Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee

(Informationssicherheitsverordnung, ISV)

vom … Vorentwurf vom 24. August 2022

Der Schweizerische Bundesrat,

gestützt auf die Artikel 2 Absätze 3 und 4, 12 Absatz 3, 83 Absatz 3, 84 Absatz 1, 85 Absätze 1 und 2 und 86 Absatz 4 des Informationssicherheitsgesetzes vom 18. Dezember 2020[1] (ISG),

verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand
(Art. 1 ISG)

Diese Verordnung regelt die Aufgaben, Verantwortlichkeiten und Kompetenzen sowie die Verfahren zur Gewährleistung der Informationssicherheit bei der Bundesverwaltung und der Armee.

Art. 2 Geltungsbereich
(Art. 2–3 und 84 Abs. 3 ISG)

[1] Diese Verordnung gilt für:

a. den Bundesrat;

b. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[2] (RVOV);

c. die Armee.

[2] Das ISG und die vorliegende Verordnung gelten für Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 7*a* RVOV[3] wie folgt:

1 SR **128**
2 SR **172.010.1**
3 SR **172.010.1**

a. Für Verwaltungseinheiten, die auf Informatikmittel der internen IKT-Leistungserbringer nach Artikel 9 der Verordnung vom 25. November 2020[4] über die digitale Transformation und die Informatik (VDTI) zugreifen, sofern diese der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 zugeordnet sind: das gesamte ISG und die vorliegende Verordnung;

b. Für Verwaltungseinheiten, die Informatikmittel der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 einsetzen: das gesamte ISG und die vorliegende Verordnung;

c. Für Verwaltungseinheiten, die nicht unter Buchstaben a oder b fallen, die aber klassifizierte Informationen des Bundes bearbeiten: die Artikel 9–15 und 27–73 ISG sowie die Bestimmungen des 4. Abschnitts der vorliegenden Verordnung.

3 Die Bundeskanzlei oder die Departemente können beim Bundesrat beantragen, Verwaltungseinheiten der dezentralen Bundesverwaltung, die nicht unter Absatz 2 fallen, dem ISG und der vorliegenden Verordnung oder Teilen davon zu unterstellen.

4 Im Anhang 1 werden aufgeführt:

a. die Verwaltungseinheiten nach Absatz 2;

b. die Verwaltungseinheiten nach Absatz 3 und die jeweilige Geltung des ISG und der vorliegenden Verordnung.

5 Organisationen nach Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[3] (RVOG) sind vom Geltungsbereich des ISG und der vorliegenden Verordnung ausgenommen.

6 Für die Kantone gelten unter Vorbehalt von Artikel 3 Absatz 2 ISG:

a. bei der Bearbeitung von klassifizierten Informationen des Bundes: die Bestimmungen des 4. Abschnitts;

b. beim Zugriff auf Informatikmittel des Bundes: die Artikel 28–30 und 34.

2. Abschnitt: Grundsätze

Art. 3 Sicherheitsziele

(Art. 7 Abs. 2 Bst. a ISG)

1 Die Organisationen nach Artikel 2 sorgen gemeinsam für einen risikobasierten Schutz ihrer Informationen und Informatikmittel sowie für eine angemessene Resilienz gegenüber Informationssicherheitsrisiken.

2 Sie tragen durch die Zusammenarbeit und den Informationsaustausch mit den anderen Bundesbehörden, den Kantonen, den Gemeinden, der Wirtschaft, der Gesellschaft, der Wissenschaft und den internationalen Partnern zur Verbesserung der Informationssicherheit der Schweiz bei.

4 SR **172.010.58**

3 Sie setzen sich für eine nationale und internationale Harmonisierung der Sicherheitsvorschriften und -niveaus ein, um die Interaktion von Bundesbehörden mit anderen Behörden des Bundes sowie der Kantone und der Gemeinden zu ermöglichen.

Art. 4 Verantwortung

1 Die Verwaltungseinheiten sind für den Schutz der Informationen, die sie bearbeiten oder deren Bearbeitung sie in Auftrag geben, sowie die Sicherheit ihrer Informatikmittel, die sie selber betreiben oder durch Dritte betreiben lassen, verantwortlich.

2 Die Verwaltungseinheiten nehmen in ihrem Zuständigkeitsbereich alle Aufgaben wahr, die diese Verordnung oder das Bundesrecht nicht einer anderen Organisation oder Stelle zuweist.

3 Die Mitarbeitenden der Bundesverwaltung sowie die Angehörigen der Armee, die Informationen bearbeiten oder Informatikmittel des Bundes nutzen, sind für die vorschriftskonforme Bearbeitung und Nutzung verantwortlich.

4 Die Vorgesetzten aller Stufen sind für die aufgabenbezogene Schulung ihrer Mitarbeitenden im Bereich der Informationssicherheit sowie für die Überprüfung der Einhaltung der Vorschriften durch diese verantwortlich.

3. Abschnitt: Management der Informationssicherheit

Art. 5 Informationssicherheits-Managementsystem
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten erstellen je ein Informationssicherheits-Managementsystem (ISMS).

2 Sie legen die Ziele für ihr ISMS fest, prüfen jährlich, ob die Ziele erreicht werden, und erheben die dafür nötigen Kennzahlen.

3 Sie lassen ihr ISMS mindestens alle drei Jahre von einer unabhängigen Stelle oder vom Departement überprüfen und sorgen für die kontinuierliche Verbesserung des Systems.

4 Sie koordinieren ihr ISMS mit dem ordentlichen Risikomanagement, dem betrieblichen Kontinuitätsmanagement und dem Krisenmanagement.

Art. 6 Pflege der Rechtsgrundlagen und vertraglichen Verpflichtungen
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten, die Departemente und die Fachstelle des Bundes für Informationssicherheit führen je ein Verzeichnis der in ihrem Zuständigkeitsbereich massgebenden Rechtsgrundlagen und vertraglichen Verpflichtungen zur Informationssicherheit und halten es aktuell.

2 Die Verwaltungseinheiten und die Departemente konsultieren die Fachstelle des Bundes für Informationssicherheit bei sicherheitsrelevanten Vorgaben und Vorhaben.

Art. 7 Inventarisierung der Schutzobjekte
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten führen ein Inventar ihrer Schutzobjekte und halten es aktuell.

2 Als Schutzobjekte gelten:

a. Sammlungen von Informationen, die zur Erfüllung einer Aufgabe des Bundes bearbeitet werden;

b. Informatikmittel nach Artikel 5 Buchstabe a ISG.

3 Das Inventar dient dem Nachweis:

a. des Schutzbedarfs der Schutzobjekte;

b. der Verantwortlichkeiten für die Schutzobjekte;

c. gegebenenfalls der geteilten Nutzung der Schutzobjekte;

d. der Beteiligung von Dritten;

e. des Ergebnisses der Risikobeurteilung;

f. der Umsetzung der Sicherheitsmassnahmen und der Übernahme der Restrisiken;

g. der periodischen Kontrollen und Audits.

Art. 8 Risikomanagement
(Art. 7 Abs. 2 Bst. b und 8 ISG)

1 Die Verwaltungseinheiten beurteilen laufend die Risiken für ihre Schutzobjekte und nehmen dazu insbesondere folgende Aufgaben wahr:

a. Sie analysieren regelmässig Bedrohungen und Schwachstellen und bewerten deren Auswirkungen auf die Schutzobjekte.

b. Sie setzen die notwendigen Massnahmen um und kontrollieren die Wirkung.

c. Sie kontrollieren die Einhaltung der Vorgaben.

d. Sie weisen die die Akzeptanz der Restrisiken nach.

2 Die Fachstelle des Bundes für Informationssicherheit, die leistungserbringenden Verwaltungseinheiten und die Sicherheitsorgane des Bundes informieren die Verwaltungseinheiten und die Departemente über aktuelle Bedrohungen und Schwachstellen sowie über Risiken, die sie betreffen. Sie empfehlen bei Bedarf Massnahmen zur Risikominderung.

