Stand: 16.08.2007

VS-Anweisung - VSA
vom 31. März 2006
mit Erläuterungen

Inhaltsverzeichnis

V. IT-spezifische Maßnahmen

VI. Abschließende Regelungen

Eingangsformel

Nach § 35 Abs. 1 des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz – SÜG) vom 20. April 1994 (BGBl. I S. 867) in Verbindung mit Art. 86 des Grundgesetzes wird zum materiellen und organisatorischen Schutz von Verschlusssachen vom Bundesministerium des Innern die folgende Allgemeine Verwaltungsvorschrift erlassen.

I. Allgemeine Bestimmungen

§ 1 Geltungsbereich

(1) Die VS-Anweisung richtet sich an Bundesbehörden und bundesunmittelbare öffentlich-rechtliche Einrichtungen, die mit Verschlusssachen arbeiten und damit Vorkehrungen zu deren Schutz zu treffen haben.

(2) Darüber hinaus richtet sich die VS-Anweisung an Personen, die Zugang zu Verschlusssachen erhalten oder eine Tätigkeit ausüben, bei der sie sich Zugang zu Verschlusssachen verschaffen können und dabei bestimmte Schutzvorkehrungen zu beachten haben.

Zu Absatz 1
Für die Länder und Kommunen setzen die Landesregierungen eigene VS-Anweisungen, die in den Grundzügen mit der VS-Anweisung des Bundes übereinstimmen, in Kraft.

Über die Behandlung von VS in den Verfassungsorganen (Bundestag, Bundesrat und Bundesverfassungsgericht) entscheiden diese selbst, sie können von der VSA abweichende Regelungen treffen (z.B. Geheimschutzordnung des Deutschen Bundestages). Mit Verankerung der VS-Anweisung im SÜG gilt sie auch unmittelbar für die Verwaltungen der Verfassungsorgane.
Bestimmungen über die Anwendung der VS-Anweisung enthält auch die Gemeinsame Geschäftsordnung der Bundesregierung (GGO), vgl. z. B. §§ 16, 17, 18, 19 GGO und Anlage 4 zu § 39 GGO.
Für Betriebe der geheimschutzbetreuten Industrie sind die zu beachtenden Geheimschutzanforderungen im „Handbuch für den Geheimschutz in der Wirtschaft“ (Geheimschutzhandbuch) des Bundesministeriums für Wirtschaft und Technologie (BMWi) aufgeführt.

Zu Absatz 2
Vorausgesetzt wird, die Person hält sich in einer Bundesbehörde oder bundesunmittelbaren öffentlich rechtlichen Einrichtung auf oder ist im Auftrag einer solchen Stelle tätig. Bei landes- und Kommunalbehörden oder deren öffentlich rechtlichen Einrichtungen gelten die in der VS-Anweisung des jeweiligen Landes aufgeführten Regelungen.

§ 2 Begriff der Verschlusssache

(1) Nach § 4 Abs. 1 des Sicherheitsüberprüfungsgesetzes[*] vom 20. April 1994 (BGBl. I S. 867) in der jeweils geltenden Fassung sind Verschlusssachen (VS) im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse unabhängig von ihrer Darstellungsform (z. B. Schriftstücke, Zeichnungen, Karten, Fotokopien, Lichtbildmaterial, elektronische Dateien und Datenträger, elektrische Signale, Geräte, technische Einrichtungen oder das gesprochene Wort). Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung in Geheimhaltungsgrade eingestuft.

(2) Zwischenmaterial, das im Zusammenhang mit einer VS anfällt (z. B. Dateien, Vorentwürfe, Stenogramme, Tonträger, Folien oder Fehldrucke), gilt als VS im Sinne des Absatzes 1. Für die

[*] Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz – SÜG) vom 20. April 1994 (BGBl. I S. 867), zuletzt geändert durch Art. 4 des Gesetzes vom 21. Juni 2005 (BGBl I S. 1818).

Behandlung von VS-Zwischenmaterial sind Abweichungen bei der Kennzeichnung und beim Nachweis sowie bei der Vernichtung zugelassen.

(3) Können wegen der Beschaffenheit einer VS Bestimmungen der VS-Anweisung nicht angewendet werden, so ist sinngemäß zu verfahren. Dabei sind möglichst gleichwertige Sicherheitsmaßnahmen zu treffen.

Zu Absatz 1:
Die Aufstellung in Satz 1 ist nur beispielhaft.

Zu Absatz 2:
VS-Zwischenmaterial enthält in der Regel die gleichen Informationen wie die Original-VS. Es bedarf daher auch grundsätzlich des gleichen Schutzes. Abweichungen sind nur im Rahmen von § 16 Abs. 4 und Abs. 5 sowie § 28 Abs. 4 VSA zulässig.

Zu Absatz 3:
Bei VS von bestimmter Beschaffenheit (z.B. von Bauwerken, elektrischen Signalen oder dem gesprochenen Wort) können nicht alle Bestimmungen der VS-Anweisung wörtlich angewandt werden. Hier ist sinngemäß zu verfahren, um den angestrebten Schutz zu erreichen (z.B. durch Unterrichtung des Gesprächspartners über den Grad der VS-Einstufung einer mündlichen Information).

Mit der Formulierung "möglichst gleichwertige Sicherheitsmaßnahmen" in Satz 2 wird vor allem den besonderen Gegebenheiten im militärischen Bereich (VS eingestufte Geräte und Waffensysteme) Rechung getragen. Auch lassen sich nicht immer gleichwertige Schutzmaßnahmen durchführen, z. B. wenn bei der Vernichtung Eile geboten ist.

§ 3 Geheimhaltungsgrade

VS sind je nach dem Schutz, dessen sie bedürfen, gemäß § 4 Abs. 2 des Sicherheitsüberprüfungsgesetzes in folgende Geheimhaltungsgrade einzustufen:

1. ***STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,***

2. ***GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,***

3. ***VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,***

4. ***VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.***

Die Einstufung einer Information als VS erfordert eine sorgfältige Einordnung unter eine der Voraussetzungen nach Nummern 1 bis 4. Es gehört zu den Aufgaben der oder des Geheimschutzbeauftragten (GB) (vgl. §§ 5, 42 Abs. 1 VSA), Fehleinstufungen vor allem durch Beratung entgegenzuwirken und bei vermutlich falsch eingestuften VS anderer Behörden den dortigen GB zu unterrichten.

