Weisungen über die Nutzung der Informatikmittel des VBS (Informatiknutzungsweisungen VBS)

vom 15. Dezember 2016

Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) erlässt folgende Weisungen:

1. Abschnitt: Allgemeine Bestimmungen

Ziffer 1 Zweck

[1] Diese Weisungen regeln:

a. die Veröffentlichung von Informationen und Personendaten sowie den Informationsaustausch im Internet, Intranet und Extranet (Abschnitt 2);

b. die Nutzung und das Monitoring der Informatikmittel des VBS (Abschnitte 3 und 4) sowie in Umsetzung der Verordnung vom 22. Februar 2012[1] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen, die Bearbeitung von Personendaten, die bei der Nutzung der Informatikmittel des VBS anfallen;

c. das Vorgehen bei Widerhandlungen gegen Nutzungsvorschriften oder Vorschriften der integralen Sicherheit, des Datenschutzes, des Personal- oder Strafrechts.

[2] Die Informatikmittel des VBS sollen rechtskonform und wirtschaftlich eingesetzt werden. Die bei der Benutzung anfallenden Informationen und Daten sollen geschützt werden.

Ziffer 2 Geltungsbereich

Diese Weisungen gelten für alle Mitarbeitenden des VBS, für Angehörige der Armee und für schutzdienstpflichtige Personen, die im VBS Dienst leisten und Dritte, die auf Informatikmittel des VBS Zugriff haben. Vorbehalten bleiben Bestimmungen des Bundesamtes für Informatik als Leistungserbringerin für Leistungsbezüger aus dem VBS.

Ziffer 3 Begriffe

Die Begriffe werden im Anhang 1 definiert.

2. Abschnitt: Informationsschutz und Datenschutz

Ziffer 4 Klassifizierte Informationen

[1] Klassifizierte Informationen (GEHEIM, VERTRAULICH oder INTERN) dürfen nicht veröffentlicht werden.

[2] INTERN klassifizierte Informationen dürfen, sofern erforderlich, elektronisch über Closed User Groups (CUG) wie die E-Learning Plattform der Schweizer Armee (LMS VBS) für Berechtigte

[1] SR **172.010.442**

zugänglich gemacht werden. Nicht mehr benötigte oder nicht mehr aktuelle Informationen sind aus den CUG zu löschen.

[3] VERTRAULICH klassifizierte Informationen dürfen vorschriftsgemäss verschlüsselt in CUG und im LMS VBS gespeichert werden.

[4] GEHEIM klassifizierte Informationen dürfen weder verschlüsselt noch unverschlüsselt in CUG und im LMS VBS gespeichert und zugänglich gemacht werden. Die Art und Weise der Verbreitung derselben richtet sich nach den Informationsschutzvorschriften[2].

[5] Zugriffe auf eine CUG müssen über ein persönliches Login und Passwort erfolgen. Geschützte Bereiche innerhalb von sozialen Netzwerken wie Facebook, MySpace, Xing, LinkedIn usw. gelten nicht als CUG.

Ziffer 5 Bearbeitung von Personendaten

[1] Die Bearbeitung von Personendaten richtet sich nach der Datenschutzgesetzgebung. Die Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

[2] Personendaten dürfen nur veröffentlicht werden, wenn dies in einer gesetzlichen Grundlage vorgesehen ist oder ausnahmsweise im Einzelfall eine schriftliche Einwilligung eingeholt wurde. Vor der Einwilligung ist die betroffene Person über Umfang, Dauer und Zweck der Veröffentlichung und die Möglichkeit, ihre Einwilligung zurückzuziehen, aufzuklären.

Ziffer 6 Berufliche Angaben

[1] Im Intranet dürfen zwecks Erleichterung der Kommunikation Personendaten, die direkt mit der beruflichen Stellung der Mitarbeitenden in Zusammenhang stehen, wie Name, Titel, Funktion, Verwaltungseinheit, Telefonnummer, FAX, E-Mail-Adresse, verwendete Kommunikationsprotokolle und Teile von Verschlüsselungsinformationen (öffentlicher Schlüssel) veröffentlicht werden.

[2] Im Internet und Extranet dürfen nur die notwendigen beruflichen Angaben von Mitarbeitenden veröffentlicht werden, die nach ihrer Funktion regelmässig von verwaltungsexternen Dritten kontaktiert werden[3]. Die betroffenen Personen sind vorgängig zu informieren.

[3] Die nach Absatz 1 oder 2 zur Publikation vorgesehenen Personendaten dürfen weder als Einzelinformation noch in ihrer Gesamtheit einen klassifizierten Inhalt nach den Informationsschutzvorschriften enthalten.

Ziffer 7 Aufnahmen

[1] Aufnahmen (Foto/Film/Ton) dürfen nur nach Massgabe der Datenschutz- und Anlageschutzgesetzgebung und gegebenenfalls nach einschränkenderen Vorgaben der Verwaltung oder der Armee erfolgen.