3 Die Verwaltungseinheiten berichten über ihre Informationssicherheitsrisiken im Rahmen des ordentlichen Risikomanagementprozesses nach den Vorgaben der Eidgenössischen Finanzverwaltung.

Art. 9 Bewilligung und Verzeichnung von Ausnahmen
(Art. 7 Abs. 1 ISG)

1 Kann eine Verwaltungseinheit für ein Schutzobjekt eine Vorgabe nicht erfüllen, so benötigt sie eine Bewilligung der Stelle, welche die Vorgabe beschlossen hat.

2 Die Fachstelle des Bundes für Informationssicherheit und die Departemente können die Bewilligung von Ausnahmen delegieren.

3 Betrifft eine Ausnahme, die im Kompetenzbereich der Fachstelle des Bundes für Informationssicherheit liegt, auch Vorgaben der Bundeskanzlei über die digitale Transformation und die IKT-Lenkung, so hört die Fachstelle des Bundes für Informationssicherheit vorgängig die DTI-Delegierte oder den DTI-Delegierten nach Artikel 4 Absatz 1 VDTI[5] an.

4 Die Verwaltungseinheiten, die Departemente und die Fachstelle des Bundes für Informationssicherheit führen je ein Verzeichnis der Ausnahmebewilligungen, die:

a. sie selber erteilt haben;

b. für ihre Schutzobjekte erteilt wurden.

Art. 10 Zusammenarbeit mit Dritten
(Art. 9 ISG)

1 Die Verwaltungseinheiten beurteilen nach den Vorgaben von Artikel 8 die Risiken für ihre Schutzobjekte bei der Zusammenarbeit mit Dritten und ihre Abhängigkeit von Dritten.

2 Die Beschaffungsstellen nach den Artikeln 9 und 10 der Verordnung vom 24. Oktober 2012[6] über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB) wirken bei der Beurteilung mit und stellen die nötigen Informationen zur Verfügung.

3 Die Fachstelle des Bundes für Informationssicherheit empfiehlt nach Konsultation der Beschaffungskonferenz des Bundes nach Artikel 24 Org-VöB, welche Bestimmungen zur Informationssicherheit in allen Beschaffungs- und Dienstleistungsverträgen des Bundes enthalten sein sollen.

Art. 11 Schulung und Sensibilisierung
(Art. 7 Abs. 1 und 20 Abs. 1 Bst. c ISG)

1 Die Verwaltungseinheiten schulen ihre Mitarbeitenden bei Stellenantritt und anschliessend periodisch so, dass sie ihre Verantwortung in Bezug auf die Informationssicherheit wahrnehmen können. Sie führen ein Verzeichnis über die Schulungen und die Teilnahme daran.

2 Inhalt der Schulungen sind insbesondere:

a. die korrekte Identifizierung des Schutzbedarfs von Informationen;

5 SR **172.010.58**
6 SR **172.056.15**

b. der sichere Umgang mit Informationen und Informatikmitteln;

c. die korrekte Reaktion bei Verdacht auf einen Sicherheitsvorfall;

d. die Kenntnis der Sicherheitsorganisation sowie der Kontaktpersonen bei Fragen zur Informationssicherheit;

e. die Kontrollaufgaben der Vorgesetzten;

f. die Umsetzung der Informationssicherheit in Projekten und im Betrieb.

3 Die Verwaltungseinheiten, die Departemente und die Fachstelle des Bundes für Informationssicherheit sorgen für die regelmässige Sensibilisierung der Mitarbeitenden aller Stufen in Bezug auf die Risiken der Informationssicherheit.

4 Die Fachstelle des Bundes für Informationssicherheit stellt die Koordination sicher und erstellt Schulungs- und Sensibilisierungshilfsmittel.

Art. 12 Vorfallmanagement
(Art. 7 Abs. 1 und 10 Abs. 1 ISG)

1 Die Verwaltungseinheiten legen in Absprache mit ihren Leistungserbringern fest, wie Sicherheitsvorfälle und Sicherheitslücken gemeldet und bewältigt werden. Sie legen fest, wer über Sofortmassnahmen entscheidet.

2 Die Leistungserbringer melden ihren leistungsbeziehenden Verwaltungseinheiten unverzüglich entdeckte Sicherheitsvorfälle und Sicherheitslücken, die sie betreffen, und unterstützen sie bei der Bewältigung.

3 Die Fachstelle des Bundes für Informationssicherheit kann die Verwaltungseinheiten und die Departemente bei der Bewältigung von Sicherheitsvorfällen und der Behandlung von Sicherheitslücken unterstützen.

4 Die Verwaltungseinheiten prüfen bei der Bewältigung von Sicherheitsvorfällen, ob eine Meldung nach der Datenschutzgesetzgebung an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erfolgen muss.

5 Sie informieren ihr Departement und die Fachstelle des Bundes für Informationssicherheit unverzüglich über den Sicherheitsvorfall oder die Sicherheitslücke, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Die Funktionsfähigkeit der Bundesverwaltung oder der Armee könnte gefährdet sein.

b. Ein Informatikmittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» ist betroffen.

c. Es könnten mehrere Departemente betroffen sein.

d. Der Schutz klassifizierter Informationen eines Staats oder einer internationalen Organisation, mit welchem oder welcher der Bundesrat einen völkerrechtlichen Vertrag nach Artikel 87 ISG abgeschlossen hat, könnte gefährdet sein.

e. Der Sicherheitsvorfall oder die Sicherheitslücke könnte eine hohe politische Bedeutung haben.

f. Der Sicherheitsvorfall oder die Sicherheitslücke erfordert Massnahmen ausserhalb des Verfahrens nach Absatz 1.

6 Die Fachstelle des Bundes für Informationssicherheit beurteilt mit der betroffenen Verwaltungseinheit das Risiko und den Unterstützungsbedarf.

7 Sie kann in Fällen nach Absatz 5 nach Rücksprache mit der betroffenen Verwaltungseinheit und dem betroffenen Departement die Federführung für die Bewältigung eines Sicherheitsvorfalls oder die Behandlung einer Sicherheitslücke übernehmen. Dabei hat sie folgende Aufgaben und Kompetenzen:

a. Sie kann die betroffenen Verwaltungseinheiten, Leistungserbringer und Dritten verpflichten, ihr alle nötigen Informationen mitzuteilen.

b. Sie kann Sofortmassnahmen anordnen.

c. Sie kann externe Spezialistinnen und Spezialisten zur Unterstützung einsetzen.

d. Sie informiert die Leitung der betroffenen Verwaltungseinheiten und der Departemente über den Verlauf.

8 Ist nach einem Sicherheitsvorfall oder einer Sicherheitslücke die Informationssicherheit wiederhergestellt und sind die nötigen Folgearbeiten sowie deren Finanzierung definiert, so übergibt die Fachstelle des Bundes für Informationssicherheit die Federführung für die Weiterbearbeitung wieder der betroffenen Verwaltungseinheit.

Art. 13 Planung von Kontrollen und Audits

(Art. 7 Abs. 1, 81 Abs. 2 Bst. c und 83 Abs. 1 Bst. c ISG)

1 Die Verwaltungseinheiten und die Departemente legen in einem jährlichen Kontroll- und Auditplan fest, wie sie die Einhaltung der Vorschriften nach dieser Verordnung und die Wirksamkeit der Massnahmen zur Gewährleistung der Informationssicherheit in ihrem Zuständigkeitsbereich sowie bei beauftragten Dritten risikobasiert überprüfen.

2 Audits bei Dritten, die über eine Betriebssicherheitserklärung nach Artikel 61 ISG verfügen, müssen mit der Fachstelle Betriebssicherheit nach Artikel 51 Absatz 2 ISG koordiniert werden.