Die hohen Anforderungen für eine STRENG-GEHEIM-Einstufung sind nur äußerst selten und in der Regel nur im Verteidigungsbereich oder im nachrichtendienstlichen und außenpolitischen Bereich erfüllt, wenn etwa die Verteidigungsfähigkeit gefährdet sein kann (z.B. bei einem Verrat von Informationen, der die Wirkung entscheidender Waffensysteme ganz oder weitgehend in Frage stellt).

Auch die Voraussetzungen für eine GEHEIM-Einstufung sind nicht allzu häufig erfüllt; die Gefährdung der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder bzw. das Zufügen eines schweren Schadens für die Interessen bei Preisgabe einer Information (vgl. Anlage 1, Abschn. 2.2) müssen im Einzelfall eingehend begründbar sein.

§ 4 Allgemeine Grundsätze

(1) Von einer VS dürfen nur Personen Kenntnis erhalten, die aufgrund ihrer Dienstpflichten von ihr Kenntnis haben müssen. Keine Person darf über eine VS umfassender oder eher unterrichtet werden, als dies aus dienstlichen Gründen unerlässlich ist. Es gilt der Grundsatz „Kenntnis nur, wenn nötig“.

(2) Jeder, dem eine VS anvertraut oder zugänglich gemacht worden ist, trägt ohne Rücksicht darauf, wie die VS zu seiner Kenntnis oder in seinen Besitz gelangt ist, die persönliche Verantwortung für ihre sichere Aufbewahrung und vorschriftsmäßige Behandlung sowie für die Geheimhaltung ihres Inhalts gemäß den Bestimmungen dieser VS-Anweisung.

(3) Der Bedrohung der VS durch Verlust der Vertraulichkeit, Verfügbarkeit[*1] und Integrität[2] ist mit Schutzmaßnahmen entsprechend dem Stand der Technik entgegenzuwirken. Diese sind entsprechend Anlage 5 zu dokumentieren.

Zu Absatz 1:
Der Grundsatz „Kenntnis nur, wenn nötig“ gilt für alle Geheimhaltungsgrade.

Bei VS-VERTRAULICH oder höher eingestuften VS ist zusätzliche Voraussetzung für eine Kenntnisnahme die Ermächtigung zum Zugang zu VS (vgl. § 10 Abs. 3 VSA); bei VS-NUR FÜR DEN DIENSTGEBRAUCH genügt für die Kenntnisnahme die dienstliche Notwendigkeit. Niemand ist allein aufgrund seines Amtes, Dienstgrades, seiner Stellung oder Ermächtigung berechtigt, Zugang zu VS zu erhalten. Auch nach dem Informationsfreiheitsgesetz besteht kein Anspruch auf Informationszugang zu VS (§ 3 Nr. 4 IFG). Dies sollte jedoch nicht zu ungerechtfertigter Einstufung von Vorgängen als VS verleiten, da mit Klagen von Antragstellern zu rechnen ist (siehe auch Erläuterung zu § 8 Abs. 1).

Zu Absatz 3:
Von vergleichbarer Bedeutung wie der Schutz der Vertraulichkeit ist die Absicherung des zuverlässigen Zugangs zu VS (Verfügbarkeit) und von deren Unversehrtheit (Integrität). Es muss z. B. verhindert werden, dass eine Anlage zu einer VS unbemerkt verändert oder gar entfernt werden kann. Um Schäden zu vermeiden, müssen alle Schutzmaßnahmen auf dem aktuellen Stand der Entwicklung gehalten werden. Nicht gemeint mit der Formulierung „Stand der Technik“ ist, dass auch immer sofort die neueste Technik verwendet werden muss, sondern dass bekannt gewordene Schwachstellen behoben werden. So sollen z. B. veraltete Schlösser ausgetauscht oder bei Computern laufend neue Kennungen für den Virenschutz und Patches für bekannt gewordene Sicherheitslücken der Programme eingespielt werden. Hierzu zählen auch Maßnahmen gegen neue Bedrohungen wie z.B. Penetrationstests (§ 39 Abs. 3).

§ 5 Verantwortung und Zuständigkeit

(1) Die Dienststellenleitung ist innerhalb ihres Zuständigkeitsbereiches für die ordnungsgemäße Arbeit mit VS (Kenntnisnahmen, Herstellung, Vervielfältigung, Verwaltung, elektronische Übertragung, Vernichtung oder anderweitige Verwendung) und die Durchführung der VS-Anweisung verantwortlich.

(2) Die Leitungen größerer Dienststellen können ihre Aufgaben nach der VS-Anweisung ganz oder teilweise auf einen Mitarbeiter oder eine Mitarbeiterin ihrer Dienststelle übertragen.

(3) Bei den Obersten Bundesbehörden, den größeren Bundesober- und -mittelbehörden und den entsprechenden bundesunmittelbaren öffentlich-rechtlichen Einrichtungen sind, wenn sie mit VS-VERTRAULICH oder höher eingestuften VS arbeiten, ein Geheimschutzbeauftragter oder eine Geheimschutzbeauftragte und eine zur Vertretung berechtigte Person zu bestellen. Andere VS verwaltende Behörden können Geheimschutzbeauftragte bestellen. Soweit dies nicht geschieht, nimmt die Dienststellenleitung die Aufgaben der Geheimschutzbeauftragten wahr.

(4) Geheimschutzbeauftragte haben in den Dienststellen für die Durchführung der VS-Anweisung zu sorgen und die Dienststellenleitungen in allen Fragen des Geheimschutzes zu beraten.

---

[*] Begriffsbestimmungen am Ende

(5) Geheimschutzbeauftragte haben ein unmittelbares Vortragsrecht bei der Dienststellenleitung.