[2] Aufnahmen von:

a. Mitarbeitenden, Angehörigen der Armee sowie schutzdienstpflichtigen Personen, die im VBS Dienst leisten, dürfen im Internet, Intranet und Extranet nur einzelfallweise und ausschliesslich mit Zustimmung der Betroffenen veröffentlicht werden;
b. Mitarbeitenden, Angehörigen der Armee sowie schutzdienstpflichtigen Personen, die im VBS Dienst leisten und dienstlichen Tätigkeiten nachgehen (wie Sportanlass, Gefechtseinsatz, Parkdienst, Militärrituale) und nicht eindeutig identifizierbar sind, dürfen ohne Einwilligung der Betroffenen und ohne Nennung ihres Namens zur Illustration veröffentlicht werden;
c. Personen von öffentlichem Interesse und mit regem Publikums- oder Truppenkontakt (Personen des öffentlichen Lebens) können veröffentlicht werden.

[3] Darstellungen von Gewalteinwirkungen (wie Verletzten- und Unfallbilder) dürfen nur unter Beachtung des Verhältnismässigkeitsprinzips zugänglich gemacht werden. Darstellungen, die ge-

[2] http://intranet.vbs.admin.ch > Querschnittsaufgaben > Integrale Sicherheit > Erlasse Integrale Sicherheit > Informationsschutz.
[3] Artikel 5 der Organisationsverordnung vom 29. Oktober 2008 für die Bundeskanzlei (OV-BK; SR **172.210.10**).

gen die guten Sitten verstossen und dem Ansehen des VBS oder der Armee schaden, dürfen nicht zugänglich gemacht werden.

[4] Das Bildmaterial, das innerhalb der Mediathek des VBS zur Verfügung gestellt wird, darf im Rahmen der Nutzungsbedingungen frei verwendet werden.

Ziffer 8 Auskunftsrecht

Mitarbeitende können beim Arbeitgeber, Angehörige der Armee sowie Schutzdienstpflichtige beim Kommandanten und Dritte, die im Auftrag des VBS eine Dienstleistung erbringen, beim Auftraggeber Auskunft darüber verlangen, ob und zu welchem Zweck ihre Person betreffende Auswertungen der Systemprotokolle erfolgt sind und welche ihrer Daten bearbeitet werden[4].

3. Abschnitt: Nutzung der Informatikmittel für dienstliche und private Zwecke

Ziffer 9 Umgang mit Daten bei Ferien, Krankheit, Unfall, Austritt und Tod (Anhang 2)

[1] Austretende Mitarbeitende übergeben ihre dienstlichen Daten nach Absprache den Vorgesetzten. Nicht dienstliche Daten entfernen sie aus den Informatikmitteln des VBS. Übergabe und Löschung können von den Austretenden und den Vorgesetzten gegenseitig schriftlich bestätigt werden.

[2] Falls der Zugriff nach Absatz 1 nicht gewährleistet ist, kann der Arbeitgeber zur Erfüllung seiner gesetzlichen Aufgabe unter Beizug der Informatiksicherheitsbeauftragten der Verwaltungseinheiten (ISBO) und den zuständigen Datenschutzberatenden auf die dienstlichen Daten von Mitarbeitenden zugreifen bei:

a. Abwesenheit (Krankheit/Unfall/Austritt) des Mitarbeitenden sofern dessen schriftliches Einverständnis nicht eingeholt werden kann;

b. Todesfall oder Freistellung des Mitarbeitenden.

[3] Offensichtlich private und als „PRIVAT“ gekennzeichnete Daten sind nicht zu sichten und auf einem externen Speicher zu sichern. Der Speicher mit den privaten Daten ist dem betroffenen Mitarbeitenden oder, wenn dies nicht mehr möglich ist, dessen Angehörigen durch den Vorgesetzten unter Angabe einer Frist von mindestens 30 Tagen zur Abgabe anzubieten. Diese Vorgänge sind zu protokollieren. Das datierte Protokoll ist von den Beteiligten zu visieren.

[4] Der Arbeitgeber schaltet mit Einbezug der ISBO zudem bei Bedarf auf dem E-Mail-Konto der abwesenden Mitarbeitenden ein Antwortmail auf, worin auf die Abwesenheit aufmerksam gemacht wird und für dienstliche Anfragen auf eine Ansprechstelle verwiesen wird. Im Todesfall und bei Freistellung veranlassen die direkten Vorgesetzten die sofortige Sperrung des E-Mail-Kontos. Das im Anhang 2 festgelegte Vorgehen ist zu befolgen.

[5] Das Vorgehen für personenbezogene Auswertungen infolge eines Missbrauchsverdachts wird in Ziffer 17 ff. geregelt.

Ziffer 10 Private Nutzung der Informatikmittel

[1] Die private Nutzung der Informatikinfrastruktur und Informatikmittel ist in verhältnismässigem Rahmen gestattet und hat grundsätzlich ausserhalb der Arbeitszeit oder während den Pausen zu erfolgen. Private Daten sind mit „PRIVAT“ zu kennzeichnen.

[2] Das VBS haftet weder für den Verlust noch für die Beschädigung von privaten Daten.