3 Die Fachstelle des Bundes für Informationssicherheit erhebt den Kontroll- und Auditbedarf zur Gewährleistung der Informationssicherheit der gesamten Bundesverwaltung und der Armee und teilt ihn der Eidgenössischen Finanzkontrolle mit.

Art. 14 Berichterstattung

(Art. 7 Abs. 1, 81 Abs. 2 Bst. c und 83 Abs. 1 Bst. h ISG)

1 Die Departemente und die Bundeskanzlei erstatten der Fachstelle des Bundes für Informationssicherheit jährlich Bericht über den Stand der Informationssicherheit in ihrem Zuständigkeitsbereich.

2 Sie erheben bei den Verwaltungseinheiten und ihren Leistungserbringern die dafür nötigen Informationen.

3 Die Fachstelle des Bundes für Informationssicherheit erstattet dem Bundesrat jährlich Bericht über den Stand der Informationssicherheit beim Bund.

4 Sie legt die Modalitäten der Berichterstattung der internen Leistungserbringer nach Artikel 9 VDTI[7] fest.

5 Sie koordiniert die Berichterstattung mit den verpflichteten Behörden nach Artikel 2 Absatz 1 ISG.

Art. 15 Vorgaben zum Management der Informationssicherheit
(Art. 85 ISG)

Die Fachstelle des Bundes für Informationssicherheit erlässt generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die minimalen Anforderungen an das Management der Informationssicherheit nach den Artikeln 5–14.

4. Abschnitt: Klassifizierte Informationen

Art. 16 Grundsätze
(Art. 11 ISG)

1 Die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen sowie die Erstellung klassifizierter Informationsträger sind auf das Minimum zu beschränken.

2 Werden Informationen zu einem Sammelwerk zusammengefasst, ist zu prüfen, ob dieses klassifiziert oder einer höheren Klassifizierungsstufe zugeordnet werden muss.

3 Bei Gesuchen um Zugang zu amtlichen Dokumenten überprüft die zuständige Stelle unabhängig von einem allfälligen Klassifizierungsvermerk, ob der Zugang nach dem Öffentlichkeitsgesetz vom 17. Dezember 2004[8] zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist.

Art. 17 Klassifizierende Stellen
(Art. 12 ISG)

1 Folgende Personen und Stellen sind für die Klassifizierung und Entklassifizierung von Informationen zuständig:

a. die Mitarbeitenden des Bundes sowie die Angehörigen der Armee: für Informationsträger, die sie erstellen oder erstellen lassen, und für Informationen, die sie mündlich mitteilen;

b. die Mitarbeitenden von Betrieben mit einer gültigen Betriebssicherheitserklärung nach Artikel 61 ISG: für Informationsträger, die sie im Auftrag des Bundes erstellen;

7 SR **172.010.58**
8 SR **152.3**

c. die für die Aufgabe verantwortliche Person: für Schutzobjekte nach Artikel 7 Absatz 2 Buchstabe a.

2 Die Verwaltungseinheiten, die Bundeskanzlei und die Departemente legen in einem Klassifizierungskatalog fest, wie Informationen, die in ihrem Zuständigkeitsbereich häufig bearbeitet werden, zu klassifizieren sind.

3 Die Fachstelle des Bundes für Informationssicherheit überprüft die Klassifizierungskataloge nach Absatz 2 und gibt bei Bedarf eine Empfehlung ab.

4 Sie legt nach der Konsultation der Konferenz der Informationssicherheitsbeauftragten fest, wie Informationen, die in der Bundesverwaltung und in der Armee häufig bearbeitet werden, zu klassifizieren sind.

Art. 18 Klassifizierungsstufe «intern»
(Art. 13 Abs. 1 ISG)

Als «intern» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d ISG wie folgt beeinträchtigen kann:

a. Ein wichtiger Geschäftsprozess des Bundesrats oder der Bundesverwaltung oder ein wichtiger Führungsprozess der Armee ist erschwert.

b. Die Durchführung von Einsätzen der Strafverfolgungsbehörden, des Nachrichtendiensts des Bundes (NDB), der Armee oder der anderen Sicherheitsorgane des Bundes ist erschwert.

c. Einzelne Personen sind körperlich verletzt.

d. Die nukleare Sicherheit oder die Sicherung von Kernanlagen und Kernmaterialien ist mittelbar gefährdet.

e. Die Schweiz ist aussenpolitisch oder wirtschaftlich benachteiligt.

f. Die Beziehungen zwischen Bund und Kantonen oder zwischen den Kantonen sind über Monate gestört.

Art. 19 Klassifizierungsstufe «vertraulich»
(Art. 13 Abs. 2 ISG)

Als «vertraulich» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d ISG wie folgt erheblich beeinträchtigen kann:

a. Die Entscheidungs- oder Handlungsfähigkeit des Bundesrats, des Parlaments, mehrerer Verwaltungseinheiten oder mehrerer Truppenkörper der Armee ist über mehrere Tage erschwert.

b. Die zielkonforme Durchführung von Operationen der Strafverfolgungsbehörden, des NDB, der Armee oder der anderen Sicherheitsorgane des Bundes ist gefährdet.

c. Die operativen Mittel und Methoden der Nachrichtendienste und Strafverfolgungsbehörden des Bundes oder die Identität von Quellen und exponierten Personen sind offengelegt.

d. Die Sicherheit der Bevölkerung ist über mehrere Tage gefährdet oder einzelne Personen oder Personengruppen kommen zu Tode.

e. Die nukleare Sicherheit oder die Sicherung von Kernanlagen und Kernmaterialien ist gefährdet.

f. Die wirtschaftliche Landesversorgung oder der Betrieb von kritischen Infrastrukturen ist erschwert.

g. Die Schweiz ist aussenpolitisch oder wirtschaftlich erheblich benachteiligt oder die diplomatischen Beziehungen zu einem Staat oder zu einer internationalen Organisation sind abgebrochen.

h. Die Verhandlungsposition der Schweiz in wichtigen aussenpolitischen Geschäften ist vorübergehend erheblich geschwächt.

Art. 20 Klassifizierungsstufe «geheim»
(Art. 13 Abs. 3 ISG)

Als «geheim» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d ISG wie folgt schwerwiegend beeinträchtigen kann:

a. Der Bundesrat, das Parlament, mehrere Verwaltungseinheiten oder mehrere Truppenkörper der Armee sind über Tage entscheidungs- oder handlungsunfähig oder deren Entscheidungs- oder Handlungsfähigkeit ist über Wochen erschwert.

b. Die Durchführung von strategisch bedeutsamen Operationen der Strafverfolgungsbehörden, des NDB, der Armee oder der anderen Sicherheitsorgane des Bundes ist gefährdet oder über Tage in besonders hohem Mass erschwert.

c. Strategische Quellen, die Identität besonders exponierter Personen oder die strategischen Mittel und Methoden der Nachrichtendienste und Strafverfolgungsbehörden des Bundes sind offengelegt.

d. Die Sicherheit der Bevölkerung ist über Wochen in besonders hohem Mass gefährdet oder eine grosse Anzahl Personen kommt zu Tode.

e. Die nukleare Sicherheit oder die Sicherung von Kernanlagen und Kernmaterialien ist in besonders hohem Mass gefährdet.

f. Die wirtschaftliche Landesversorgung oder der Betrieb von kritischen Infrastrukturen fallen über Tage aus.

g. Die Schweiz leidet über Wochen unter besonders hohen aussenpolitischen oder wirtschaftlichen Konsequenzen wie Embargomassnahmen oder Sanktionen.

h. Die Verhandlungsposition der Schweiz in strategischen aussenpolitischen Geschäften ist über Jahre geschwächt.

Art. 21 Bearbeitungsvorgaben
(Art. 6 Abs. 2, 84 Abs. 1 und 85 ISG)

1 Die Fachstelle des Bundes für Informationssicherheit erlässt generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die Bearbeitung klassifizierter Informationen und die organisatorischen, personellen, technischen und baulichen Anforderungen für deren Schutz.

