Fachhochschule Nordwestschweiz
Hochschule für Informatik

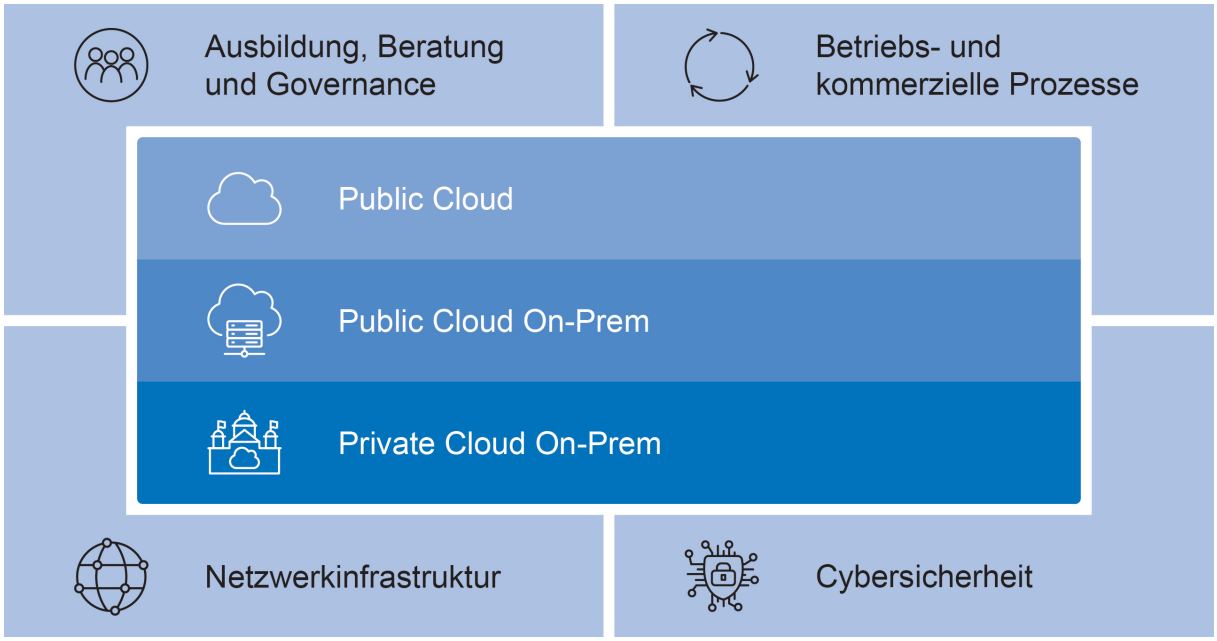
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik
und Telekommunikation BIT

Cloud Governance in einer multi-provider Cloud

Projektvereinbarung IP5

Windisch, März 2025



Studentin/Student	Frithjof Hoppe Benjamin Dätwyler
Expertin/Experte	Sebastian Matyas
Fachbetreuer/in	Sebastian Graf
Auftraggeberin	Thierry Perroud
Projektnummer	25FS_IMVS29

Fachhochschule Nordwestschweiz, Hochschule für Informatik

Inhaltsverzeichnis

1 Ausgangslage

Das Bundesamt für Informatik und Telekommunikation verfolgt mit dem Swiss Government Cloud (SGC) Vorhaben die Transformation der Cloud-Infrastruktur der Bundesverwaltung. Vision ist es einen auf die Bedürfnisse des Bundes zugeschnittene hybride Multi-Cloud Infrastruktur aufzubauen.

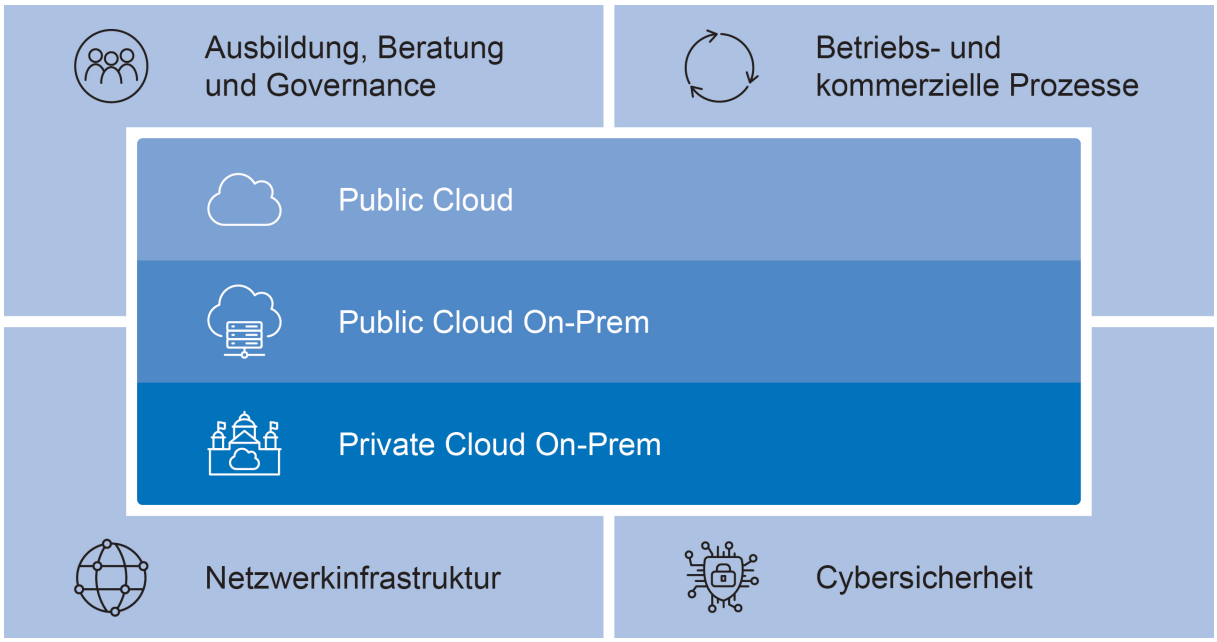


Abbildung 1.1: Das Vorhaben SGC im Überblick

Heute verteilt sich die Infrastruktur des Bundesamt für Informatik und Telekommunikation (nachfolgenden als BIT bezeichnet) vereinfacht dargestellt wie folgt:

- OnPremise/Private-Cloud Hosting Umgebung welches durch das BIT selbst betrieben wird
- Public-Cloud Hosting Umgebung bei unterschiedlichen Cloud-Anbietern wie Microsoft Azure und Amazon AWS

2 Problemstellung

Mit dem Betreiben von Services geht die Einhaltung von governance Regeln einher.