Ziffer 11 Verbotene Nutzungen

[1] Es ist verboten, die Informatikmittel des VBS wie folgt zu nutzen, ausser die Nutzung erfolge zu dienstlichen Zwecken:

a. ändern der Konfiguration von Hard- und Software der Informatikmittel VBS;

b. widerrechtliches Kopieren, Verändern und Löschen von Daten;

[4] Artikel 8 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG; SR **235.1**).

c. Verwendung der Informatikmittel zwecks Erlangen eines nicht autorisierten Zugangs zu Systemen oder Diensten;

d. Verbindung privater Hardware mit der Informatikinfrastruktur VBS oder Installation und Verwendung privater Software auf derselben;

e. Beanspruchung von Ressourcen (insbesondere Arbeitszeit, Bandbreite, Datenmenge, Speicherplatz etc.) für private Zwecke, die einen Umfang einnimmt, der in einem Missverhältnis zur dienstlichen Verwendung der Informatikmittel steht;

f. verwenden der Informatikmittel zu privaten Zwecken kommerzieller Natur;

g. benutzen der Infrastruktur für Hacking, Cracking anderer oder eigener Systeme, insbesondere das Kopieren oder Einsetzen derartiger Software;

h. herunterladen, ausführen oder installieren von Software, die nicht das VBS oder der zuständige Leistungserbringer zur Verfügung gestellt hat. Für Mobile Devices gilt die Nutzungsvereinbarung;

i. herunterladen, ausführen oder speichern von privaten Foto-, Musik- und Filmsammlungen. Vorbehalten bleiben abweichende Nutzungsvereinbarungen;

j. aufrufen, betrachten, speichern und verbreiten von Websiten, Links und Dateien mit rassistischem, gewaltverherrlichendem, pornografischem, geschäftsschädigendem oder strafrechtlich relevantem Inhalt;

k. verbreiten von Meinungsäusserungen auf Chat-Foren, in Newsgroups, in sozialen Netzwerken und ähnlichem, die dem Ansehen des Bundes oder seinen Mitarbeitenden, dem VBS, dem Zivilschutz oder der Armee schaden;

l. erstellen oder verbreiten von schädlichen Programmcodes wie Viren, Trojanern und Würmern;

m. Synchronisation dienstlicher Daten auf private IKT-Mittel;

n. nutzen von nicht allgemein freigegebenen Diensten (DynDNS usw.) ohne Bewilligung der oder des Informatiksicherheitsbeauftragten des VBS (ISBD).

o. nutzen von öffentlichen Online-Speicherdiensten und anderen Cloud-Diensten (Bsp. iClouds, SkyDrive, Google Drive, Dropbox, Webmail usw.) für die Speicherung, Verarbeitung oder Übermittlung von dienstlichen Informationen.

[2] Insbesondere ist verboten, das E-Mail wie folgt zu nutzen, ausser die Nutzung erfolge zu dienstlichen Zwecken:

a. versenden von Massenmails (ausser durch berechtigte Stellen) und E-Mails mit vorgetäuschten E-Mail-Absenderadressen;

b. versenden von E-Mails mit rechtswidrigem, pornografischem, rassistischem, sexistischem, gewaltverherrlichendem oder belästigendem Inhalt (stalking);

c. übermitteln von klassifizierten Informationen entgegen den Informationsschutzvorschriften;

d. unverschlüsseltes Übermitteln von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen;

e. umleiten der internen dienstlichen Mailbox auf eine externe oder private Adresse;

f. verwenden der dienstlichen E-Mail Adresse zu kommerziellen Zwecken;

g. öffnen oder weiterleiten von E-Mails mit zweifelhaftem Absender oder von E-Mails mit zweifelhaftem Betreff oder Anhang. Zweifelhafte E-Mails oder Dateien sind nach vorgängiger Absprache mit der oder dem zuständigen ISBO dem Computer Emergency Response Team des Leistungserbringers (CERT) zur Analyse abzugeben.

Ziffer 12 Schutzrechte Dritter

Bei der Verwendung und Bearbeitung von Daten aus dem Intranet, dem Internet und dem Extranet sind Urheberrechte und verwandte Schutzrechte Dritter, wie Persönlichkeitsrechte und Vergütungsansprüche, zu beachten[5].

[5] Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG; SR **231.1**).

4. Abschnitt: Aufzeichnung und Auswertung der System- und Personendaten

Ziffer 13 Aufzeichnung der System- und Personendaten

Die für den technischen Betrieb der elektronischen Infrastruktur des VBS verantwortlichen Leistungserbringer (LE VBS) zeichnen die bei der Nutzung der elektronischen Infrastruktur anfallenden System- und Personendaten auf, um den ordnungsgemässen und störungsfreien Betrieb und die regelmässige Anpassung der technischen Schutzmassnahmen sicherzustellen. Sie zeichnen Personendaten nach Artikel 57*l* des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[6] (RVOG) zudem auf, um:

a. alle Daten, auch den Inhalt der elektronischen Post, zu sichern (Backup-Daten);

b. die Informations- und Dienstleistungssicherheit aufrecht zu erhalten, die technische Wartung sicherzustellen, die Einhaltung der Nutzungsregelungen zu kontrollieren, den Zugriff auf Datensammlungen nachvollziehen und die Kosten, die durch die Benutzung der elektronischen Infrastruktur enstehen, erfassen zu können;

c. die Bewirtschaftung der Arbeitszeiten des Personals sicherzustellen;

d. den Zutritt zu und die Verweildauer in Gebäuden, Objekten, Anlagen und Räumen des VBS nachzuvollziehen.