2 Sie hört vorgängig die folgenden Stellen an:

a. den kryptografischen Dienst der Armee;

b. die für die Beschaffung von kryptologischen Gütern zuständigen Stellen nach Artikel 10 Absatz 1 Buchstabe d Org-VöB[9]; und

c. die für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee.

3 Sie trägt den einschlägigen internationalen Standards Rechnung.

4 Die Bundeskanzlei regelt die Bearbeitung klassifizierter Bundesratsgeschäfte.

5 Die Bearbeitung klassifizierter Informationen aus dem Ausland erfolgt nach den Vorschriften, die der ausländischen Klassifizierungsstufe entsprechen. Vorbehalten bleiben abweichende Vorschriften eines völkerrechtlichen Vertrags nach Artikel 87 ISG.

Art. 22 Einsatzbezogene Sicherheitsmassnahmen
(Art. 6 Abs. 2 und 85 ISG)

1 Werden klassifizierte Informationen im Rahmen eines Einsatzes oder einer Operation bearbeitet und sind diese nur einem geschlossenen, eindeutig bestimmbaren Benutzerkreis zugänglich, so können die folgenden Personen nach Konsultation der Fachstelle des Bundes für Informationssicherheit einsatz- oder operationsspezifisch Vorschriften zur vereinfachten Bearbeitung beschliessen:

a. die Direktorin oder der Direktor des Bundesamts für Polizei;

b. die Direktorin oder der Direktor des NDB;

c. die Chefin oder der Chef der Armee;

d. die Chefin oder der Chef des Kommandos Operationen;

e. die Direktorin oder der Direktor des Bundesamts für Zoll und Grenzsicherheit.

2 Die Stellen nach Absatz 1 sorgen dafür, dass eindeutig erkennbar ist, ob Vorschriften zur vereinfachten Bearbeitung gelten.

3 Ausserhalb des Benutzerkreises sowie für die Aufbewahrung im Hinblick auf die Archivierung gelten die Bearbeitungsvorgaben nach Artikel 21.

9 SR **172.056.15**

Art. 23 Sicherheitsakkreditierung von Informatikmitteln
(83 Abs. 1 Bst. e ISG)

1 Informatikmittel müssen vor der Inbetriebnahme sicherheitsmässig akkreditiert werden, wenn eine der folgenden Voraussetzung erfüllt ist:

a. Sie werden für amtsübergreifende Aufgaben eingesetzt, bei denen als «geheim» klassifizierte Informationen bearbeitet werden.

b. Sie werden für behörden- oder departementsübergreifende Aufgaben eingesetzt, bei denen als «vertraulich» klassifizierte Informationen bearbeitet werden.

c. Die Sicherheitsakkreditierung ist für die nationale oder internationale Zusammenarbeit erforderlich.

2 Die Sicherheitsakkreditierung belegt, dass das Informatikmittel die minimalen Sicherheitsanforderungen für die entsprechende Klassifizierungsstufe erfüllt und die Restrisiken nach dem Stand der Technik tragbar sind.

3 Sie wird bei wesentlichen Änderungen der Risiken oder bei wesentlichen Änderungen am Informatikmittel wiederholt.

4 Kann die Sicherheitsakkreditierung nicht erteilt werden, weil das Informatikmittel die minimalen Sicherheitsanforderungen nicht erfüllt, so entscheidet der Bundesrat über die Restrisiken.

5 Die Fachstelle des Bundes für Informationssicherheit nimmt folgende Aufgaben wahr:

a. Sie erteilt die Sicherheitsakkreditierung nach Konsultation des kryptografischen Diensts der Armee sowie der Stellen nach Artikel 10 Absatz 1 Buchstabe d Org-VöB[10].

b. Sie kann die Kompetenz zur Sicherheitsakkreditierung ausschliesslich militärischer Systeme der Gruppe Verteidigung delegieren.

6 Das [zuständige Departement] legt das Verfahren der Sicherheitsakkreditierung fest und berücksichtigt dabei die einschlägigen internationalen Standards.

Art. 24 Schutz bei der Gefährdung von klassifizierten Informationen
(Art. 10 Abs. 1 und 11 Abs. 1 ISG)

1 Wer feststellt, dass klassifizierte Informationen gefährdet, abhandengekommen oder missbräuchlich verwendet worden sind oder Informationen offensichtlich falsch oder fälschlicherweise nicht klassifiziert sind, muss die nötigen Schutzmassnahmen treffen.

2 Sie oder er benachrichtigt unverzüglich die klassifizierende Stelle und die zuständigen Sicherheitsorgane.

10 SR **172.056.15**

Art. 25 Überprüfung von Schutzbedarf und Kreis der Berechtigten
(Art. 11 Abs. 2 ISG)

Die klassifizierenden Stellen überprüfen den Schutzbedarf ihrer klassifizierten Informationen und den Kreis der Berechtigten mindestens alle fünf Jahre sowie immer, wenn die Informationen dem Bundesarchiv zur Archivierung angeboten werden.

Art. 26 Archivierung
(Art. 12 Abs. 3 ISG)

[1] Die Archivierung klassifizierter Informationen richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

[2] Das Bundesarchiv sorgt dafür, dass die Informationssicherheit nach dieser Verordnung gewährleistet ist.

[3] Die Klassifizierung von Archivgut entfällt mit Ablauf der Schutzfrist. Eine Verlängerung der Schutzfrist richtet sich nach Artikel 14 der Archivierungsverordnung vom 8. September 1999[11].

5. Abschnitt: Sicherheit beim Einsatz von Informatikmitteln

Art. 27 Sicherheitsverfahren
(Art. 16 ISG)

[1] Die Verwaltungseinheiten müssen den Schutzbedarf ihrer Schutzobjekte und deren Relevanz für das betriebliche Kontinuitätsmanagement nachweisen können.

[2] Sie setzen die Mindestvorgaben der jeweiligen Sicherheitsstufe um und prüfen, ob zusätzliche Sicherheitsmassnahmen erforderlich sind.

[3] Sie weisen Risiken, die nicht hinreichend reduziert werden können (Restrisiken), aus.

[4] Die Sicherheitsverantwortlichen nach Artikel 36 entscheiden, ob Restrisiken getragen werden. Sie können diesen Entscheid anderen Mitgliedern der Geschäftsleitung delegieren.

[5] Das Sicherheitsverfahren wird bei wesentlichen Änderungen der Bedrohung, der Technologie, der Aufgaben oder der Organisationsverhältnisse wiederholt.

[6] Die Verwaltungseinheiten prüfen jährlich, ob eine wesentliche Änderung nach Absatz 5 stattgefunden hat.

11 SR **152.11**

Art. 28 Zuordnung zu den Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz»
(Art. 17 ISG)

[1]Die Sicherheitsstufe «hoher Schutz» wird einem Informatikmittel zugeordnet, wenn eine Verletzung der Informationssicherheit eine Beeinträchtigung nach Artikel 19 oder einen Schaden von fünfzig bis fünfhundert Millionen Franken zur Folge haben kann.

[2] Die Sicherheitsstufe «sehr hoher Schutz» wird einem Informatikmittel zugeordnet, wenn eine Verletzung der Informationssicherheit eine Beeinträchtigung nach Artikel 20 oder einen Schaden von mindestens fünfhundert Millionen Franken zur Folge haben kann.

Art. 29 Sicherheitsmassnahmen
(Art. 6 Abs. 3, 18 und 85 ISG)

[1] Die Fachstelle des Bundes für Informationssicherheit erlässt generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die Mindestanforderungen für die jeweiligen Sicherheitsstufen nach Artikel 17 ISG.

[2] Sie berücksichtigt dabei die Anforderungen für die Sicherheit von Personendaten nach der Datenschutzgesetzgebung sowie von anderen Informationen, die der Bund aufgrund gesetzlicher oder vertraglicher Verpflichtungen schützen muss.