Die Sicherheitsanforderungen der Fachanwendungen entstehen oft aus Standards / Richtlinien / Normen der BV welche manuell und plattformspezifisch umgesetzt werden. Nennenswert ist hier u.A. Si001 für den IT Grundschutz in der Bundesverwaltung welcher ein Mindestmass an Vorgaben gibt.

Die daraus resultierenden Regeln werden oft unterschiedlich definiert, abgelegt und angewendet. Zusätzlich besteht die Gefahr, dass Standards/Richtlinien/Normen der BV unterschiedlich interpretiert werden können und somit dann andere Regeln angewendet werden.

Mit Ausblick auf das SGC Vorhaben bekommt diese Situation nochmals mehr an Bedeutung weil die Anzahl an Plattformen steigt und es somit schwieriger wird die Übersicht zu wahren.

3 Zielsetzung

3.1 Forschungsfragen

3.1.1 Compliance-Aspekte

Welche wichtigen Aspekte eines Schutzobjektes sind für die Compliance zu berücksichtigen?

// Frage aus meeting mit Graf am 05.03. ZU löschen? *Welche wichtigen Aspekte sind für die Compliance auf der SGC zu berücksichtigen? Wie können diese Aspekte auf die verschiedenen Plattformen angewendet werden? Wie werden diese Aspekte heute innerhalb des BITs implementiert?*

Die einzelnen Serviceangebote der Cloud-Provider bieten jeweils unterschiedliche Servicelevel, zum Teil auch variierend zwischen Standorten. Die wichtigsten Aspekte (von Schutzobjekten) welche in eine Compliancеprüfung gehören sollen identifiziert werden.

Wir wollen erforschen, wie ein Mapping zwischen den relevanten Eigenschaften von Services in der Cloud und den Aspekten von Schutzobjekten implementiert werden kann.

3.1.2 Erforschung bestehende Produkte, Konzepte, Ansätze und Frameworks

Welche Konzepte und etwaige Produkte existieren bereits zur plattformübergreifenden Prüfung und Enforcement von Compliance?

Im Rahmen der Lösungsfindung soll von bereits bestehenden Produkten profitiert werden. Wir wollen herausfinden, welche Produkte bereits existieren und wie diese die Compliancеprüfung durchführen. Nützliche Ansätze und Konzepte sollen hervorgehoben und für eine allfällige Eigenimplementation ggf. in Betracht gezogen werden. Hier wollen wir Produkte untersuchen welche die Compliancеprüfung direkt/proprietär umsetzen, unabhängig von der dahinterliegenden Technologie.

Welche bestehenden Frameworks, Sprachen oder Konzepte sind am besten geeignet zur Umsetzung von cloud-übergreifender Compliance?

Schutzobjekte (z.B. Applikationen) werden in der SGC cloud-nativ (via zugehörigem Deployment Code) deployed. Somit wäre der Deployment Code der richtige Ort festzulegen, welche Compliance-Regeln eingehalten werden müssen. Wir möchten hier Konzepte, Ansätze und Frameworks erforschen, welche die cloud-native Umsetzung der Compliance ermöglichen.

3.1.3 Konzeption eines Frameworks

Wie muss ein Framework Compliance Regeln implementieren sodass eine Anwendung durch verschiedenen Interessengruppen möglich ist?

Um verschiedenen Regelwerke (Si001 etc.) einheitlich anzuwenden ist eine Art Sprache notwendig die es den verschiedenen Experten (sei es CISO, Projektverantwortlichen) erlaubt ihre Bedürfnisse auszuformulieren. Diese muss gleichzeitig durch ein System interpretiert werden können damit die entsprechenden Massnahmen ergriffen werden können.

3.2 Ziele

Die folgenden Ziele gelten für die gesamte Arbeit und orientieren sich an den Forschungsfragen. Aktuell wird davon ausgegnagen dass die Erkenntinsse in einem Artefakt resultieren welches

die genantne Ziele implementiert. Dieses Artefakt wird nachfolgend als Framework bezeichnet welches jedoch die Art umd des Artefakts nicht einschränken soll.

#	**Ziel**
1	Ein Konzept für die technische Umsetzung einer plattformübergreifenden (mindestens zwei Public on eine Private Cloud) Cloud-Governance im Rahmen des SGC-Vorhabens bis zum 14.08.2025 umgesetzt
2	Ein Framework welches mindestens die Ist-Situation einer multi plattformübergreifende Cloud-Umgebung gegenüber Governancen Vorgaben analysiert ist bis zum 14.08.2025 umgesetzt

Tabelle 3.1: Ziele

3.2.1 Abgrenzung

Bei der Thematik die behandelt werden soll handelt es sich um ein weites Feld, weshalb die Zielerreichung wie folgt eingeschränkt wird:

- Das Framework deckt einen Servicetyp (z.B. k8s) einer Public-Cloud Plattform ab
- Das Framework deckt einen Servicetyp einer Public-Cloud und einer private Cloud Plattform des BIT ab
- Das Framework deckt mindestens zwei Public-Cloud Plattformen und eine private Cloud Plattform ab
- Das Framework kann mindestens reaktiv zur Prüfung der Compliance eingesetzt werden

3.3 Meilensteine

Die folgenden Meilensteine sind ebenfalls im

#	**Datum**	**Meilenstein**
1	09.03.2025	Projektvereinbarung signiert
2	xx.xx.xx	Bestehenden Praktiken der verschiedenen internen Interessengruppen sind bekannt
2	xx.xx.xx	Recherche von bestehenden Produkten, deren Funktionalität, Gemeinsamkeiten und Deckung von Anforderungen ist erfolgt
3	xx.xx.xx	erster Entwurf Konzept für Framework
3	xx.xx.xx	Implementation erster PoC
3	14.08.25	Abgabe Arbeit

Tabelle 3.2: Meilensteine

4 Technologien

Die effektiv verwendeten Technologie ergeben sich erst durch die Arbeit. Folgende Liste soll einen ungefähren Eindruck ergeben, die Motivation aufzeigen und ist nicht abschliessend:

- **Infrastructure as Code und Policy as Code** IaC Tool wie Terraform oder Pollumi provisionieren von Ressourcen in Cloud-Umgebugen. Ähnlich dazu besitzten die verschiedenen Cloud-Provider ihre eigenen Configuration Languages und services. Diese können als Basis für eine eigenen DSL dienen. Beispiele: Azure Sentinel, Open Policy Agent / Rego
- **Public Cloud / Hyperscaler** Repräsentiert durch die verschiedenen grösseren Plattformen wie AWS, Azure, (RedHat) Openshift im potentiellen SGC Umfeld dienen diese uns als Analyse-Objekte
- **CSPM Tools** Cloud services posture management richet unterstützt unter Anderem die Erkennung und Abwehr von Risiken in Bezug auf eine Cloud-Umgebung und die allg Einhaltung von Vorgaben. Hier exisieren von diversen Hyperscalern bereits Plattformen von denen wir profitieren können. Beispiele: Azure Defender, AWS Security Hub etc.
- **CWPP Tools** Cloud workfload protection tools erkennen die workload welche in einer bspw Cloud-Umgebung vorhanden sind und führt automatisch Bewertungen durch. Tools bzw die Idee dieser Art könnten die Grundlage für unser angedachtes Framework darstellen. Beispiele: Falco, Twistlock
-

5 Projektorganisation

Das ip5 Projekt läuft ab der Freigabe der Projektvereinbarung bis zum 14.08.2025. Die erbrachte Leistung sollte den erwarteten 180h pro Teammitglied entsprechen. Wir orientieren uns hierzu an der agilen Methodik Kanban. Hierunter verstehen wir konkret, dass:

- Die verschiedenen Tasks werden für jeden Projektbeteiligten sichtbar geführt (TODO hier link GithubBoard)
- Das Team inklusive dem PO synchen sich mindestens alle zwei Wochen um den aktuellen Stand zu tracken
- Die Arbeit erfolgt nicht in sprints sondern allg nach Priorität welche aus den jeweiligen Syncs hervorgeht
- Den Stakeholde wird alle 4 Wochen der aktuelle Stand präsentiert, bei welchem sie Ihren Input eingeben können

5.1 Austausch

Der Austausch inklusive den Synch wird zwischen den beteiligten erfolgt bevorzugt über den vorgesehen Teams-Kanal, damit alle Interessierten auch passiv teilnehmen können.

Objekt	Ort
Projektarbeit	Die Projekt arbeit wird auf im ip5-paper repo als LaTex Dokument abgelelgt
Code-Basis	Die verschiedenen Code-Bases werden unter ein separaten Github Organization im Sinne des EMBAG öffentlich abgelegt

Tabelle 5.1: Verwendete Plattformen

5.2 Zeitplan

Das folgende Gantt-Diaramm stellt die Arbeit mit den Meilensteinen und groben Tasks da. Zu erwähnen ist hierbei, dass die detaillierten Tasks mittels Kanban-Board getracked werden.

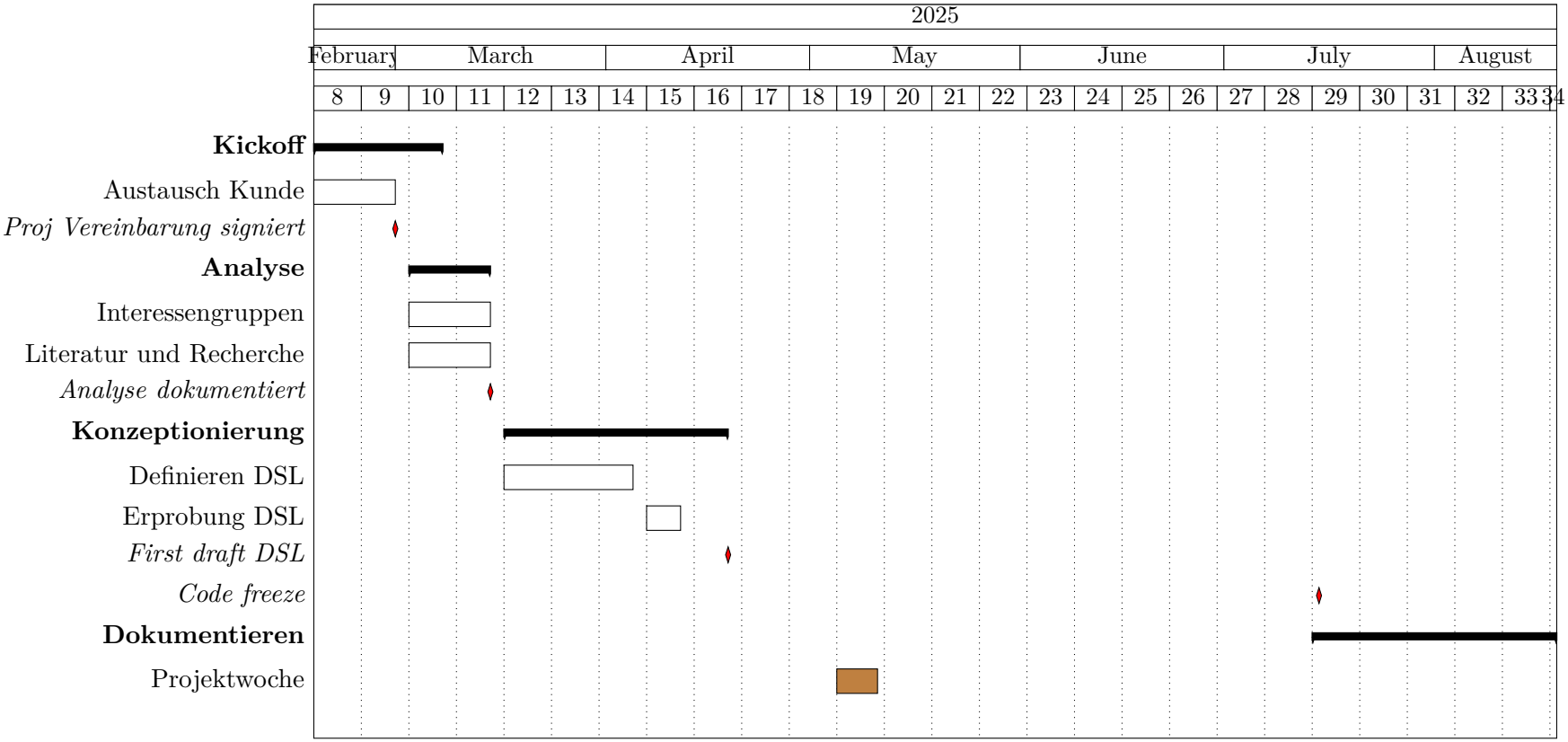


Abbildung 5.1: Time Plan

A Si001

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Version 5.1

Si001 – IT-Grundschutz in der Bundesverwaltung

vom 5. Juli 2024

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Gegenstand

[1] Auf der Basis von Artikel 29 Absatz 1 ISV[1] legt diese Weisung die Mindestanforderungen der Sicherheitsstufe «Grundschutz» nach Artikel 17 Absatz 1 ISG[2] für sämtliche Informatikmittel, sofern diese nicht höher eingestuft werden müssen, fest. Gemäss Artikel 18 Absatz 2 ISG müssen diese Anforderungen von sämtlichen Informatikmitteln erfüllt werden.