(6) Dienststellen, die VS mit Informationstechnik (IT) verarbeiten, bestimmen verantwortliche Personen mit IT-Fachkenntnissen, z. B. IT-Sicherheitsbeauftragte, die die Geheimschutzbeauftragten bei der Umsetzung der VS-Anweisung unterstützen. Die Verantwortlichen mit IT-Fachkenntnissen sollen nicht zugleich Aufgaben von Systemadministratoren bei für VS eingesetzten IT-Systemen wahrnehmen und müssen in Bezug auf die VS-Anweisung besonders geschult sein. Sie haben ebenfalls ein unmittelbares Vortragsrecht bei der Dienststellenleitung. Werden Verantwortliche mit IT-Fachkenntnissen für Geheimschutzmaßnahmen nicht bestimmt, so verbleiben deren Aufgaben bei den Geheimschutzbeauftragten oder der Dienststellenleitung.

Zu Absatz 1:
Als Dienststellenleitung ist die Leiterin oder der Leiter einer Dienststelle (Minister oder Ministerin siehe § 6 Abs. 1 GGO), Präsident oder Präsidentin, Amtleiter oder Amtleiterin sowie dessen oder deren Vertretung anzusehen.
Die Fachaufsicht durch vorgesetzte Dienststellen bleibt unberührt.

Zu Absatz 2:
Die originären Aufgaben der oder des Geheimschutzbeauftragten (GB) werden durch die Aufgabenübertragung nicht berührt.

Die Verantwortung der Dienststellenleitung nach der VS-Anweisung soll nicht auf die Geheimschutzbeauftragten, sondern möglichst auf einen leitenden Mitarbeiter oder eine leitende Mitarbeiterin z.B. der Abteilungsleitung übertragen werden, damit bei möglichen Konflikten zwischen Geheimschutz- und anderen Interessen eine übergeordnete Entscheidungsinstanz erhalten bleibt.

Zu Absatz 3:
Bei VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS braucht ein GB nicht bestellt zu werden. Die Funktion des GB bei größeren Dienststellen sollte möglichst ein leitender Beamter oder Angestellter, möglichst Jurist, sein. Die Allgemeine Verwaltungsvorschrift des BMI zu § 3 SÜG regelt, dass zur Wahrung der Kontinuität und Wirksamkeit der Geheimschutzpraxis die Geheimschutzbeauftragten und ihre Mitarbeiter ihre Tätigkeit mehrere Jahre ausüben und besonders geschult sein sollen.
Zu Absatz 4:
Die oder der GB kann sich dazu nach Bedarf durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) fachlich beraten lassen (vgl. auch § 7 VSA).

Zu Absatz 5:
Soweit seitens der Dienststellenleitung keine diesbezüglichen speziellen Festlegungen getroffen worden sind, obliegt es den Geheimschutzbeauftragten, welches Mitglied der Dienststellenleitung informiert wird.
Das unmittelbare Vortragsrecht beim Dienstellenleiter oder der Dienststellenleiterin schließt das unmittelbare (schriftliche) Vorlagerecht ein.

Hat der Dienststellenleiter oder die Dienststellenleiterin die Aufgaben nach der VS-Anweisung auf einen Mitarbeiter oder eine Mitarbeiterin übertragen (vgl. § 5 Abs. 2 VSA), so bezieht sich das unmittelbare Vortragsrecht der oder des GB auf diese.

Zu Absatz 6:
Die Hauptaufgabe der Verantwortlichen mit IT-Fachkenntnissen besteht darin, für die Durchführung der VSA bei Verarbeitung von VS mit IT zu sorgen und den Geheimschutzbeauftragten in allen Fragen des IT-Geheimschutzes zu beraten. Aufgrund der Aufgabenübertragung sind die Verantwortlichen mit IT-Fachkenntnissen gegenüber den Geheimschutzbeauftragten für den Bereich IT-Geheimschutz verantwortlich. Im Allgemeinen wird von einer fachlichen Unterstellung der Verantwortlichen mit IT-Fachkenntnissen unter die Geheimschutzbeauftragten ausgegangen. Ist aufgrund besonderer Verhältnisse in der Dienststelle eine Unterstellung nicht zweckmäßig, so muss durch die Dienststellenleitung eine enge Zusammenarbeit gewährleistet werden.
Die Verantwortlichen mit IT-Fachkenntnissen haben auch ein unmittelbares Vortragsrecht bei der Dienststellenleitung. Vorschläge und Bedenken können sie unmittelbar der Leitung vortragen, wenn sie sich nicht mit den Geheimschutzbeauftragten einigen konnten und wegen der besonderen Bedeutung der Angelegenheit eine Entscheidung der Leitung für erforderlich halten.
Durch die Wahrnehmung dieser Funktion dürfen keine wesentlichen Interessenkonflikte (z.B. Eigenkontrolle) zu anderen Aufgaben des Funktionsträgers auftreten.

Da IT-Geheimschutz ein breites Themenfeld ist, dessen konzeptionelle Beherrschung sowohl Fachwissen als auch Erfahrung voraussetzt, sollten die Verantwortlichen mit IT-Fachkenntnissen auch über Fachwissen im Geheimschutz verfügen. Um dies zu gewährleisten, bedarf es einer entsprechenden Fortbildung.

§ 6 Geheimschutzdokumentation

(1) Jede Dienststelle, die nicht nur gelegentlich mit VS arbeitet, hat für eine Geheimschutzdokumentation zu sorgen, in der alle wesentlichen Konzepte, Vorschriften und dienststellenspezifischen Maßnahmen zum Zwecke des Geheimschutzes entsprechend Anlage 5 dokumentiert werden.

(2) Die Geheimschutzdokumentation ist bei geheimschutzrelevanten Änderungen zu aktualisieren und soll bei Sicherheitsvorkommnissen, mindestens aber alle zwei Jahre auf Aktualität, Vollständigkeit und Erforderlichkeit bestehender und noch zu treffender Geheimschutzmaßnahmen überprüft werden.

(3) Die Dokumentation kann elektronisch geführt werden. Sofern die Arbeit mit VS persönlich zugeordnet werden muss, sind entsprechende technische Maßnahmen nach § 18 Abs. 2 zu treffen. Diese müssen eine sichere Zuordnung zu Personen erlauben und können insbesondere mittels fortgeschrittener oder qualifizierter elektronischer Signatur[3] erfolgen.