Ziffer 14 Zugriffsberechtigung und Aufbewahrungsdauer

[1] Auf aufgezeichnete und regelmässig bearbeitete Daten (bewirtschaftete Daten) nach Artikel 1 der Verordnung vom 22. Februar 2012[7] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen, dürfen die LE VBS und das CERT, soweit für die Erfüllung ihres Auftrages nach den Ziffern 15-17 erforderlich, zugreifen.

[2] Auf nicht bewirtschaftete Daten, wie zum Beispiel in FAX- oder Kopiergeräten, hat nur die Verwaltungseinheit Zugriff, in deren Nutzungszuständigkeit sich das Gerät befindet. Sie sorgt in Zusammenarbeit mit dem LE VBS für die Vernichtung dieser Daten spätestens vor der Weitergabe oder der Entsorgung des Gerätes.

[3] Bewirtschaftete Daten werden gestützt auf Artikel 4 der Verordnung vom 22. Februar 2012[8] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen, soweit der Auswertungszweck dies erfordert und unter Vorbehalt besonderer gesetzlicher Bestimmungen[9], längstens wie folgt aufbewahrt:

a. Backup-Daten: bis zur Übernahme durch das Bundesarchiv oder 2 Jahre nach Nichtübernahme durch das Bundesarchiv;

b. Daten über die Nutzung der elektronischen Infrastruktur: 2 Jahre;

c. Arbeitszeitkontrolldaten: 5 Jahre;

d. Zutrittskontrolldaten: 3 Jahre; bei militärischen Anlagen: 5 Jahre[10].

Ziffer 15 Nicht personenbezogene und nicht namentlich personenbezogene Auswertungen

[1] Die nicht personenbezogene Auswertung aufgezeichneter Daten richtet sich nach Artikel 57*m* RVOG.

[2] Die nicht namentlich personenbezogene Auswertung aufgezeichneter Daten richtet sich nach Artikel 57*n* RVOG.

[3] Auswertungen sind zwecks Nachvollziehbarkeit zu protokollieren.

---

[6] SR **172.010**
[7] SR **172.010.442**
[8] SR **172.010.442**
[9] vgl. z.B. Aufbewahrungsdauer für Personaldossiers, Artikel 13 der Verordnung vom 26. Oktober 2011 über den Schutz von Personaldaten des Bundespersonals (BPDV; SR **172.220.111.4**).
[10] Weisungen CdA vom 1.1.2013 über die Bewilligungsverfahren zum Schutz militärischer Anlagen.

Ziffer 16 Namentlich personenbezogene Auswertungen

[1] Technische Schutzmassnahmen, Sensibilisierungskampagnen und Auswertungen ohne Rückschlussmöglichkeit auf Personen haben Vorrang vor namentlich personenbezogenen Auswertungen.

[2] Das CERT kann unter Beizug des ISBD bzw. der ISBO bewirtschaftete Daten gestützt auf Artikel 57*o* RVOG namentlich personenbezogen auswerten, sofern nur damit:

a. die Ursache einer erheblichen Störung und deren zeitgerechte Beseitigung sichergestellt werden kann. Eine erhebliche Störung liegt vor, wenn die Nutzung der Informatikmittel durch einen Defekt, eine missbräuchliche oder ausserordentliche Nutzung oder einen Cyberangriff verunmöglicht oder stark eingeschränkt wird;

b. die unmittelbare Gefahr einer Schädigung der Informatikinfrastruktur beseitigt werden kann.

[3] Das CERT führt, abgesehen von den in Absatz 2 genannten Fällen, namentlich personenbezogene Auswertungen von bewirtschafteten und nicht bewirtschafteten Daten nach Artikel 57*o* RVOG gestützt auf einen hinreichend begründeten Auftrag gemäss Formular (Anhang 4) durch. Dieser Auftrag wird erteilt durch:

a. eine zivile oder militärische Strafbehörde oder durch das Oberauditorat. Das CERT ist vorgängig allenfalls gemäss Artikel 94 der Bundespersonalverordnung vom 3. Juli 2001[11] (BPV) vom Amtsgeheimnis zu entbinden;

b. das Bundesamt der betroffenen Mitarbeitenden, wenn ein konkreter Verdacht auf eine Widerhandlung gegen die vorliegenden Nutzungsvorschriften oder Vorschriften der integralen Sicherheit, des Datenschutzes, des Personal- oder Strafrechts vorliegen;

c. das Bundesamt für die Bereitstellung von Dienstleistungen, wie die Erfassung und Fakturierung erbrachter Leistungen oder die Kontrolle der individuellen Arbeitszeiten.