[2] Jede Verwaltungseinheit (VE) ist für die Sicherheit ihrer Informatikmittel selbst verantwortlich und muss für sie diese Weisung umsetzen und einhalten, bzw. deren Umsetzung und Einhaltung kontrollieren.

[3] Die Umsetzung und Einhaltung dieser Weisung 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 Informatikschutzobjektverantwortlichen (gemäss Kapitel 2 Absatz 1 dieser Weisung),
b) der oder dem Informationssicherheitsverantwortlichen der VE (gemäss Artikel 36 ISV),
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 Informatikmittels beteiligten Leistungserbringer (LE) die sie betreffenden Anforderungen erfüllen.

[4] Die Kontrolle der Umsetzung und Einhaltung dieser Weisung 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 der oder dem Informationssicherheitsverantwortlichen abgesprochen und mitdokumentiert sein. Für ein Informatikschutzobjekt, 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] Gemäss Artikel 29 Absatz 1 ISV gilt diese Weisung für alle Organisationen nach Artikel 2 Absätze 1 – 3 ISV.

[2] Weitere rechtliche Rahmenbedingungen ergeben sich aus

a) der Bundesgesetzgebung über den Datenschutz für den Umgang mit Personendaten, sowie
b) 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 Weisung nicht erfüllen, braucht sie gemäss Artikel 9 Absatz 1 ISV eine

[1] SR 128.1

[2] SR 128

Ausnahmebewilligung. Diese kann auf eine der in den folgenden drei Absätzen 2 – 4 ausgeführten 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-Grundschutz» 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] Die oder der Informationssicherheitsverantwortliche der verantwortlichen VE kann einen formalen Ausnahmeantrag bewilligen, wenn die folgenden Voraussetzungen (kumulativ) erfüllt sind:

a) Die oder der Informationssicherheitsverantwortliche ist in den Ausnahmebewilligungsprozess so eingebunden, dass sie oder er ihre oder seine Verantwortung wahrnehmen kann.
b) Bei der Ausnahme geht es ausschliesslich um die Verwendung von Informationen der verantwortlichen VE oder andere Informatikschutzobjekte, 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.
d) 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.
e) Die oder der Informationssicherheitsverantwortliche führt ein aktuelles Verzeichnis der erteilten Ausnahmebewilligungen und bringt diese auf Anfrage der Fachstelle des Bundes für Informationssicherheit zur Kenntnis.

[4] Alle anderen Ausnahmeanträge können über das IKT-Anforderungs- und Vorgabenmanagement Bund (P035) eingereicht werden. Im entsprechenden Antrag müssen die Unterschreitungen des IT-Grundschutzes 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] Gemäss Artikel 17 Absatz 1 ISG gilt die Sicherheitsstufe «Grundschutz» für sämtliche Informatikmittel, es sei denn, sie müssen höher eingestuft werden. Der im Gesetz verwendete Ausdruck «sämtliche Informatikmittel» umfasst hierbei sowohl einzelne als auch mehrere gleichartige oder zusammenhängende Informatikmittel, da mit dem ISG/ISV eine umfassende Sicherheitsabdeckung angestrebt wird. Insbesondere auch in der Praxis der Bundesverwaltung werden solche Informatikmittel oft als zusammenhängende Einheiten betrachtet, die daher nachfolgend in dieser Weisung als **Informatikschutzobjekte** bezeichnet werden. Diese Sichtweise ermöglicht eine präzisere Identifikation und Verwaltung der zu schützenden Einheiten und trägt zur Klarheit und Effizienz in der Umsetzung der nachfolgenden Sicherheitsmassnahmen bei. Für jedes Informatikschutzobjekt muss eine **Informatikschutzobjektverantwortliche** oder ein **Informatikschutzobjekt-verantwortlicher** definiert sein.

[2] In dieser Weisung bedeuten zudem:

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

b) **Informationssicherheits- und Datenschutz (ISDS) Konzept:** Strukturierte Beschreibung der Sicherheitsanforderungen eines Informatikschutzobjekts, der geplanten und umgesetzten Sicherheitsmassnahmen, sowie der verbleibenden Restrisiken.

c) **Informationen:** Elektronisch gespeicherte, verarbeitete und/oder übertragene Daten[3]. 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 wird[4]. Im zweiten Fall kann das IT-System als virtualisiert bezeichnet werden.

e) Ein IT-System gilt als[5]

- **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, Messwerte[6] 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

[3] In dieser Weisung 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 präzis, 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 akkustische und/oder optische Signale handeln.

OSI-Referenzmodell arbeitet ein PEP bis und mit Schicht 7 (Anwendungsschicht), und kontrolliert in diesem Sinne auch das (die) vermittelte(n) Kommunikationsprotokoll(e).

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 Netzwerkomponenten und Verbindungen) zum Datenaustauch zwischen IT-Systemen.

h) **Netzweksegment (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 netzwerkmässige 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 netzwerkmässig 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 Kommunikationsbeziehungen[7]. Eine Kommunikation zwischen zwei oder mehr gleichen Zonen[8] 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).

[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.

3 Grundsätze und Prinzipien

[1] **Form der Leistungserbringung:** Der IT-Grundschutz gilt für alle Informatikschutzobjekte unabhängig von der Form der Leistungserbringung, d. h. die LE betreffenden Sicherheitsanforderungen und -massnahmen müssen sowohl von internen als auch von externen LE umgesetzt werden. Bei externen LE muss insbesondere sichergestellt sein, dass die Informatiksicherheitsvorgaben eingehalten[9] und die entsprechende Einwilligung der vorgesetzten Behörde gemäss den amts- bzw. departementsspezifischen Prozessen eingeholt sind (vgl. [Si001-Hi04]).

[2] **Virtualisierung:** Der IT-Grundschutz gilt unabhängig von der Frage, ob ein Informatikschutzobjekt 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 Informatikschutzobjekts 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.

[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 entsprechen[10], 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 Anwendungen[11], die aktivierten Dienste und Zusatzfunktionalitäten («Features») von IT-Systemen und Anwendungen, sowie die zulässigen Kommunikationsbeziehungen im Rahmen von Zonenpolicies[12].

[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 mit berücksichtigt 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:** Informatikschutzobjekte müssen so entwickelt, konfiguriert und betrieben werden, dass alle in einem spezifischen Umfeld sinnvollen Sicherheitsmassnahmen standardmässig aktiviert sind und ihre Wirkung entfalten können, ohne dass sich die Benutzerinnen und Benutzer darum kümmern müssen.