§ 7 Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik

(1) Bei der Durchführung der VS-Anweisung wirkt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit. Es berät Dienststellen, die mit VS arbeiten, und kann sich im Einvernehmen mit der zuständigen Obersten Bundesbehörde über die Handhabung der VS-Anweisung unterrichten. Die Mitwirkung umfasst auch technische Prüfungen und Schulung. Das BSI kann sich dabei zu seiner Unterstützung anderer Stellen bedienen; dies bedarf bei Einbeziehung privater Stellen in jedem Einzelfall vorher der Billigung des Bundesministeriums des Innern. Im Bereich des Bundesministeriums der Verteidigung nimmt das Amt für den Militärischen Abschirmdienst im Benehmen mit dem BSI diese Aufgaben wahr.

(2) Das BSI gibt zur Umsetzung dieser Anweisung Hinweise zum Schutz vor Bedrohungen des Geheimschutzes und zur Methodik von Schutzmaßnahmen für VS heraus. Diese bedürfen der Billigung des Bundesministeriums des Innern.

(3) Das Bundesamt für Verfassungsschutz, das Amt für den Militärischen Abschirmdienst und der Bundesnachrichtendienst teilen nachrichtendienstliche Erkenntnisse, die für den materiellen Schutz von Verschlusssachen von Bedeutung sein können, dem BSI unverzüglich mit. Sofern sich die Erkenntnisse auf den Geheimschutz in der Wirtschaft beziehen, ist das Bundesministerium für Wirtschaft und Technologie unverzüglich zu informieren.

Zu Absatz 1:
Die Mitwirkung des BSI betrifft alle Gebiete des materiellen Geheimschutzes, nicht nur Informationstechnik. Sie erfolgt durch Beratung und durch Schulung der Geheimschutzbeauftragten sowie ihrer Mitarbeiter und ist insbesondere darauf gerichtet, im Geltungsbereich der VSA durchgängig ein qualitativ hohes Niveau des materiellen Geheimschutzes zu bewirken. Vor allem bei technischen Prüfungen durch das BSI sind das Fachwissen und die z. T. erforderliche Technik in anderen Dienststellen normalerweise nicht vorhanden.
Das Amt für den Militärischen Abschirmdienst wirkt gemäß § 1 Abs. 3 Nr. 2 MAD-Gesetz bei technischen Maßnahmen zum Schutz von VS im Geschäftsbereich des Bundesministeriums für Verteidigung mit.

Zu Absatz 2:
Die Hinweise werden in Form von technischen Leitlinien des BSI herausgegeben.

II. Behandlung von VS und organisatorische Maßnahmen

§ 8 Einstufung in Geheimhaltungsgrade

(1) Die eine VS herausgebende Stelle bestimmt über die Notwendigkeit der VS-Einstufung und den Geheimhaltungsgrad. Von einer Einstufung als VS ist nur Gebrauch zu machen, soweit dies notwendig ist. § 9 Abs. 1 und 2 sowie die Hinweise zur Einstufung von VS in Anlage 1 sind zu beachten.

(2) ***Zur Arbeitserleichterung und einheitlichen Praxis kann die Dienststellenleitung Richtlinien zur Einstufung von Verschlusssachen für häufiger vorkommende Fälle festlegen.***

Zu Absatz 1:
Der einer VS zugewiesene Geheimhaltungsgrad darf nicht ohne Zustimmung der herausgebenden Stelle geändert oder aufgehoben werden (vgl. § 9).
Herausgebende Stelle ist innerbehördlich die zuständige Organisationseinheit, außerbehördlich ist es die Dienststelle. vgl. auch Erläuterungen zu § 3 VSA.
Ziel ist es, die tatsächlichen geheimhaltungsbedürftigen Informationen des Staates optimal zu schützen. Ungerechtfertigte oder zu hohe VS-Einstufungen führen zu einer Verwässerung des Geheimschutzes und zu mangelnder Akzeptanz der Maßnahmen des Geheimschutzes insgesamt. Dabei ist zu berücksichtigen, dass
mit dem Sicherheitsüberprüfungsgesetz die Voraussetzungen für eine VS-Einstufung gesetzlich vorgeben werden (vgl. § 4 SÜG) und
die VS-Einstufung in VS-VERTRAULICH oder höher bei allen mit der VS befassten Personen aufwendige, mit Eingriffen in die Grundrechte der Beschäftigten verbundene Sicherheitsüberprüfungen zur Folge hat. Außerdem sind aufwendige Schutzmaßnahmen erforderlich.

Zu Absatz 2:
Der Hinweis auf die Dienstellenleitung schließt übergreifende Regelungen innerhalb einer Organisationseinheit ein (z. B. "Rahmenanweisung zur VS-Einstufung in der Bundespolizei")

§ 9 Änderung und Aufhebung der VS-Einstufung

(1) Die herausgebende Stelle oder deren Rechtsnachfolger hat den Geheimhaltungsgrad einer VS zu ändern oder aufzuheben, sobald die Gründe für die bisherige Einstufung sich ändern oder weggefallen sind. Von der Änderung hat die herausgebende Stelle oder deren Rechtsnachfolger alle Empfänger der VS schriftlich oder per E-Mail mit qualifizierter elektronischer Signatur oder durch vergleichbar sichere Maßnahmen zu benachrichtigen. Eine Heraufstufung von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufter VS ist nur zulässig, wenn eine Benachrichtigung aller Empfänger der ursprünglichen VS sichergestellt ist.

(2) Ist die Einstufung einer VS von einem bestimmten Zeitpunkt ab oder mit dem Eintritt eines bestimmten Ereignisses nicht mehr oder nicht mehr im ursprünglichen Umfange erforderlich, so ist dies deutlich erkennbar auf der VS oder zugehöriger Dokumentation zu vermerken.

(3) Die VS-Einstufung ist nach 30 Jahren aufgehoben, sofern auf der VS keine kürzere oder längere Frist bestimmt ist. Die Frist beginnt am 1. Januar des auf die Einstufung folgenden Jahres, sie wird durch Änderungen der Einstufung nicht verändert. Für die Bestimmung einer längeren Frist als 30 Jahre gilt Folgendes:

1. ***Die Frist kann um höchstens 30 Jahre verlängert werden. Von der Fristverlängerung ist nur der notwendige Gebrauch zu machen. Sie ist auf der VS oder einem Beiblatt schriftlich zu begründen.***

2. ***Die Verlängerung der Frist kann für einzelne VS oder pauschal für die in einem bestimmten Bereich entstehenden VS verfügt werden. Sie bedarf der Zustimmung der zuständigen Obersten Bundesbehörde.***

3. ***Auf der ersten Seite des Entwurfs der VS und auf allen Ausfertigungen ist ein Hinweis auf die verlängerte Frist anzugeben: „Die VS-Einstufung endet mit Ablauf des Jahres...“. Bei anderen***

Darstellungsformen von VS (z. B. Geräten) ist sinngemäß zu verfahren, z. B. Kennzeichnung in der zugehörigen Dokumentation.