[3] Bei den folgenden Informatikmitteln muss die Wirksamkeit der Sicherheitsmassnahmen vor der Inbetriebnahme, bei wesentlichen Änderungen der Risiken während des Betriebs, mindestens aber alle fünf Jahre überprüft werden:

a. Informatikmittel der Sicherheitsstufe «hoher Schutz», die für die Erfüllung behörden- oder departementsübergreifender Aufgaben eingesetzt werden;

b. Informatikmittel der Sicherheitsstufe «sehr hoher Schutz».

[4] Die Departemente und die Bundeskanzlei nehmen ihre Informatikmittel der Sicherheitsstufe «sehr hoher Schutz» in ihr Kontinuitätsmanagement auf.

Art. 30 Sicherheit beim Betrieb
(Art. 19 ISG)

[1] Die Verwaltungseinheiten stellen sicher, dass die Verantwortlichkeiten für die Informationssicherheit auf der betrieblichen Ebene in den Projekt- und Leistungsvereinbarungen mit den internen Leistungserbringern festgehalten sind.

[2] Die internen Leistungserbringer stellen den Verwaltungseinheiten, der Bundeskanzlei, den Departementen und der Fachstelle des Bundes für Informationssicherheit die Informationen zur Verfügung, welche diese für die Gewährleistung der Informationssicherheit benötigen.

[3] Sie stellen sicher, dass sie über die nötigen personellen und finanziellen Kapazitäten und Fähigkeiten zur frühzeitigen Entdeckung, zur technischen Analyse und zur Bewältigung von Sicherheitsvorfällen und Behandlung von Sicherheitslücken verfügen,

die sie selber oder, im Rahmen der Vereinbarungen nach Absatz 2, ihre Leistungsbezüger betreffen.

4 Sie überwachen die Nutzung ihrer Informatikinfrastruktur und durchsuchen sie regelmässig nach technischen Bedrohungen und Schwachstellen. Sie können Dritte mit der Durchsuchung beauftragen.

5 Die Bearbeitung von Personendaten im Rahmen der Überwachung und Durchsuchung nach Absatz 4 richtet sich nach der Verordnung vom 22. Februar 2012[12] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen.

6. Abschnitt: Personelle Massnahmen und physischer Schutz

Art. 31 Prüfung der Identität von Personen und Maschinen

(Art. 20 und 85 ISG)

1 Die Fachstelle des Bundes für Informationssicherheit erlässt nach Konsultation der oder des DTI-Delegierten generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die minimalen technischen Anforderungen an die risikobasierte Prüfung der Identität von Personen und Maschinen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes benötigen.

2 Die Bearbeitung von Personendaten bei der Prüfung der Identität in Identitätsverwaltungs-Systemen nach Artikel 24 ISG richtet sich nach den Bestimmungen der Verordnung vom 19. Oktober 2016[13] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes.

Art. 32 Personensicherheit

(Art. 6 Abs. 2 und 3, 8 und 20 Abs. 1 Bst. a und c ISG)

1 Die Verwaltungseinheiten stellen sicher, dass Mitarbeitende, die einer Personensicherheitsprüfung nach der Verordnung vom …[14] über die Personensicherheitsprüfungen (VPSP) unterliegen, jährlich für die massgebende sicherheitsempfindliche Tätigkeit und die entsprechenden Risiken sensibilisiert werden.

2 Mitarbeitende nach Absatz 1 sind verpflichtet, ihrem Arbeitgeber Umstände aus ihrem privaten und beruflichen Umfeld, welche die vorschriftskonforme Ausübung der sicherheitsempfindlichen Tätigkeit gefährden, zu melden.

12 SR **172.010.442**
13 SR **172.010.59**
14 SR **128.xxx**

Art. 33 Verdacht auf strafbares Verhalten
(Art. 7 Abs. 2 Bst. c ISG)

[1] Kommt bei der Verletzung von Informationssicherheitsvorschriften zugleich eine strafbare Handlung in Betracht, überweisen die Departemente die Akten mit den Einvernahmeprotokollen der Bundesanwaltschaft oder dem Oberauditor der Schweizer Armee.

[2] Sie stellen Gegenstände sicher, die geeignet sind, in einem Verfahren als Beweismittel zu dienen.

Art. 34 Physische Schutzmassnahmen
(Art. 22 und 85 ISG)

[1] Die Fachstelle des Bundes für Informationssicherheit erlässt nach Konsultation der für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die minimal erforderlichen Massnahmen zum physischen Schutz von Informationen und Informatikmitteln.

[2] Sie berücksichtigt dabei:

a. den gesamten Lebenszyklus der Informationen und Informatikmittel;

b. die arbeitsplatzspezifischen Anforderungen; und

c. die Unterbringungsstrategien und -konzepte der Bundesverwaltung und der Armee.

Art. 35 Sicherheitszonen
(Art. 23 und 85 ISG)

[1] Die Verwaltungseinheiten können folgende Sicherheitszonen einrichten:

a. Sicherheitszone 1: Räumlichkeiten und Bereiche, in denen häufig als «vertraulich» klassifizierte Informationen bearbeitet oder Informatikmittel der Sicherheitsstufe «hoher Schutz» betrieben werden;

b. Sicherheitszone 2: Räumlichkeiten und Bereiche, in denen häufig als «geheim» klassifizierte Informationen bearbeitet oder Informatikmittel der Sicherheitsstufe «sehr hoher Schutz» betrieben werden.

[2] Die Räumlichkeiten und Bereiche nach Absatz 1 gelten nur als Sicherheitszone, wenn die für die Objektsicherheit zuständige Stelle der Bundesverwaltung oder der Armee vor deren Inbetriebnahme und anschliessend mindestens alle fünf Jahre bestätigt, dass die Sicherheitsanforderungen erfüllt sind.

[3] Die Fachstelle des Bundes für Informationssicherheit erlässt nach Konsultation der für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die Sicherheitsanforderungen für die Sicherheitszonen und deren Einrichtung.

7. Abschnitt: Sicherheitsorganisation

Art. 36 Sicherheitsverantwortliche der Bundeskanzlei und der Verwaltungseinheiten
(Art. 7 Abs. 1 ISG)

1 Die Bundeskanzlerin oder der Bundeskanzler, die Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten der zentralen und dezentralen Bundesverwaltung tragen in ihrem Zuständigkeitsbereich die Sicherheitsverantwortung.

2 Sie können die Sicherheitsverantwortung einem Mitglied der Geschäftsleitung delegieren, sofern diesem die erforderlichen Befugnisse zustehen, Massnahmen zu veranlassen, zu kontrollieren und zu korrigieren.

3 Die Sicherheitsverantwortlichen der Bundeskanzlei und der Verwaltungseinheiten nehmen insbesondere folgende Aufgaben wahr:

a. Sie stellen den Aufbau, den Betrieb, die Überprüfung und die kontinuierliche Verbesserung des ISMS in ihrem Zuständigkeitsbereich sicher und erlassen die dafür nötigen Vorgaben.

b. Sie treffen alle Entscheide, welche die Informationssicherheit in ihrem Zuständigkeitsbereich massgeblich beeinflussen, insbesondere betreffend Organisation, Prozesse, Risikoakzeptanz und Sicherheitsziele.

c. Sie entscheiden über die erforderlichen Massnahmen, insbesondere über die Durchführung von Schulungs- und Sensibilisierungsmassnahmen.

d. Sie genehmigen den jährlichen Kontroll- und Auditplan und stellen die dafür nötigen Ressourcen zur Verfügung.

4 Die Bundeskanzlerin oder der Bundeskanzler, Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten der zentralen und dezentralen Bundesverwaltung beauftragen ihre Informationssicherheitsbeauftragten nach Artikel 37 und sorgen dafür, dass:

a. sie über angemessene Kompetenzen und Ressourcen verfügen; und

b. ihnen keine Aufgaben übertragen werden, die einen Interessenkonflikt mit den Aufgaben nach Artikel 37 zu Folgen haben können.