---

[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 geben die «Empfehlungen zu kryptografischen Verfahren für den Grundschutz» der FUB ZEO KRYPT vom 24.1.2023 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.

[10] **Produkteneutralität:** Die Vorgaben und Empfehlungen sind grundsätzlich produkteneutral. Aussagen für oder gegen den Einsatz bestimmter Produkte werden nur abgegeben, wenn sie entweder einen IKT-SD betreffen[13] oder es andere gewichtige Gründe aus der Sicht der Informatiksicherheit gibt.

4 Sicherheitsanforderungen

[1] Für jedes Informatikschutzobjekt 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 strukturiert[14].

[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 Informatikschutzobjekte auch eingesetzt werden.

Organisation	
O1	Verantwortlichkeit Für das Informatikschutzobjekt muss eine verantwortliche Person (innerhalb der verantwortlichen VE) als Informatikschutzobjektverantwortliche/r definiert sein. Diese Person ist für die Umsetzung dieser Weisung zuständig. Sie muss sich ihrer Verantwortung bewusst und fachtechnisch in der Lage sein, die Verantwortung auch wahrzunehmen.
O2	Dokumentation O2.1 Für das Informatikschutzobjekt 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 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, d) die Schlüsselverwaltung beim Einsatz kryptografischer Verfahren, e) die Modalitäten und Prozesse bei Änderung (im Rahmen des «Change Managements»), Reparatur, Entsorgung und Verlust, f) die vertraglichen Vereinbarungen, sowie

[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.

	g) die Audit-Prozesse und -Aktivitäten[15] zur Kontrolle der Umsetzung und Einhaltung dieser Weisung mit einschliessen. O2.2 Wird das Informatikschutzobjekt (IT-System oder Anwendung) nicht in einer Zone der Bundesverwaltung betrieben (z. B. in einer Public Cloud), muss in der Dokumentation beschrieben sein, a) wie in dieser Umgebung dem Schutzbedarf des Objekts entsprochen werden kann, und b) mit welchen komplementären Sicherheitsmassnahmen sichergestellt wird, dass sich für andere Informatikschutzobjekte der Bundesverwaltung keine zusätzlichen Bedrohungen und Risiken ergeben.
O3	Geschäftskontinuität Für das Informatikschutzobjekt 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.
O4	Cybervorfälle Das Informatikschutzobjekt muss in den Prozess zur Bewältigung von Cybervorfällen eingebunden sein.
Personal	
P1	Sensibilisierung und Schulung P1.1 Alle Benutzerinnen und Benutzer des Informatikschutzobjekts müssen im Bereich der Informatiksicherheit stufen- bzw. funktionsgerecht sensibilisiert und geschult sein. P1.2 Alle Benutzerinnen und Benutzer des Informatikschutzobjekts müssen die für das Schutzobjekt relevanten Einsatzrichtlinien kennen und sind zu deren Einhaltung verpflichtet[16].
P2	Meldepflicht Alle Benutzerinnen und Benutzer des Informatikschutzobjekts müssen sicherheitskritische Ereignisse, wie z.B. anormales und verdächtiges Systemverhalten oder physischer Verlust, möglichst zeitnah der dafür zuständigen Stelle melden (z. B. Servicedesk des LE).

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

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

Technik	
T1	Betrieb Das Informatikschutzobjekt muss dem Stand der Technik entsprechend und unter Berück-sichtigung von branchenüblichen Sicherheitsvorgaben und -empfehlungen («Best Practices») betrieben werden.
T2	Konfiguration und Einstellung T2.1 Das Informatikschutzobjekt muss vor der ersten Inbetriebnahme so konfiguriert und eingestellt sein, dass a) es vor unberechtigtem Zugriff geschützt ist, b) 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 c) wichtige sicherheitsrelevante Aktivitäten und Ereignisse (mit Zeitangaben) aufgezeichnet und zeitnah ausgewertet werden. T2.2 Sicherheitskonfigurationen und -einstellungen dürfen nur autorisiert aktiviert, geändert, deaktiviert und deinstalliert werden.
T3	Produktive Umgebung Die produktive Umgebung des Informatikschutzobjekts 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.
T4	Schwachstellen und Verwundbarkeiten Das Informatikschutzobjekt 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).
T5	Authentifikation und Autorisation T5.1 Jeder Zugriff auf ein Informatikschutzobjekt muss seinem Schutzbedarf entsprechend authentifiziert[17] und gemäss dem «Least Privilege»- bzw. «Need-to-Know»-Prinzip autorisiert sein. T5.2 Alle Zugriffsrechte auf das Informatikschutzobjekt müssen im Rahmen eines definierten und dokumentierten Prozesses[18] verwaltet und stets aktuell gehalten werden. Insbesondere müssen die Rechte mindestens jährlich in Bezug auf Notwendigkeit und Richtigkeit überprüft und nicht mehr benötigte Rechte (bzw. Konti) entfernt werden.

[17] 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).

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

	T5.3 Für das Informatikschutzobjekt 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.
T6	Benutzerauthentifikation 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 erfolgen[19]. T6.2 Die Benutzerauthentifikation gegenüber einem MDM-System muss auf der Basis der vom jeweiligen Betriebssystem unterstützten Verfahren erfolgen, wie z.B. PIN[20] 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. T6.3 Die Benutzerauthentifikation gegenüber einer Netzwerkkomponente muss auf der Basis eines Authentifikations- und Identitätsnachweismittels mindestens der Sicherheitsstufe «hoch» gemäss Anhang B erfolgen.
T7	Passwörter Für die Benutzerauthentifikation mittels Passwort gelten die folgenden Anforderungen. T7.1* Das Passwort a) muss persönlich[21] sein b) muss einmalig[22] sein c) darf nicht weitergegeben werden d) darf nicht aufgeschrieben bzw. muss geschützt abgelegt oder mit einem Passwort-Verschlüsselungsprogramm verwaltet werden[23] 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 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. T7.2* Ein administrativ gesetztes Initialpasswort muss bei seinem Erstgebrauch geändert werden.

[19] Die Notwendigkeit einer 2-Faktoren-Authentisierung ergibt sich aus dem BRB vom 4. 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.

[20] 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.

[21] Unpersönliche Funktionsaccounts dürfen nur in begründeten Einzelfällen vergeben werden und dürfen nicht für Zugriffe auf Informatikschutzobjekte mit erhöhtem Schutzbedarf verwendet werden.

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

[23] Auf APS ist die Persönliche Passwortverwaltung (Schale 1) einzusetzen.