4. ***Die nachträgliche Fristverlängerung ist als Änderung entsprechend Absatz 1 zu behandeln. Befinden sich die VS im Geheimarchiv des Bundesarchivs, ist auch das Bundesarchiv entsprechend zu benachrichtigen.***

(4) Bei zum Zeitpunkt des Inkrafttretens der VS-Anweisung mehr als 30 Jahre alten VS kann die herausgebende Stelle oder deren Rechtsnachfolger eine Fristverlängerung der VS-Einstufung entsprechend Absatz 3 Nr. 1 bis 4 bestimmen. Die zuständige Oberste Bundesbehörde kann für die Prüfung von Fristverlängerungen pauschal eine Übergangsfrist von längstens 5 Jahren festlegen, in der diese VS zunächst eingestuft verbleiben.

(5) Absatz 3 gilt nicht für VS-Einstufungen ausländischer und zwischenstaatlicher Stellen. Ihre VS-Einstufung kann nur von der herausgebenden Stelle geändert oder aufgehoben werden, sofern nicht zwischenstaatliche Vereinbarungen ein abweichendes Verfahren regeln.

Zu Absatz 1:
Besteht Anlass zu der Annahme, dass die Gründe für die bisherigen Einstufungen einer VS weggefallen sind, so sollte möglichst eine völlige Aufhebung der VS-Einstufung, zumindest aber (bei höher eingestuften VS) eine Herabstufung auf VS-NUR FÜR DEN DIENSTGEBRAUCH erfolgen. Damit entfällt der mit dem Schutz der VS verbundene Verwaltungsaufwand ganz oder wird auf ein Minimum reduziert.
Die Aufhebung der VS-Einstufung von Informationen, auch „Offenlegung“ genannt, bedeutet nicht automatisch, dass diese "veröffentlicht" werden können. Sie unterliegen danach immer noch der allgemeinen Verschwiegenheitspflicht.
Eine vergleichbar sichere Maßnahme wie die Verwendung einer qualifizierten elektronischen Signatur ist z. B. die Verschlüsselung und fortgeschrittene elektronische Signatur mit einem vom BSI zugelassenen Kryptoprodukt.

Zu Absatz 2:
Ohne Kennzeichnung einer Frist ist eine VS-Einstufung nach 30 Jahren aufgehoben (vgl. Abs. 3). Wenn die Voraussetzungen für eine befristete Einstufung vorliegen, so ist diese Form der Einstufung anzuwenden. Dies kann z. B. der Fall sein, um die Vorbereitung von polizeilichen Maßnahmen vor unbefugter Kenntnisnahme zu schützen, die Maßnahmen selbst oder deren Ergebnisse aber später öffentlich sind (z.B. im Gerichtsverfahren).
Zu Absatz 3:
Auf VS, für deren Einstufung eine längere Frist als 30 Jahre bestimmt wurde, gleichgültig ob von der Herausgabe an oder gemäß nachträglicher Verlängerung, trifft Absatz 4 nur zu, wenn die Frist bereits abgelaufen ist. Beispiel: Schon bei der Herausgabe einer VS kann eine längere Frist als 30 Jahre festgelegt werden. Die Bestimmung einer längeren Frist richtet sich auch in diesem Fall immer nach Absatz 3, Nummer 1-4.
So kommen Quellenschutz für Zeugen bzw. deren Familien oder noch benutzte Technik in Frage, nicht aber Kapazitätsprobleme der Dienststellen.
Eine Benachrichtigung aller Empfänger der VS über die Verlängerung der VS-Einstufung ist insoweit zwingend erforderlich, da ansonsten der Empfänger nach Ablauf der Frist von einer Offenlegung ausgehen kann.

Zu Absatz 4:
Der Absatz regelt den Tatbestand für VS mit aufgehobener Einstufung nach Absatz 3 Satz 1 und 2. Die pauschale Fristverlängerung ermöglicht eine Übergangsfrist von maximal 5 Jahren, ohne dass eine Festlegung über die Verlängerung der Einstufung erforderlich ist. Für VS, deren Einstufung bereits nach Abs. 3 verlängert wurde und nicht abgelaufen ist, trifft Abs. 4 nicht zu.
Im Weiteren trifft diese Regelung nicht für VS zu, bei denen nach dem 1. Juni 2006 die Frist von 30 Jahren überschritten wurde und keine längere Frist bestimmt wurde.

§ 10 Zugang zu VS und Tätigkeiten mit der Möglichkeit, sich Zugang zu VS zu verschaffen

(1) VS-VERTRAULICH oder höher eingestufte VS dürfen Dritten nur mit Zustimmung der zuständigen Organisationseinheit (z. B. Referat, Abteilung) zugänglich gemacht werden.

(2) In Räumen, in denen VS-VERTRAULICH oder höher eingestufte VS verwaltet werden (z. B. VS-Registratur), dürfen nur Personen tätig sein, die entsprechend ermächtigt sind.

(3) Bevor eine Person Zugang zu VS-VERTRAULICH oder höher eingestuften VS erhält, ist sie gemäß dem Sicherheitsüberprüfungsgesetz und den allgemeinen Verwaltungsvorschriften zur Durchführung von Sicherheitsüberprüfungen zu überprüfen und zum Zugang zu VS zu ermächtigen. Zugang zu solchen VS haben Personen, die diese bearbeiten oder anderweitig Kenntnis von ihrem Inhalt erhalten.