[4] Auswertungen sind zwecks Nachvollziehbarkeit zu protokollieren.

5. Abschnitt: Untersuchungsprozess (Anhang 3)

Ziffer 17 Vorgehen bei Verdacht auf Widerhandlung

[1] Wer infolge eines Ereignisses oder nach einer nicht personenbezogenen Auswertung einen konkreten Verdacht auf eine Widerhandlung gegen Nutzungsvorschriften oder Vorschriften der integralen Sicherheit, des Datenschutzes, des Personal- oder Strafrechts hat:

a. trifft die notwendigen Sofortmassnahmen (Bsp. Information an Vorgesetzten, Meldung ISBO etc.);

b. setzt eine Sicherheitsmeldung (SIME)[12] an die Informations- und Objektsicherheit (IOS) ab, und

c. informiert die Koordinationsstelle Vorfälle (KOVOR; E-Mail: KOVOR@gs-vbs.admin.ch).

[2] Die KOVOR setzt sich zusammen aus je einer Vertretung aus der IOS (Vorsitz), dem Personalrecht VBS und dem CERT. Sie erhält von der IOS sämtliche SIME-Meldungen gemäss Absatz 1.

[3] Die KOVOR:

a. nimmt eine summarische Einschätzung des gemeldeten Sachverhaltes vor. Dabei prüft sie, ob ein hinreichender Verdacht vorliegt und ob eine zeitliche Dringlichkeit zum Handeln besteht, falls notwendig in Rücksprache mit der Koordinationsstelle zur Bekämpfung der Internetkriminalität des Bundes (KOBIK);

b. kann zusätzliche Informationen, insbesondere über die Identität der betroffenen Person beschaffen;

c. kann eine Vertretung des zuständigen Personal- und Rechtsdienstes sowie der zuständigen Sicherheitsorganisation beiziehen;

[11] SR **172.220.111.3**
[12] http://intranet.vbs.admin.ch > Querschnittaufgaben > Integrale Sicherheit > Dokumente > Meldeformular SIME.

d. kann nach Absprache mit dem zuständigen Rechtsdienst die betroffene Person informell zum Sachverhalt befragen;

e. ordnet nötigenfalls unter Einbezug der zuständigen Sicherheitsorganisation zusätzliche Sofortmassnahmen, insbesondere zur Sicherung der Informatikmittel zu Beweiszwecken, an;

f. teilt dem betroffenen Bundesamt oder Kommandanten mit, ob es sich nach ihrer Einschätzung um einen leichten, einen mittelschweren oder einen gravierenden Fall handelt und schlägt das weitere Vorgehen vor.

[4] Das zuständige Bundesamt oder der zuständige Kommandant entscheidet nach der Empfehlung der KOVOR über das weitere Vorgehen.

[5] Das zuständige Bundesamt kann bei Vorliegen eines konkreten Verdachtes dem CERT einen begründeten Auftrag (Anhang 4) zur personenbezogenen, namentlichen Auswertung der Daten erteilen. Gleichzeitig ist die betroffene Person über die angeordnete Auswertung gestützt auf Artikel 57*o* Absatz 2 Buchstabe b RVOG zu informieren. Im Bereich von Militärstrafverfahren richten sich die Zuständigkeit für die Erteilung eines Auftrages und das weitere Vorgehen nach Artikel 70 ff. des Militärstrafprozesses vom 23. März 1979[13].

[6] Das CERT wertet die Daten gemäss Auftrag aus und erstellt einen Analysebericht. Falls im Rahmen der Auswertung eine Ausweitung des Auftrages notwendig wird, ergänzt der Auftraggeber den ursprünglichen Auftrag. Die Auswertungen sind zwecks Nachvollziehbarkeit und Überprüfbarkeit zu protokollieren. Das CERT vernichtet nach Rücksprache mit dem Auftraggeber ein Jahr nach Ablieferung des Berichts die bei der Auswertung angefallenen Daten.

[7] Das zuständige Bundesamt:

a. stellt das Verfahren ein, wenn sich der Verdacht nicht erhärtet hat, und informiert die Betroffenen;

b. trifft als Arbeitgeber die für den geordneten Vollzug der Aufgaben nötigen Massnahmen im Sinne von Artikel 25 des Bundespersonalgesetzes vom 24. März 2000[14];

c. überweist, wenn der Tatbestand einer strafbaren Handlung in Betracht kommt, die Akten nach Rücksprache und Einwilligung der Generalsekretärin oder des Generalsekretärs VBS im Sinne von Artikel 102 BPV der Bundesanwaltschaft. Vorbehalten bleibt die Zuständigkeit der Militärstrafgerichte oder kantonaler Behörden bei Personen, die nicht dem BPG unterstehen;

d. stellt Antrag auf Eröffnung einer Administrativuntersuchung nach Artikel 27*a* ff. der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[15], wenn ein Sachverhalt vorliegt, der im öffentlichen Interesse ein Einschreiten von Amtes wegen erfordert.