	T7.3* Wenn das Passwort geändert wird, muss sichergestellt sein, dass das neue Passwort keinem der 10 zuletzt verwendeten Passwörtern entspricht. T7.4* Nach maximal 5 Fehleingaben muss das Passwort gesperrt und darf nur im Rahmen eines definierten Prozesses wieder freigegeben werden. T7.5 Bei Verdacht auf Kenntnisnahme durch Unberechtigte oder Missbrauch muss das Passwort umgehend geändert werden. T7.6* Server-seitig muss sichergestellt sein, dass das Passwort nicht im Klartext ausgelesen oder im Rahmen eines anderen Angriffs leicht kompromittiert werden kann.
T8	Administrative Zugriffe und Fernzugriffe T8.1 Administrative Zugriffe auf das Informatikschutzobjekt müssen auf eine dokumentierte und kontrollierte Art und Weise erfolgen. Insbesondere müssen solche Zugriffe kryptografisch abgesichert sein und nachvollziehbar aufgezeichnet und ausgewertet werden. 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 verfügen[24], müssen einer Schicht in einem Schichtenmodell[25] 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. T8.3 Ein direkter Fernzugriff durch einen externen Anbieter ist zulässig, wenn a) der Inhaber des Objekts einverstanden ist und bezüglich möglicher Amtsgeheimnisverletzungen gemäss den amts- bzw. departementsspezifischen Prozessen eingewilligt hat (vgl. [Si001-Hi03, Si001-Hi04), b) der Zugriff über ein dediziertes Konto erfolgt und die entsprechende Benutzerauthentifikation auf einem Authentifikations- und Identitätsnachweismittel mindestens der Stufe «mittel» gemäss Anhang B basiert, c) die Nutzung dieses Kontos zeitlich begrenzt ist und überwacht wird, d) wenn technisch möglich der Zugriff über einen Jumphost erfolgt, e) die netzwerktechnische Verbindung für den Zugriff kryptografisch abgesichert ist (z. B. mit Hilfe von SSH) und f) die Auditierbarkeit der externalisierten Prozesse jederzeit sichergestellt ist.

[24] Idealerweise werden die Konti im Rahmen einer Privileged Access Management (PAM) Lösung verwaltet und sind nur für die Dauer einer bestimmten Administrationstätigkeit gültig.
[25] Ein solches Schichtenmodell ist z. B. im Rahmen der Architekturrichtlinie AR012 definiert.

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 Weisung vertraglich geregelt ist (z. B. im Rahmen einer Cloud-Lösung).
I2	Vertraulichkeit und Integrität I2.1 Die Vertraulichkeit und Integrität von geschäftsrelevanten Informationen müssen jederzeit ihrem Schutzbedarf entsprechend und unter Berücksichtigung der physischen Gegebenheiten mit Hilfe kryptografischer Verfahren geschützt sein[26] (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. I2.2 Die eingesetzten IT-Systeme müssen geeignet sein, den Schutz der Vertraulichkeit und Integrität der Informationen zu gewähren[27].
I3	Verfügbarkeit I3.1 Die Verfügbarkeit von geschäftsrelevanten Informationen muss jederzeit dem Schutzbedarf entsprechend sichergestellt sein. I3.2 Die für Informationen verantwortliche VE muss über eine Backup-Strategie verfügen[28] 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 sein. Namentlich für die Reparatur und Entsorgung von Datenträgern[29] müssen geeignete Prozesse definiert und umgesetzt sein.

[26] Insbesondere müssen Informationen mit erhöhtem Schutzbedarf, die auf Festplatten von physisch nicht speziell geschützten Server-Systemen gespeichert sind, mit einer Festplattenverschlüsselung geschützt sein.
[27] So ist z.m 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].
[28] 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.
[29] Bei der Entsorgung von Datenträgern ist insbesondere darauf zu achten, dass keine Rückschlüsse auf den Inhalt oder die gespeicherten Daten möglich sind.

IT-Systeme	
S1	Zonenzugehörigkeit Das IT-System muss einer Zone zugehören und gemäss der entsprechenden Zonenpolicy betrieben werden[30].
S2	Updates und Fehlerkorrekturen 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 werden[31], oder das IT-System in einer dedizierten und möglichst stark abgeschotteten Zone betrieben wird (z.B. Technik Zone) und mit Hilfe von komplementären Sicherheitsmassnahmen sichergestellt ist, dass sich für andere Informatikschutzobjekte 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.
S3	Dienstkonti S3.1 Von Systemdiensten benutzte Konti (Dienstkonti) müssen spezifisch[32] und nur mit den für die Diensterbringung minimal erforderlichen Rechten ausgerüstet sein. S3.2* Die Dienstkonti müssen automatisiert verwalten 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.
S4	Integritäts- und Malwareschutz 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 werden[33]. S4.2 Wird ein Integritätsverlust festgestellt, muss das IT-System unmittelbar vom Netzwerk getrennt, gesichert und untersucht werden. Im Falle einer bestätigten Kompromittierung muss das IT-System vollständig gelöscht und neu aufgesetzt werden. S4.3 Das IT-System muss in ein auf [SB003] aufbauendes Malwareschutzkonzept eigebunden sein, das insbesondere auch regelt,

[30] 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.
[31] 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.
[32] Ein Dienstkonto ist spezifisch, wenn es für nur einen Dienst verwendet wird.
[33] Gemäss dem BRB vom 16. Dezember 2009.

	wie bei einem Malwarebefall vorzugehen ist und welche Stellen wie informiert werden müssen.
S5	Bundesclients 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. 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 freigeschalten Bundesclients physisch geschützt sein (z. B. durch Abschliessen des Raumes). S5.3 Auf dem Bundesclient darf keine Autorun-Funktion beim Anschluss externer Datenträger (z. B. USB-Sticks) aktiviert sein. S5.4 Die Benutzerinnen und Benutzer des APS dürfen über keine lokalen Administratorenrechte verfügen. S5.5 Ein administrativer Zugriff zu Supportzwecken auf das APS ist nur mit einer vorgängigen, expliziten Einwilligung der Benutzenden erlaubt.
S6	Peripheriegeräte S6.1 Das Peripheriegerät darf eingesetzt werden, wenn a) es durch eine Beschaffungstelle des Bundes beschafft worden ist und b) seine Integrierbarkeit[34] und grundsätzliche Sicherheit vom LE nachweislich bestätigt worden ist. S6.2 Das Peripheriegerät muss vom LE minimal konfiguriert und vor nicht berechtigten Änderungen (der Konfiguration) geschützt sein. S6.3 Wird das Gerät zum Drucken klassifizierter Dokumente benutzt, muss 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 Empfehlungen[35] überschrieben werden können, wobei die Überschreibung entweder manuell vom Benutzer oder automatisiert ausgelöst werden kann. S6.4 Für die Nutzung von privaten Peripheriegeräten beim Mobilen Arbeiten muss die Einsatzrichtlinie [E026] eingehalten werden.