(4) Bevor einer Person eine Tätigkeit übertragen wird, bei der sie sich Zugang zu VS-VERTRAULICH oder höher eingestuften VS verschaffen kann, muss sie gemäß dem Sicherheitsüberprüfungsgesetz und den allgemeinen Verwaltungsvorschriften zur Durchführung von Sicherheitsüberprüfungen überprüft und für eine solche Tätigkeit zugelassen worden sein. Zugang zu VS können sich Personen verschaffen, die

1. ***als Boten oder Kuriere VS befördern,***
2. ***VS-Verwahrgelasse oder Sicherheitsbereiche bewachen,***
3. ***in einem Sicherheitsbereich tätig sind,***
4. ***Alarmanlagen zum Schutze von VS installieren, warten oder instand setzen,***
5. ***Schlüssel oder Zahlenkombinationen zu VS-Verwahrgelassen, VS-Schlüsselbehältern oder Alarmanlagen zum Schutze von VS verwalten,***
6. ***im Rahmen ihrer Tätigkeit an technischen Systemen oder Komponenten, die für die Verarbeitung von VS-VERTRAULICH oder höher eingestuften VS eingesetzt sind, wesentliche Maßnahmen zum Geheimschutz unwirksam machen oder unbefugten Zugriff auf diese VS erlangen können.***

(5) Das Erfordernis für Ermächtigungen und Zulassungen in militärischen Sicherheitsbereichen regelt das Bundesministerium der Verteidigung.

Zu Absatz 1:
Als zuständige Organisationseinheit im Sinne dieses Abschnitts gilt der Herausgeber der VS oder die Organisationseinheit des Empfängers der VS, die mit der Bearbeitung des Sachverhalts (durch die Dienststellenleitung) beauftragt wurde.
Begründung: siehe Erläuterungen zu § 5 Abs.1

Zu Absatz 2:
Die Bestimmung ist nur anzuwenden, soweit VS auch tatsächlich verwaltungsmäßig bearbeitet werden. Sie erstreckt sich nicht auf die Zeiten, in denen die VS unter Verschluss sind.

Zu Absatz 3:
Unter "anderweitig Kenntnis von ihrem Inhalt erhalten" fällt z.B. das Herstellen, Mitzeichnen, Mitprüfen, Vervielfältigen, Versenden, ungesicherte Befördern oder Vernichten von VS.

Nach § 2 SÜG kann auf eine Sicherheitsüberprüfung verzichtet werden, wenn bereits eine gleich- oder höherwertige Sicherheitsüberprüfung (z.B. von einem anderem Bundesressort, einem Bundesland oder einem anderen Staat) durchgeführt wurde.

Bei VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH bedarf es einer Überprüfung und Ermächtigung oder Zulassung nicht; hier genügt die dienstliche Notwendigkeit zum Zugang.
Bei Privatpersonen ist im Einzelfall jedoch eine Verpflichtung gemäß Muster 1 Anlage 3 angezeigt. Siehe hierzu Anlage 6, Ziffer 4.5 VSA.

Zu Absatz 4:
Als Person, die unter die Ziffer 6 fallen sind u. a. IT-Wartungspersonal oder Administratoren von VS-IT-Systemen anzusehen. Sie sind sinngemäß wie VS-Verwalter zu betrachten, für ihre Tätigkeit genügt jedoch die Zulassung für eine Tätigkeit mit Zugang zu VS.

§ 11 Ermächtigungen und Zulassungen

(1) Ermächtigungen und Zulassungen sowie ihre Erweiterung, Einschränkung oder Aufhebung nehmen die Dienststellenleitung oder in deren Auftrag der oder die Geheimschutzbeauftragte oder besonders

beauftragte Mitarbeiter vor. Ermächtigungen und Zulassungen sind auf das notwendige Maß zu beschränken. Sie erlöschen spätestens bei Ausscheiden der betroffenen Person aus der Dienststelle. Die VS-Registratur ist über Ermächtigungen und Zulassungen sowie deren Erweiterung, Einschränkung, Aufhebung oder Erlöschen im erforderlichen Umfange zu unterrichten.

(2) Die ermächtigten oder für eine Tätigkeit nach § 10 Abs. 4 zugelassenen Personen sind über die wesentlichen Geheimschutzbestimmungen, Anbahnungs- und Anwerbemethoden fremder Nachrichtendienste und sonstige Gefährdungen sowie über die Möglichkeiten straf- und disziplinarrechtlicher Ahndung oder arbeitsrechtlicher Maßnahmen bei Verstößen gegen die Geheimhaltungsvorschriften zu unterrichten. Die Unterrichtung ist mindestens alle 5 Jahre zu wiederholen. Den ermächtigten Personen sind gegen Empfangsbestätigung die für ihre Tätigkeit erforderlichen Vorschriften zum Schutze von VS auszuhändigen oder anderweitig zugänglich zu machen.

(3) Die in den Absätzen 1 und 2 genannten Maßnahmen sind zu dokumentieren (z. B. Muster nach Anlage 3 oder elektronisch). Sie sind, soweit der Dienststellenleiter oder die Dienststellenleiterin persönlich betroffen ist, von der vorgesetzten Behörde durchzuführen.

Zu Absatz 1:
Ermächtigungen oder Zulassungen können bei Bedarf auch mündlich vorab ausgesprochen werden. Sie gelten grundsätzlich auch für NATO- und andere nichtdeutsche VS des vergleichbaren Geheimhaltungsgrades (vgl. Anlage 4).

Voraussetzung für die Ermächtigung oder Zulassung ist eine Sicherheitsüberprüfung, die nur mit Zustimmung des Betroffenen erfolgen darf, soweit gesetzlich nichts anderes bestimmt ist (vgl. § 2 SÜG).

Für folgende Personengruppen gelten bezüglich der Ermächtigung Besonderheiten:
- Dienststellenleiter oder Dienststellenleiterin

Sie werden durch die vorgesetzte Behörde ermächtigt (vgl. Absatz 3).

- Privatpersonen

Sie werden gemäß Anlage 6 Abschn. 4.5 zur Geheimhaltung verpflichtet (Anlage3, Muster 1). Näheres siehe dazugehörige Erläuterungen.