[8] Das Bundesamt informiert die KOVOR über Art und Weise der Erledigung des Vorfalls und seine Erkenntnisse.

Ziffer 18 Berichterstattung und Aufbewahrung der Protokolle

[1] Das CERT erstattet dem Datenschutzberater VBS oder der Datenschutzberaterin VBS und der oder dem ISBD jährlich Bericht über die vorgenommenen Auswertungen.

[2] Es vernichtet die Daten von personenbezogenen Auswertungen nach Rücksprache mit dem Auftraggeber, jedoch spätestens ein Jahr nach der letzten Bearbeitung.

[13] SR **322.1**
[14] SR **172.220.1**
[15] SR **172.010.1**

6. Abschnitt: Schlussbestimmungen

Ziffer 19 Information

[1] Die Vorgesetzten informieren die Mitarbeitenden, die Angehörigen der Armee und die Schutzdienstpflichtigen, die im VBS Dienst leisten, sowie mandatierte Dritte, welche die Informatikmittel VBS nutzen, über die vorliegenden Weisungen und deren Bezugsquellen.

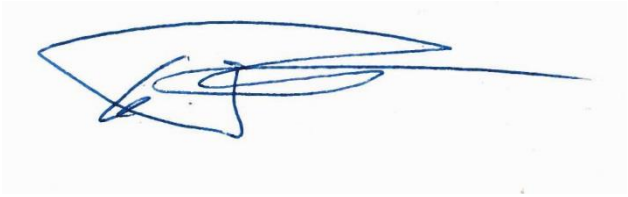
[2] Diese bestätigen die Kenntnisnahme gegenüber den Vorgesetzten.

Ziffer 20 Aufhebung bisherigen Rechts und Inkrafttreten

Die vorliegenden Weisungen treten am 1. Januar 2017 in Kraft und gelten bis am 31. Dezember 2021.

15. Dezember 2016

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport



Guy Parmelin

Beilagen:

Anhang 1: Begriffskatalog

Anhang 2: Prozess „Umgang mit Personendaten bei Ferien, Krankheit, Unfall, Austritt, Tod“

Anhang 3: Untersuchungsprozess

Anhang 4: Antrag auf personenbezogene Auswertung

Geht an:

Direktunterstellte C VBS

z.K an:

Personalrecht VBS (zur Publikation im InfoPers und im LMS VBS)

KOVOR (per E-Mail an KOVOR@gs-vbs.admin.ch)

Anhang 1 (zu Ziffer 3):

Begriffskatalog

Begriff	Bedeutung
Backup-Daten	Alle Daten inkl. Inhalt der elektronischen Post, die gesichert werden.
Computer Emergency Response Teams (CERT)	Sind verantwortlich für die Detektion und Behandlung von Sicherheitsvorfällen im VBS; bauen und betreiben die dafür geeigneten Infrastrukturen auf. Weitere Aufgabenbereiche sind Beratung für Prävention und Schwachstellenerkennung. Beispiele solcher CERTs: milCERT der FUB und CSIRT des BIT.
Cyber-Angriff	Ein Cyber-Angriff ist der gezielte Angriff auf grössere, für eine spezifische Infrastruktur wichtige Computernetzwerke von aussen.
Cracking	Illegales Eindringen in IT-Systeme zum eigenen Vorteil oder zum Nachteil eines Dritten.
Closed User Groups (CUG)	Geschlossene Teilnehmergruppen innerhalb von geschützten Websites, zu denen man durch Eingabe eines Benutzernamens und des dazugehörenden Passworts Zugang erlangt.
Elektronischer Informationsaustausch	Informationen, die in digitaler Form als Text, Ton und / oder Bild mittels Medium (Datenträger wie USB-Stick, MP3-Player, CD, DVD etc.) oder über Datenübertragungseinrichtungen (Netzwerke wie LAN, WLAN, Intranet, Internet etc.) mittels Diensten (E-Mail, Fax, File Transfer, Videokonferenz, digitale Telefonie etc.) ausgetauscht werden.
Extranet	Das Extranet ist eine Komponente, die nur von einer festgelegten Gruppe externer Benutzer verwendet werden kann.
Hacking	Illegales Eindringen in IT-Systeme zwecks Aufdeckung von Schwachstellen.
Informationen	Aufzeichnungen auf Informationsträgern und mündliche Äusserungen.
Informatikmittel (Informatikinfrastruktur)	Alle Mittel der Informations- und Telekommunikationstechnologie, die im Eigentum der Schweizerischen Eidgenossenschaft sind oder die durch diese beschafft wurden. Es handelt sich insbesondere um Desktopcomputer, Laptops, Datenträger, Drucker, Fotokopierer, Telefone (Festnetz- und Mobiltelefone), Personal Digital Assistent, Scanner, Telekommunikationsnetze (Daten- und Sprachkommunikation) und auf diesen Mitteln laufende Software sowie entsprechendes Verbrauchsmaterial. Private Informatikmittel: alle anderen
Informatiksicherheitsbeauftragte oder Informatiksicherheitsbeauftragter VBS (ISBD)	Nimmt die Aufgaben gemäss Ziffer 2.1 Absatz 2 der Weisungen des Bundesrates vom 1. Juli 2015[16] über die IKT-Sicherheit in der Bundesverwaltung (WIsB) wahr.
Informatiksicherheitsbeauftragte der Verwaltungseinheiten (ISBO)	Nehmen die Aufgaben gemäss Ziffer 2.1 Absatz 4 WIsB wahr.
Intranet	Netzwerk, welches nur bundesintern verfügbar ist.
KOVOR	Koordinationsstelle Vorfälle: IOS (Vorsitz), Personalrecht VBS und CERT.
LE VBS	Leistungserbringer VBS
Monitoring	Ist ein Überbegriff für alle Arten der unmittelbaren systematischen Erfassung und Protokollierung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel. Das Monitoring ist klar abzugrenzen von den durch eine richterliche Instanz im Rahmen eines Strafverfahrens angeordneten