[34] Die Integrierbarkeit bedeutet z. B. auch, dass das Gerät für Funktionen wie ScanToMail an die Mitarbeiterverzeichnisse der Bundesverwaltung angebunden werden kann.
[35] Z.B. DoD 5220.22-M oder NIST SP 800-88

Anwendungen	
A1	Beschaffung / Entwicklung A1.1 Die Anwendung muss im Rahmen eines methodischen Vorgehens (vorzugsweise nach HERMES[36]) und unter frühzeitiger Berücksichtigung von einschlägigen Sicherheitsvorgaben und -empfehlungen[37] («Best Practices») beschafft bzw. entwickelt werden. A1.2 Bei der Entwicklung der Anwendungssoftware muss insbesondere sichergestellt sein, dass 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	Wartung und Pflege 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).
Zonen	
Z1	Konformität Z1.1 Die Zone muss konform zum Zonenmodell Bund sein und über einen Inhaber, einen eindeutigen Namen[38], eine Zonenpolicy und einen Betreiber[39] 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 netzwerkmässige Erschliessung in der Zonenpolicy beschrieben sein. 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

[36] https://www.hermes.admin.ch
[37] 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.
[38] Die Eindeutigkeit kann z. B. dadurch erreicht werden, dass der Inhaber als Suffix dem Namen angehängt wird (z.B. SZ-BIT für eine vom BIT betriebene Server Zone). Falls ein Inhaber eine Zone mehrfach umsetzen lässt, müssen die entsprechenden Namen unterscheidbar sein.
[39] 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.

	zusätzlichen Bedrohungen und Risiken für andere IT-Systeme und Anwendungen in- und ausserhalb der Zone ausgeht. Z1.3 Die Zone muss in ein Verzeichnis integriert sein, das von oder im Auftrag von der oder dem zuständigen Informationssicherheitsverantwortlichen geführt. Eine Informationssicherheitsverantwortliche der ein Informationssicherheitsverantwortlicher ist zuständig, wenn die VE, für die sie oder er zuständig ist, entweder als Inhaber oder Betreiber der Zone auftritt.
Z2	Zugriffe Z2.1 Ein eingeschränkter[40] 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: 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-System[41]. c) Automatisierte und im Einverständnis mit dem Zoneninhaber durchgeführte Zugriffe im Rahmen von Sicherheitsüberprüfungen von Web-Auftritten (Scans). 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. 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).
Z3	Zonenübergreifende Kommunikation Jede zonenübergreifende Kommunikation muss über eine PEZ erfolgen[42]. Diese hat sicherzustellen, dass die Kommunikation konform zu den betroffenen Zonenpolicies ist. Dazu müssen die erlaubten Kommunikationsmuster und -beziehungen in den Policies so präzis wie möglich (idealerweise auf der

[40] 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.

[41] 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.

[42] 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.

	Anwendungsschicht und in Form einer «Allow List») spezifiziert sein. Ist eine Konformitätsprüfung in einer PEZ nicht möglich (z. B. im Falle End-zu-End 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.
Z4	PEZ 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. 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. Im Einsatzgebiet des IKT-SD Datenkommunikation (DAKO) erfolgt die Regelung im Rahmen von [Si004]. 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.
Z5	Überwachung 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. 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.

5 Inkraftsetzung

[1] Die Weisung tritt am 5. Juli 2024 in Kraft.

[2] Für Informatikschutzobjekte, die vor der Inkraftsetzung dieser Weisung in Betrieb genommen worden sind, gelten die zu diesem Zeitpunkt geltenden Vorgaben.

Abkürzungen

APS	Arbeitsplatzsystem
BA	Büroautomation
BACS	Bundesamt für Cybersicherheit

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
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
ISDS	Informationssicherheits- und Datenschutz
ISG	Informationssicherheitsgesetz
ISO	International Organization for Standardization
IT	Informationstechnik
ITSCM	IT Service Continuity Management
JSON	JavaScript Object Notation
JWT	JSON Web Token
LB	Leistungsbezüger
LE	Leistungserbringer
LoA	Level of Assurance
MDM	Mobile Device Management
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
SSZ	Shared Service Zone
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

[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
[ISG]	Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020
[ISV]	Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) vom 8. November 2023
[SB003]	Malwareschutz Strategie in der Bundesverwaltung, 2021
[Si001-Hi01]	Massnahmenumsetzung zum IKT-Grundschutz 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
[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.