Art. 37 Informationssicherheitsbeauftragte der Verwaltungseinheiten
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten bezeichnen eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten oder mehrere Informationssicherheitsbeauftragte sowie deren oder dessen Stellvertretung.

2 Die Informationssicherheitsbeauftragten haben insbesondere folgende Aufgaben:

a. Sie betreiben das ISMS der Verwaltungseinheit im Auftrag der oder des Sicherheitsverantwortlichen.

b. Sie erarbeiten die nötigen Entscheidgrundlagen zuhanden der oder des Sicherheitsverantwortlichen und beantragen ihr oder ihm den Beschluss von Massnahmen.

c. Sie sind die zentrale Anlaufstelle der Verwaltungseinheit für Fragen zur Informationssicherheit und beraten und unterstützen die zuständigen Personen und Stellen bei der Erfüllung ihrer Aufgaben und Pflichten im Bereich der Informationssicherheit.

d. Sie sorgen für die Umsetzung der Informationssicherheitsvorgaben und für die Anwendung des Sicherheitsverfahrens nach Artikel 27.

e. Sie beaufsichtigen das Verzeichnis der Rechtsgrundlagen, das Inventar der Schutzobjekte und das Verzeichnis der Ausnahmebewilligungen.

f. Sie beaufsichtigen die Planung der Schulung und Sensibilisierung nach Artikel 11 und beantragen der oder dem Sicherheitsverantwortlichen die Durchführung von zusätzlichen Schulungs- und Sensibilisierungsmassnahmen.

g. Sie stellen Antrag auf Einleitung des Betriebssicherheitsverfahrens nach Artikel 4 der Verordnung über das Betriebssicherheitsverfahren vom …[15].

h. Sie koordinieren die Meldung und Bewältigung von Sicherheitsvorfällen und Behandlung von Sicherheitslücken in der Verwaltungseinheit sowie bei beauftragten Dritten.

i. Sie erstellen den jährlichen Kontroll- und Auditplan und unterbreiten ihn der oder dem Sicherheitsverantwortlichen zur Genehmigung.

j. Sie können im Auftrag der oder des Sicherheitsverantwortlichen den Umgang mit Informationen an offenen, geteilten oder nicht abschliessbaren Arbeitsplätzen und in den Informatikmitteln der Verwaltungseinheit kontrollieren oder kontrollieren lassen.

k. Sie berichten der oder dem Sicherheitsverantwortlichen halbjährlich über den Stand der Informationssicherheit.

Art. 38 Informationssicherheit bei den Standarddiensten
(Art. 7 Abs. 1 ISG)

[1] Die oder der DTI-Delegierte ist für die Gewährleistung der Informationssicherheit bei den Standarddiensten nach Artikel 17 Absatz 1 Buchstabe e VDTI[16] zuständig.

[2] Sie oder er bezeichnet eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten oder mehrere Informationssicherheitsbeauftragte sowie deren oder dessen Stellvertretung.

[3] Die oder der Informationssicherheitsbeauftragte nimmt für die Standarddienste die Aufgaben nach Artikel 37 Absatz 2 wahr und informiert die Bundesverwaltung und die Armee über die Risiken.

15 SR **128.xxx**
16 SR **172.010.58**

Art. 39 Sicherheitsverantwortung der Departemente
(Art. 7 Abs. 1 und 81 ISG)

[1] Die Departemente sind für die Steuerung und Überwachung der Informationssicherheit in ihrem Zuständigkeitsbereich verantwortlich.

[2] Sie haben dabei insbesondere folgende Aufgaben:

a. Sie bestimmen die Informationssicherheitspolitik und die Sicherheitsorganisation des Departements, einschliesslich der fachlichen Führung der Informationssicherheitsbeauftragten der Verwaltungseinheiten.

b. Sie erlassen die nötigen Weisungen und überwachen die Umsetzung.

c. Sie überwachen die ISMS der Verwaltungseinheiten und erheben die dafür nötigen Kennzahlen.

d. Sie legen jährlich die Sicherheitsziele für die Verwaltungseinheiten fest und überprüfen, ob sie erreicht wurden.

e. Sie sorgen für eine risikobasierte Überprüfung der Informationssicherheit.

f. Sie beauftragen ihre Informationssicherheitsbeauftragten nach Artikel 40 und sorgen dafür, dass:

   1. sie über angemessene Kompetenzen und Ressourcen verfügen;

   2. ihnen keine Aufgaben übertragen werden, die einen Interessenkonflikt mit ihren Aufgaben nach Artikel 40 zur Folge haben können.

[3] Sie können Aufgaben und Kompetenzen, welche diese Verordnung den Verwaltungseinheiten zuweist, übernehmen.

[4] Sie können für ihren Zuständigkeitsbereich Sicherheitsanforderungen festlegen, die über die Mindestanforderungen der Fachstelle des Bundes für Informationssicherheit oder der Verwaltungseinheit hinausgehen.

[5] Sofern die Departementsvorsteherin oder der Departementsvorsteher nicht anders entscheidet, ist die Generalsekretärin oder der Generalsekretär in deren oder dessen Auftrag für die Sicherheit im Departement verantwortlich.

Art. 40 Informationssicherheitsbeauftragte der Departemente
(Art. 7 Abs. 1 und 81 ISG)

Die Informationssicherheitsbeauftragten der Departemente haben zusätzlich zu den Aufgaben nach Artikel 81 Absatz 2 ISG folgende Aufgaben:

a. Sie sorgen für die departementsübergreifende Koordination der Informationssicherheit.

b. Sie erarbeiten die nötigen Entscheidgrundlagen zuhanden der oder des Sicherheitsverantwortlichen und beantragen ihr oder ihm den Beschluss von Massnahmen.

c. Sie koordinieren die Meldung und Bewältigung von Sicherheitsvorfällen und die Behandlung von Sicherheitslücken, welche mehrere Verwaltungseinheiten betreffen.

d. Sie vertreten das Departement in Fachgremien.

e. Sie werden bei der Wahl der Informationssicherheitsbeauftragten der Verwaltungseinheiten nach Artikel 37 konsultiert.

f. Sie kontrollieren periodisch sowie beim Wechsel oder beim Abgang eines Mitglieds des Bundesrats oder der Bundeskanzlerin oder des Bundeskanzlers, ob alle als «geheim» klassifizierten Informationsträger vollständig vorhanden sind.

g. Sie bewilligen die Einleitung von Personensicherheitsprüfungen bei Dritten (Art. 8 Abs. 2 Bst. b VPSP[17]).

h. Sie berichten der oder dem Sicherheitsverantwortlichen des Departements jährlich über den Stand der Informationssicherheit im Departement.

Art. 41 Fachstelle des Bundes für Informationssicherheit
(Art. 7 Abs. 1 und 83 ISG)

1 Die Fachstelle des Bundes für Informationssicherheit hat für die Bundesverwaltung und die Armee folgende Aufgaben:

a. Sie erarbeitet Strategien zu sicherheitsrelevanten Themen.

b. Sie kann bei sicherheitsrelevanten Vorhaben Informationen verlangen, dazu Stellung nehmen und Änderungen verlangen.

c. Sie wirkt bei der Ausbildung der Sicherheitsorganisation mit.

d. Sie stellt Vorlagen und Hilfsmittel bereit.

2 Sie kann zur Beurteilung und Verbesserung des Stands der Informationssicherheit des Bundes in der Informatikinfrastruktur der Bundesverwaltung und der Armee oder im Internet nach technischen Bedrohungen und Schwachstellen suchen; sie kann andere Stellen der Bundesverwaltung oder der Armee sowie Dritte damit beauftragen.