- Personen unter 21 Jahren

Eine Ermächtigung ist frühestens ab Vollendung des 16. Lebensjahr möglich (§ 2 Abs. 1 SÜG); sie sollte i.d.R. aber nicht vor Vollendung des 18. Lebensjahres (Eintritt der Volljährigkeit) erfolgen.
Im Hinblick darauf, dass das Jugendstrafrecht im Falle von Geheimnisverrat auch bei volljährigen Personen (= Heranwachenden) noch Anwendung finden kann (§ 1 Abs. 2 JGG), sollte eine Ermächtigung zum Zugang zu STRENG GEHEIM nicht vor Vollendung des 21. Lebensjahres erfolgen.

- Ausländische Staatsangehörige

Voraussetzung für eine Ermächtigung von ausländischen Staatsangehörigen ist, dass (ggf. in Zusammenarbeit mit dem Heimatland) eine entsprechende Sicherheitsüberprüfung durchgeführt werden kann.

Eine Ermächtigung zu NATO-VS ist grundsätzlich nur für ausländische Staatsangehörige aus einem NATO-Staat möglich. Ausnahmen regeln die entsprechenden Hinweise zum NATO-Dokument C-M (2002) 49.

Vgl. auch § 2 Abs. 3 Nr. 3 SÜG.

- Richter

Die verfassungsrechtliche Stellung der Richter, soweit sie Aufgaben der Rechtsprechung wahrnehmen (Art. 103 Abs. 1 GG) hat zu der Ausnahme von einer Sicherheitsüberprüfung im SÜG geführt (Vgl. § 2 Abs. 3 Nr. 2 SÜG). Die Ausnahme bezieht sich nur auf nationale VS, Für die Kenntnisnahme von VS, die z.B. von der NATO, der EU

oder einem anderen Staat herausgegeben wurden, müssen sich auch diese Personen einer entsprechenden Sicherheitsüberprüfung unterziehen.
Sofern Richter Verwaltungsaufgaben erfüllen und dabei Zugang zu Verschlusssachen haben müssen, sind sie einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz zu unterziehen; privilegiert ist nur die rechtsprechende Tätigkeit des Richters.

- Mitglieder der Verfassungsorgane des Bundes (Abgeordnete, Mitglieder des Bundesrates, Richter am Bundesverfassungsgericht, Minister, Parlamentarische Staatssekretäre)

Die verfassungsrechtliche Stellung der Mitglieder der Verfassungsorgane nimmt diesen Personenkreis von der unmittelbaren Geltung des SÜG aus (vgl. § 2 Abs. 3 Nr. 1 SÜG). Daher bedarf es für diesen Personenkreis keiner Sicherheitsüberprüfung.
Diese Ausnahmeregelung bezieht sich ausschließlich auf nationale VS. Für die Kenntnisnahme von VS, die z.B. von der NATO, der EU oder einem anderen Staat herausgegeben wurden, müssen sich auch diese Personen einer entsprechenden Sicherheitsüberprüfung unterziehen.

Die Ermächtigungen und Zulassungen sind im Kontext zu der durchgeführten Sicherheitsüberprüfung zu sehen. Das Sicherheitsüberprüfungsgesetz fordert im Grunde eine Sicherheitsbeurteilung bezogen auf die jeweils ausgeübte oder auszuübende Tätigkeit.
Satz 2 von § 11 Abs. 1 beinhaltet auch, dass nicht mehr oder nur noch in geringerem Umfang erforderliche Ermächtigungen oder Zulassungen aufzuheben oder einzuschränken sind.

Gemäß Satz 3 erlischt die Ermächtigung oder Zulassung spätestens beim Ausscheiden aus der Dienststelle, welche die Ermächtigung oder Zulassung ausgesprochen hat. Die Dienststelle kann verfügen, dass die Ermächtigung oder Zulassung auch bei anderen Anlässen (z.B. Umsetzung innerhalb der Dienststelle) erlischt.

Siehe auch Erläuterungen zu § 25 VSA.

Zu Absatz 2:
Die Unterrichtung obliegt der oder dem Geheimschutzbeauftragten oder einer von ihr oder ihm beauftragten fachkundigen Person.
Die Möglichkeit der unmittelbaren Kenntnisnahme über den Inhalt der VSA ist für den VS-Ermächtigten sicherzustellen (z. B. in elektronischer Form im Intranet). Das gilt auch für ergänzende Hinweise und Richtlinien sowie ggf. hausinterne Geheimschutzvorschriften und -dienstanweisungen.
Zu den Aufgaben der oder des Geheimschutzbeauftragten gehört, sich über die aktuellen und relevanten Geheimschutzangelegenheiten kundig zu machen. Hierbei wird er durch entsprechende Informationen des BfV, des BSI und der Dienststellenleitung unterstützt.

Zu Absatz 3:
Dienststellenleiter(innen) bedürfen für den Zugang zu VS ebenfalls einer Ermächtigung; bezüglich Minister(in), siehe Erläuterungen zu Absatz 1.

§ 12 Veränderungen von Ermächtigungen und Zulassungen

(1) Personen, deren Ermächtigung aufgehoben wird oder erlischt, sind verpflichtet, VS sowie persönliche Vermerke und Aufzeichnungen, die ihrer Art nach eine entsprechende Behandlung erfordern, unaufgefordert abzuliefern und darüber eine Erklärung zu unterschreiben (Anlage 3, Muster 4). Dies gilt entsprechend im Falle der Einschränkung der Ermächtigung.

(2) Bei Einschränkung, Aufhebung oder Erlöschen der Ermächtigung oder Zulassung ist die betroffene Person auf das Fortbestehen der Geheimschutzpflichten hinzuweisen.

(3) Die nach dem Ausscheiden aus dem Dienst bestehende Verpflichtung zur Wahrung aller Dienstgeheimnisse erstreckt sich in besonderem Maße auf die aus VS gewonnenen Kenntnisse.

Zu Absatz 1:
Die Verpflichtung gilt für Personen, die gemäß § 10 Abs. 3 VSA zum Zugang zu VS ermächtigt waren. VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS können von der Erklärung ausgenommen werden, soweit die Person aus dienstlichen Gründen weiterhin damit befasst werden muss. Vgl. auch Erläuterungen zu § 11 Abs. 1

§ 13 Allgemeine Dienstpflichten zum Schutze von VS

(1) Erörterungen über VS in Gegenwart Unbefugter und in der Öffentlichkeit, insbesondere in Verkehrsmitteln, Gaststätten und Kantinen, sind zu unterlassen.