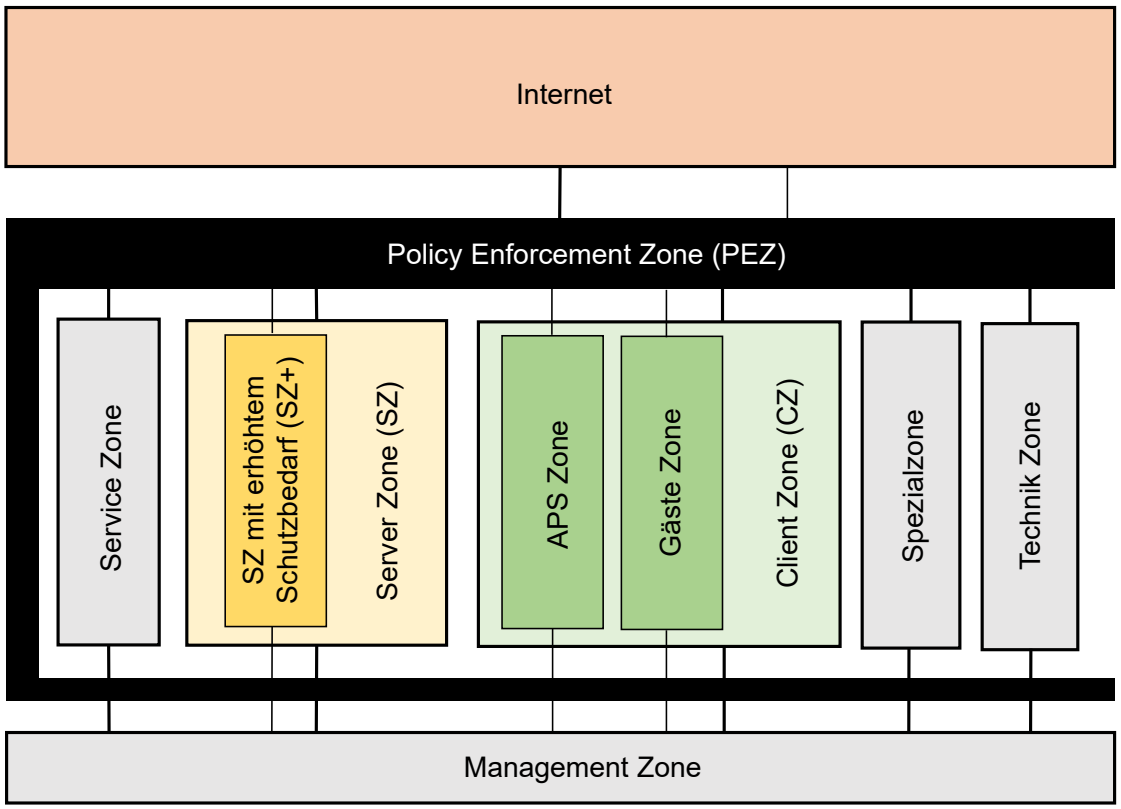


Abbildung A.1: Zonenmodell Bund

Im Zonenmodell Bund werden die folgenden Zonen und Unterzonen unterschieden:

a) **Internet:** Zone, welche keine der Kriterien für die übrigen Zonen entspricht und an welche keine (Sicherheits-) Anforderungen gestellt werden können.
b) **Policy Enforcement Zone (PEZ):** Zone für PEPs, die zur Durchsetzung der Regeln für die externe Kommunikation anderer Zonen erforderlich sind.
c) **Service Zone:** Zone für Server-Systeme, die für die Erbringung von Infrastrukturdiensten erforderlich sind (z. B. DNS- und Zeitserver).
d) **Server Zone (SZ):** Zone für Server-Systeme.
e) **Server Zone mit erhöhtem Schutzbedarf (SZ+):** Unterzone der SZ für Server-Systeme, auf denen insbesondere Anwendungen mit erhöhtem Schutzbedarf gemäss Schutzbedarfsanalyse (Schuban) betrieben werden.
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 Betreibbarkeit 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+) eingeteilt[43]:

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 Identitätstäuschung 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 Identitätstäuschung missbraucht werden. Beispiele sind Username und Passwort mit SMS-Verifikationscode oder Gerätebindung, OTP-Softwarelösungen (z. B. Google Authenticator), FIDO2-Implementierungen (z. B. Passkeys) mit Synchronisations- und Schlüsselexportiermoglichkeiten 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 (z. B. an die «Session») 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-Implementierungen (z. B. Passkeys) ohne Synchronisations- und Schlüsselexportiermoglichkeiten und Swisscom Mobile ID. Wird die Authentifikationsinformation als Föderationstoken eingesetzt, dann muss diese gegen Integritätsangriffe geschützt und auf eine dem Stand der Technik entsprechende Art an den Anwenderkontext (z.B. an die «Session») gebunden sein. Beispiele sind SSO-Identity/SSO-Federation des SSO-Portals, sowie Kerberos-Tickets der User-Forests und im Rahmen von eIAM ausgegebene SAML-Token, wenn diese auf der Basis einer Benutzerauthentifizierung mit einem von der SG-PKI ausgegebenen Klasse-B-Zertifikat ausgestellt worden sind.

[43] 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.

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 ür 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.

Sicherheits-stufe	Beispiele von Authentifikations- und Identitätsnachweismitteln
tief	• Benutzername und Passwort • «Bearer-Token» (z. B. Cookies)
mittel	• Benutzername und Passwort mit SMS-Verifikationscode[44] • Benutzername und Passwort mit Gerätebindung • OTP-Softwarelösung (z.B. Google Authenticator) • FIDO2-Implementierungen (z. B. Passkeys) mit Synchronisations- und Schlüsselexportiermöglichkeiten • 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	• OTP-Token (z.B. RSA, Vasco, …) • OTP-Lösung auf der Basis eines TPM • FIDO2-Implementierungen (z. B. Passkeys) ohne Synchronisations- und Schlüsselexportiermöglichkeiten • Swisscom Mobile ID • SSO-Identity/SSO-Federation des SSO-Portals • Kerberos-Tickets der User-Forests (SG-PKI[45]) • Im Rahmen von eIAM ausgegebene SAML-Token (SG-PKI[45])
hoch+	• 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.

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

[45] Gemäss den Ausführungen im Text müssen sowohl die Kerberos-Tickets als auch die SAML-Token auf der Basis einer Benutzerauthentifizierung mit einem von der SG-PKI ausgegebenen Klasse-B-Zertifikat ausgestellt worden sein.

Anhang C: Zonenpolicy «Netzdomäne blau»

C.1 Anforderungen und Vorgaben an die IKT-Systeme

[1] Die «Netzdomäne blau» und die Shared Service Zone (SSZ) sind aus Gründen der Rückwärtskompatibilität noch verfügbar. Für die SSZ liegt eine Zonenpolicy vor.

[2] Bis die Inhaberschaften der Netzdomäne blau geklärt und entsprechende Vorgaben erlassen sind, gelten sowohl die Zonenpolicy aus Anhang C mit allen Abweichungsbewilligungen (Ausnahmen) und Vereinbarungen[46] als auch die Zugriffsmatrix aus Anhang D.

[3] Ein IKT-System darf in der Netzdomäne blau betrieben werden, wenn es die Anforderungen des Sicherheitsverfahrens gemäss Artikel 16 ISG und Artikel 27 ISV erfüllt.

C.2 Anforderungen und Vorgaben an die Netzdomäne blau

[1] Die Netzdomäne blau kann netzwerkmässig segmentiert sein.

[2] Eine Unterzonierung im Sinne von Kapitel 2 Absatz 2 Buchstabe j) ist möglich.

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

[46] Dabei handelt es sich um eine Vereinbarung mit den Parlamentsdiensten.

durch eine Überprüfung der Nachrichteninhalte[47] 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].

[47] 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[48]	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[49]
	Password or PIN token	n	j[50]	n	n	n	n

Tabelle D.2: Authentifizierung von Partnersystemen und entsprechenden Prozessen

[48] Der einzige Anwendungsfall ist die Administration von Systemen via Admin-LAN (Management Zone LE).
[49] Nur zulässig für den Zugriff auf Sedex und andere Anwendungen, über die nur standardisierte Nachrichten ausgetauscht und/oder definierte Abläufe verfolgt werden können.
[50] Nur zulässig für Telemetriedaten (Messgeräte).