[16] www.isb.admin.ch > IKT-Vorgaben > Sicherheit

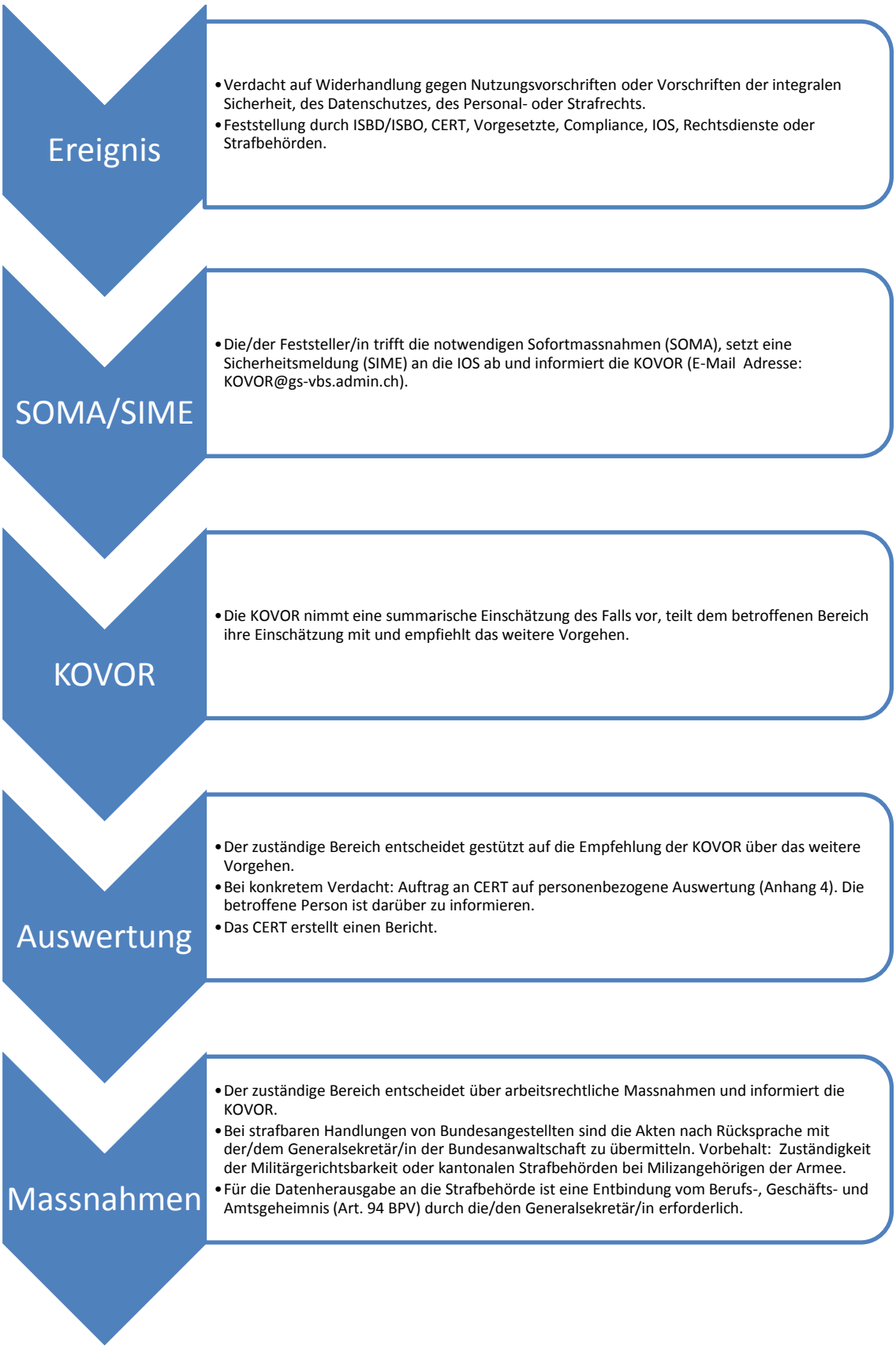
	Überwachungsmassnahmen.
Newsgroup	Forum im Intranet, Internet oder Extranet für Diskussionen über einen bestimmten Themenbereich.
Öffentlicher Schlüssel	Die Zertifikate bestehen aus einem öffentlichen Schlüssel (englisch public key) und einem privaten Schlüssel (engl. private key, deutsch auch „geheimer Schlüssel“) . Der öffentliche Schlüssel ist nicht geheim, er soll möglichst vielen anderen Benutzern bekannt sein, beispielsweise durch Verteilung über zentrale Systeme. Mit ihm können Nachrichten verschlüsselt oder digitale Unterschriften geprüft werden. Dabei ist es wichtig, dass ein öffentlicher Schlüssel eindeutig einem Benutzer zugeordnet werden kann. Der öffentliche Schlüssel beinhaltet Teilinformationen des privaten Schlüssel. Um einen Geheimtext wieder zu entschlüsseln oder eine Nachricht zu signieren, wird der private Schlüssel benötigt. Nur ein Benutzer verfügt über den privaten (geheimen) Schlüssel. Dieser Umstand ermöglicht es erst, eine Signatur eindeutig einem Benutzer zuzuordnen.
Personendaten	Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.
Randdaten	Randdaten sind Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Informatikmittel.
Soziale Netzwerke	Netzgemeinschaften mit teilweise eingeschränktem Zugang wie Facebook, MySpace, Xing, LinkedIn usw.

