Anforderung ist in I2 übernommen (Authentifikationsdaten sind geschäftsrelevant und haben einen hohen Schutzbedarf).
- Zu 13.1.10: Diese Anforderung ist in Z2.1 a) übernommen.
- Zu 14.1.1: Diese Anforderung ist in S6.1 und S6.4 (inklusive [E026]) übernommen.
- Zu 14.1.2: Diese Anforderung ist in T2.1 und T7.2* übernommen.
- Zu 14.1.3: Diese Anforderung ist in T2.2 übernommen.
- Zu 14.1.4: Diese Anforderung ist in T2.1 b) übernommen.
- Zu 14.2.1: Diese Anforderung ist in I2 übernommen. Demnach müssen Testdaten wie produktive Daten behandelt werden.
- Zu 15.1.1: Diese Anforderung ist in Grundstz und Prinzip 1 (Form der Leistungserbringung) bzw. in O2.1 f) und I1* übernommen.
- Zu 15.2.1: Dass die «Offenbarung von Amtsgeheimnissen an externe IKT-Anbieter zu minimieren ist» versteht sich von selbst und muss hier nicht erwähnt werden. Ansonsten ist die Anforderung weitgehend in T8.3 übernommen.
- Zu 16.1/2: Diese Anforderungen sind im Rahmen des Prozesses zur Bewältigung von Cybervorfällen gemäss O4 abgedeckt.
- Zu 17.1.1: Diese Anforderung ist für ITSCM und BCM in O3 übernommen.