3 Sie konsultiert bei der Erfüllung der Aufgaben nach Absatz 1 sowie nach Artikel 83 Absatz 1 ISG die Konferenz der Informationssicherheitsbeauftragten.

4 Sie vertritt im internationalen Verhältnis als nationale Sicherheitsbehörde die Schweiz und nimmt dabei folgende Aufgaben wahr:

a. Sie erarbeitet die völkerrechtlichen Verträge nach Artikel 87 ISG und überwacht deren Umsetzung.

b. Sie stellt sicher, dass Sicherheitsvorfälle, die klassifizierte Informationen von Partnerstaaten betreffen, sachgerecht abgeklärt werden.

c. Sie kann die in den völkerrechtlichen Verträgen vorgesehenen Kontrollen durchführen oder diese in Auftrag geben.

d. Sie vertritt die Schweiz in internationalen Fachgremien.

17 SR **128.xxx**

e. Sie bewilligt den Empfang von Personen aus dem Ausland, die für klassifizierte Projekte in die Schweiz reisen, sowie die Entsendung von Personen, die für klassifizierte Projekte ins Ausland reisen.

f. Sie stellt die Bescheinigungen im internationalen Verhältnis nach Artikel 30 VPSP[18] aus.

5 Die Fachstelle des Bundes für Informationssicherheit ist dem *[zuständigen Departement]* zugeordnet.

8. Abschnitt: Kosten und Evaluation

Art. 42 Kosten

1 Die dezentral anfallenden Kosten für die Informationssicherheit sind Teil der Projekt- und Betriebskosten.

2 Die Verwaltungseinheiten stellen sicher, dass diese Kosten bei der Planung hinreichend berücksichtigt und ausgewiesen werden.

3 Für die Ausstellung und Zustellung von Sicherheitsbescheinigungen im internationalen Verhältnis nach Artikel 30 VPSP[19] für Personen, die keine sicherheitsempfindliche Tätigkeit des Bundes erfüllen, erhebt die Fachstelle des Bundes für Informationssicherheit eine Gebühr von 100 Franken.

Art. 43 Evaluation
(Art. 88 ISG)

Die Fachstelle des Bundes für Informationssicherheit beantragt der Eidgenössischen Finanzkontrolle sechs Jahre nach Inkrafttreten dieser Verordnung und anschliessend alle zehn Jahre die Evaluation der Gesetzgebung über die Informationssicherheit beim Bund.

9. Abschnitt: Bearbeitung von Informationen und Personendaten

Art. 44 Allgemeines

1 Die Organisationen nach Artikel 2 Absätze 1–3 sowie die Sicherheitsorgane des Bundes können die für die Gewährleistung der Informationssicherheit zweckmässigen Informationen einschliesslich Personendaten bearbeiten.

2 Sie können untereinander sowie mit nationalen, internationalen und ausländischen Organisationen des öffentlichen und privaten Rechts Informationen einschliesslich Personendaten nach Absatz 1 austauschen, sofern:

a. keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden; und

18 SR ...
19 SR **128.xxx**

b. die Vorgaben der Bundesgesetzgebung über den Datenschutz eingehalten werden.

3 Sofern dies für die Bewältigung eines Sicherheitsvorfalls oder einer Sicherheitslücke erforderlich ist, können sie auch besonders schützenswerte Personendaten über die Identität und die Handlungen von Personen, die am Vorfall beteiligt oder vom Vorfall betroffen sind oder sein könnten, bearbeiten und untereinander austauschen.

Art. 45 ISMS-Anwendung

1 Die Organisationen nach Artikel 2 Absätze 1–3 können für das Management der Informationssicherheit ein Informationssystem (ISMS-Anwendung) betreiben.

2 Sie können in der ISMS-Anwendung alle Informationen im Zusammenhang mit dem Management der Informationssicherheit nach dieser Verordnung sowie die besonders schützenswerten Daten nach Artikel 44 Absatz 3 bearbeiten.

3 Sie können ihre ISMS-Anwendungen miteinander verknüpfen und informationssicherheitsrelevante Informationen über automatisierte Schnittstellen austauschen.

Art. 46 Elektronische Formulardienste

1 Die Fachstelle des Bundes für Informationssicherheit kann für die nachfolgenden Zwecke elektronische Formulardienste betreiben und sie mit ihrer ISMS-Anwendung verknüpfen:

a. zur Abwicklung der Reisen nach Artikel 41 Absatz 4 Buchstabe e;

b. zur Ausstellung und Zustellung von Sicherheitsbescheinigungen im internationalen Verhältnis nach Artikel 30 VPSP[20];

c. zur Ausstellung und Zustellung von internationalen Betriebssicherheitsbescheinigungen nach Artikel 66 ISG.

2 Mit den Formulardiensten nach Absatz 1 können die Personendaten nach Anhang 2 bearbeitet werden. Diese Daten dürfen längstens zehn Jahre aufbewahrt werden.

3 Die Organisationen nach Artikel 2 Absätze 1–3 können elektronische Formulardienste zur Meldung von Sicherheitsvorfällen und Sicherheitslücken betreiben und sie mit ihrer ISMS-Anwendung verknüpfen.

4 Mit den Formulardiensten nach Absatz 3 können sie Personendaten, einschliesslich besonders schützenswerte Personendaten nach Artikel 44 Absatz 3, die für die Bewältigung von Sicherheitsvorfällen und Sicherheitslücken erforderlich sind, bearbeiten.

5 Die Daten nach Absatz 4 müssen unmittelbar nach dem Versand der Meldung aus dem Formulardienst gelöscht werden. Sie dürfen vor dem Versand der Meldung während höchstens 24 Stunden vorübergehend gespeichert werden.

20 SR **128.xxx**

10. Abschnitt: Schlussbestimmungen

Art. 47 Aufhebung und Änderung anderer Erlasse

[1] Die folgenden Erlasse werden aufgehoben:

a. die Cyberrisikenverordnung vom 27. Mai 2020[21];

b. die Informationsschutzverordnung vom 4. Juli 2007[22].

[2] Die Änderung anderer Erlasse wird in Anhang 3 geregelt.

Art. 48 Übergangsbestimmungen

[1] Vor Inkrafttreten dieser Verordnung durch das Nationale Zentrum für Cybersicherheit erlassene Vorgaben zur Informatiksicherheit und bewilligte Ausnahmen gelten bis höchstens sechs Jahre nach Inkrafttreten dieser Verordnung.

[2] Über Änderungen an Vorgaben und bewilligten Ausnahmen nach Absatz 1 entscheidet die Fachstelle des Bundes für Informationssicherheit.

[3] Vor Inkrafttreten dieser Verordnung durch die Generalsekretärenkonferenz oder durch die Koordinationsstelle für den Informationsschutz im Bund erlassene Vorgaben zum Informationsschutz gelten bis höchstens fünf Jahre nach Inkrafttreten dieser Verordnung.

[4] Die Verwaltungseinheiten und die Bundeskanzlei müssen ihr ISMS bis spätestens drei Jahre nach Inkrafttreten dieser Verordnung aufbauen.

[5] Die Sicherheitsakkreditierung nach Artikel 23 wird nicht durchgeführt bei Informatikmitteln, die:

a. vor Inkrafttreten dieser Verordnung in Betrieb sind;

b. bei Inkrafttreten dieser Verordnung in Entwicklung sind, sofern sie einen unverhältnismässig hohen Aufwand verursachen würde.