Anhang 2 (zu Ziffer 9):
Prozess „Umgang mit Personendaten bei Ferien, Krankheit, Unfall, Austritt, Tod“

Normalfall	Todesfall/ Freistellung Austritt ohne erfolgte Übergabe der Daten	Unfall/ Krankheit/ Abwesenheit
Grundsatz: Mitarbeitende stellen sicher, dass bei Ihrer Abwesenheit gemäss den Weisungen des Vorgesetzten auf die Daten zugegriffen werden kann. (z.B. Share, GEVER/iGeko, CUG, Übergabe etc.)	Der direkte Vorgesetzte veranlasst die **Sperrung** der Accounts des Mitarbeitenden.	Der Arbeitgeber schaltet bei Bedarf eine **Antwortmail** auf, worin auf die Abwesenheit aufmerksam gemacht und auf eine andere Ansprechstelle verwiesen wird.
Austritt: Die Vorgesetzten stellen sicher, dass austretende Mitarbeitende ihre dienstlichen Daten vor dem Austritt übergeben. Nicht dienstliche Daten entfernen Sie aus den Informatikmitteln des VBS: Übergabe und Übernahme können schriftlich bestätigt werden.	Ist der **Zugriff** auf die zur Erfüllung der gesetzlichen Aufgabe notwendigen dienstlichen **Daten** nicht möglich (vgl. Normalfall), kann der Arbeitgeber die Daten herausverlangen. Er beantragt die Herausgabe beim zuständigen Datenschutzberatenden. Nach dessen Bewilligung liefert der ISBO die Daten aus. Login-Daten dürfen nicht weitergegeben werden. **Private Daten** sind auf einem externen Speicher zu sichern und dem Mitarbeitenden, oder wenn dies nicht mehr möglich ist, dessen Angehörigen zu übergeben. Zugriff und Datenauslieferung sind in jedem Fall zu protokollieren und von allen Beteiligten zu visieren (wer, was, warum, wo und wie).	

Anhang 3 (zu Ziffer 17):

Untersuchungsprozess



Anhang 4 (zu Ziffer 17 Absatz 5):
Formular «Auftrag auf personenbezogene Auswertung»

Siehe Beilage

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Auftrag auf personenbezogene Auswertung

(Bei Bedarf unterstützt die KOVOR beim Ausfüllen des Auftrages)

Ansprechpersonen

Auftraggeber: _____

Untersuchungsleitung: _____

Auftragnehmer (CERT): _____

Sachverhalt

_____

_____

_____

Begründung des Auftrages

_____

_____

_____

Untersuchungsbereiche

Persönliche Arbeitsstation: _____

Tablet PC: _____

Smartphone: _____

Digitalkamera: _____

Persönliche Datenablage auf BURAUT Share: _____

Bilddateien: _____

Sprachdateien: _____

Videodateien: _____

Textdateien: _____

Datenbanken: _____

Gelöschte Dateien wiederherstellen: _____

Software: _____

Softwaremanipulationen: _____

Hardware: _____

Internetverkehr: _____

E-Mail Verkehr: _____

Kamerabilder ZUKO: _____

Zusätzliche Bereiche die berücksichtigt werden müssen, erweiterter Auftrag

Zu erstellende Dokumente

Info des Betroffenen

Info weiterer Stellen (Linie, PD, Komm …)

Wer:

Wann:

Wen:

Unterschriften

Datum, Ort	Unterschrift Auftraggeber
Datum, Ort	Unterschrift CERT
Datum, Ort	Der Betroffene bestätigt, dass er vom Auftraggeber über die Auswertung informiert worden ist.

Geht an

– CERT

Zur Kenntnis an

– KOVOR