Art. 49 Inkrafttreten

Diese Verordnung tritt am … 2023 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: …
Der Bundeskanzler: Walter Thurnherr

21 [AS **2020** 2107, **2020** 5871, **2021** 132]
22 [AS **2007** 3401, **2010** 3207, **2013** 1341, **2014** 3543, **2016** 1785, **2017** 7391, **2020** 6011]

Anhang 1
(Art. 2 Abs. 2 und 3)

Verwaltungseinheiten der dezentralen Bundesverwaltung, für welche die Informationssicherheitsverordnung gilt

1. Verwaltungseinheiten, die auf Informatikmittel der internen IKT-Leistungserbringer nach Artikel 9 VDTI[23] zugreifen, sofern diese der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 zugeordnet sind:

a. …
b. …
c. …

2. Verwaltungseinheiten, die Informatikmittel der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 einsetzen:

a. …
b. …
c. …

3. Verwaltungseinheiten, die nicht unter Artikel 2 Absatz 2 Buchstabe a oder b fallen, die aber klassifizierte Informationen des Bundes bearbeiten:

a. …
b. …
c. …

4. Weitere Verwaltungseinheiten (vgl. Art. 2 Abs. 3):

a. …
b. …
c. …

23 SR **172.010.58**

Anhang 2
(Art. 46 Abs. 2)

Datenbearbeitung in den elektronischen Formulardiensten nach Artikel 46

In den Formulardiensten nach Artikel 46 dürfen folgende Personendaten bearbeitet werden:

1. Formulardienst nach Artikel 46 Absatz 1 Buchstabe a ISV

   a. Angaben zur Person:
      1. Namen und Vornamen*
      2. AHV-Nummer
      3. Anrede, Titel und Rang*
      4. Geburtsdatum*
      5. Heimatort und Geburtsort*
      6. Nationalität/en*
      7. Identitätskarten- und Passnummer sowie Ausstellungsort und Gültigkeit*

   b. Angaben zur beruflichen oder militärischen Funktion der Person:
      1. Funktion in der Organisation oder in der Armee*
      2. berufliche Adresse, E-Mail-Adresse, Telefonnummer und weitere, insbesondere elektronische Kontaktdaten
      3. positiver Entscheid über die Personensicherheitsprüfung, Prüfstufe und Gültigkeitsdauer*

   c. Angaben zur antragstellenden Organisation
      1. Name, Adresse und Kontaktdaten der Organisation*
      2. Name und Vornamen der Bezugsperson
      3. Funktion der Bezugsperson in der Organisation oder in der Armee
      4. berufliche Adresse, E-Mail-Adresse, Telefonnummer und elektronische Kontaktdaten der Bezugsperson

   d. Angaben zum Besuch:
      1. Name, Adresse, E-Mail-Adresse und Kontaktdaten der ausländischen Organisation *
      2. Grund des Besuchs*
      3. Sicherheitsstufe des Besuchs*
      4. Dauer des Besuchs*
      5. Grenzübertrittpunkte*
      6. Transportmittel*
      7. mitgeführtes Material, einschliesslich Waffen, Munition und Sprengstoffe, Fahrzeuge und sonstige Ausrüstung*

Angaben mit einem (*) werden der ausländischen Sicherheitsbehörde kommuniziert.

2. Formulardienst nach Artikel 46 Absatz 1 Buchstabe b ISV

   a. Angaben zur Person:
      1. Namen und Vornamen
      2. AHV-Nummer
      3. Anrede, Titel und Rang
      4. Geburtsdatum
      5. Heimatort und Geburtsort
      6. Nationalitäten
      7. Identitätskarten- und Passnummer sowie Ausstellungsort und Gültigkeit
   b. Angaben zur beruflichen oder militärischen Funktion der Person:
      1. Funktion in der Organisation oder in der Armee
      2. berufliche Adresse, E-Mail-Adresse, Telefonnummer und weitere, insbesondere elektronische, Kontaktdaten
      3. positiver Entscheid über die Personensicherheitsprüfung, Prüfstufe und Gültigkeitsdauer
   c. Angaben zur antragsstellenden Organisation
      1. Name, Adresse, E-Mail-Adresse und Kontaktdaten der Organisation
      2. Name und Vornamen der Bezugsperson
      3. Funktion der Bezugsperson in der Organisation oder in der Armee
      4. Berufliche Adresse, E-Mail-Adresse und weitere, insbesondere elektronische, Kontaktdaten der Bezugsperson
      5. Grund für die Erstellung der Bescheinigung.

3. Formulardienst nach Artikel 46 Absatz 1 Buchstabe c ISV

   a. Angaben zum Betrieb
      1. Vollständiger Name*
      2. Rechtsform*
      3. Unternehmens-Identifikationsnummer
      4. Adresse, E-Mail-Adresse und weitere, insbesondere elektronische Kontaktdaten*
      5. Sitz*
      6. Namen und Vornamen der Bezugsperson*
      7. Funktion der Bezugsperson im Betrieb
      8. berufliche Adresse, E-Mail-Adresse und weitere, insbesondere elektronische Kontaktdaten der Bezugsperson
   b. Angaben zur Betriebssicherheitserklärung:
      1. Ausstellungsdatum und Gültigkeitsdauer*
      2. Anwendungsbereich und Auflagen*
      3. Höchste zugelassene Klassifizierungs- oder Sicherheitsstufe*

Angaben mit einem (*) werden der ausländischen Sicherheitsbehörde kommuniziert.

4. Formulardienst nach Artikel 46 Absätze 3–5 ISV

   a. Angaben zur meldenden Person:
      1. Namen und Vornamen
      2. Adresse, E-Mail-Adresse, Telefonnummer und weitere, insbesondere elektronische Kontaktdaten
      3. Funktion in der Organisation oder in der Armee
   b. Angaben zum Schadensereignis und zur Schadenbemessung
   c. Bild-, Ton- oder Videoaufnahmen des Vorfalls oder der Sicherheitslücke
   d. Dokumente oder Dateien mit Bezug zum Vorfall oder zur Sicherheitslücke
   e. Angaben zu allenfalls am Vorfall beteiligten Personen
   f. Erste Abklärungen von Sachverständigen einschliesslich bereits getroffener Massnahmen

Anhang 3
(Art. 47 Abs. 2)

Änderung anderer Erlasse

Die nachstehenden Erlasse werden wie folgt geändert:

1. Verordnung vom 25. November 2020[24] über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung

Art. 2 Abs. 2 Einleitender Satz

2 Die nachstehenden Stellen können sich, unter dem Vorbehalt widersprechender organisationsrechtlicher Bestimmungen des Bundesrechts, durch eine Vereinbarung mit dem Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI der BK) verpflichten, diese Verordnung, die Informationssicherheitsverordnung vom […][25] und die GEVER-Verordnung vom 3. April 2019[26] einschliesslich der gestützt auf diese Verordnungen erlassenen Weisungen einzuhalten:

2. Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport vom 7. März 2003[27]

Art. 3 Abs. 2

2 Es erlässt Vorschriften zur Sicherstellung der Ausrüstung der Armee.

Art. 6 Bst. b

Aufgehoben

3. Verordnung vom 24. Juni 2009[28] über internationale militärische Kontakte

Art. 4 Bst. c

Die folgenden Stellen dürfen in ihrem Aufgabenbereich ohne Bewilligung des Militärprotokolls internationale militärische Kontakte formell aufnehmen:

24 SR **172.010.58**
25 SR …
26 SR **172.010.441**
27 SR **172.214.1**
28 SR **510.215**

c. die Fachstelle des Bundes für Informationssicherheit;

Art. 5 Abs. 1

[1] Die Abgabe von klassifizierten Informationen an ausländische Personen und Stellen sowie der Zugang ausländischer Besucher und Besucherinnen zu klassifizierten militärischen Informationen, zu klassifiziertem Material oder zu militärischen Anlagen in der Schweiz richtet sich nach den entsprechenden Informationsschutzvorschriften, insbesondere:

a. dem im konkreten Fall anwendbaren völkerrechtlichen Vertrag nach Artikel 87 des Informationssicherheitsgesetzes von 20. Dezember 2020[29];

b. der Verordnung vom …[30] über die Personensicherheitsprüfungen;

c. der Informationssicherheitsverordnung vom …[31];

d. der Verordnung über das Betriebssicherheitsverfahren vom …[32].

29 SR **128**
30 SR **...**
31 SR **...**
32 SR **...**