(2) Niemand darf sich dadurch zur Preisgabe von VS an andere Personen verleiten lassen, dass diese sich über den Vorgang unterrichtet zeigen.

(3) Personen, die zum Zugang zu VS ermächtigt sind oder eine Tätigkeit ausüben, bei der sie sich Zugang zu VS verschaffen können (§10 Abs. 4), ist der Betrieb von privaten Bild- und Tonaufzeichnungsgeräten, privater Informationstechnik und mobilen Telekommunikations-Endgeräten (dies sind z. B. Mobiltelefone, Datenträger[4], PDA[5] usw.) am Arbeitsplatz grundsätzlich untersagt. Die Geheimschutzbeauftragten – bei Konferenzen, Sitzungen und Besprechungen die verantwortlichen Leiter - können spezielle Regelungen festlegen, um den Betrieb zu erlauben oder das Mitbringen zu untersagen.

Zu Absatz 3:
Die Benutzung mobiler Telefone und sonstiger Informationstechnik (Laptop, PDA, MP3-Player) ist inzwischen im privaten Bereich stark verbreitet. Vor allem für Dienststellen, in denen seltener mit höher eingestuften VS gearbeitet wird, war daher gegenüber vorherigen Vorschriften eine Regelung erforderlich, die sich stärker an den Bedürfnissen der Praxis orientiert. Das frühere Verbot des Mitbringens solcher Geräte pauschal für alle ermächtigten Personen wurde durch eine flexible Regelung mit der Möglichkeit einer hausinternen Festlegung durch die Geheimschutzbeauftragten ersetzt. Die Formulierung "grundsätzlich" lässt Spielraum für eine angemessene Verfahrensweise. So können z. B. im persönlichen Umfeld des Ermächtigten zeitlich begrenzte Gründe vorliegen (z. B. krankes Kind) die den Betrieb eines privaten Handys am Arbeitsplatz begründen. Auch ist eine generelle Genehmigung des Betriebes von privaten Mobilfunktelefonen denkbar, sofern die Geräte keine Kamerafunktion aufweisen und nur gelegentlich höher eingestufte VS bearbeitet werden müssen. Grundsätzlich ist jedoch zu beachten, dass ein reguläres Telefon ohnehin normalerweise am Arbeitsplatz vorhanden ist.

§ 14 Herstellung von VS

(1) Arbeiten zur Herstellung von VS-VERTRAULICH oder höher eingestuften VS sind nur an den hierfür bestimmten Stellen zulässig. Die Zahl der hergestellten Ausfertigungen und evtl. angefallenes VS-Zwischenmaterial sind durch Unterschrift der Beteiligten auf dem Entwurf oder dem Auftragsformular oder mit qualifizierter elektronischer Signatur oder durch vergleichbar sichere Maßnahmen in einem Protokoll zu bestätigen.

(2) Bei STRENG GEHEIM oder GEHEIM eingestuften VS ist jede Ausfertigung mit einer laufenden Nummer zu versehen, die bei VS-Schriftstücken auf den oberen Rand der ersten Seite der Ausfertigung zu setzen ist. Bei anderen Darstellungsformen der VS ist sinngemäß zu verfahren. Ferner ist auf dem Schriftstück zu vermerken, welche Ausfertigung der einzelne Empfänger erhält.

(3) Elektronisch vorliegende VS-VERTRAULICH oder höher eingestufte VS sind nach der Bearbeitung mit einem vom BSI für den Geheimhaltungsgrad zugelassenen Programm kryptiert zu speichern oder entsprechend § 17 aufzubewahren.

Zu Absatz 1:
Soweit die Herstellung von VS durch Nutzung von Informationstechnik erfolgt, findest dies im Regelfall in einem VS-IT-Raum statt (siehe § 29 VSA).
Eine VS kann auch nur als Entwurf i.S. von Satz 2 erstellt werden (z.B. ein interner Vermerk).
Ein Entwurf darf grundsätzlich nur in einer Ausfertigung erstellt werden; andernfalls (z.B. bei besonders eilbedürftigen Mitzeichnungen) muss die Anzahl der Ausfertigungen auf dem Entwurf vermerkt sein.
Soweit Personen, die mit Vervielfältigungsarbeiten befasst sind (üblicher Weise VS-Verwalter), der Entwurf nicht vorliegt, kann die Beteiligung auch auf einem Auftragsformular vermerkt werden.

Zu Absatz 3:

Die Verschlüsselung mit einem vom BSI für den betreffenden Geheimhaltungsgrad zugelassenen Kryptosystem ist eine ausreichende Maßnahme zum Schutz der Vertraulichkeit und Integrität der VS. Zusätzlich sind Maßnahmen zur Verfügbarkeit der VS zu berücksichtigen.

§ 15 Vervielfältigung von VS

(1) Für Vervielfältigungen (Kopien, Abdrucke, Abschriften, Auszüge, Nachbauten usw.) gilt § 14 sinngemäß.

(2) Vervielfältigungen bedürfen bei STRENG GEHEIM eingestuften VS der Zustimmung der herausgebenden Stelle; die Zustimmung ist auf der VS zu vermerken. Bei GEHEIM oder VS-VERTRAULICH eingestuften VS entscheidet der Empfänger nach Prüfung der Notwendigkeit und unter Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig" über die Zulässigkeit der Vervielfältigung, soweit die herausgebende Stelle auf der VS nichts anderes verfügt hat.

(3) Anzahl und Empfänger der Vervielfältigungen von VS-VERTRAULICH oder höher eingestuften VS sind auf der zu vervielfältigenden VS oder auf einem Auftragsformular zu verfügen. Die Vervielfältigungen sind unverzüglich zu registrieren und erhalten bei STRENG GEHEIM oder GEHEIM eingestuften VS eine fortlaufende Nummer.

(4) Vervielfältigungen von VS-VERTRAULICH oder höher eingestuften VS, die durch Versand über elektronische Medien entstehen, sind unverzüglich beim Empfänger zu registrieren.

(5) In Dienststellen, in denen häufig VS-VERTRAULICH oder höher eingestufte VS hergestellt oder vervielfältigt werden, sollen hierfür bestimmte Stellen mit ermächtigtem Bedienungspersonal festgelegt werden. Soweit dies nicht geschieht, sind Vervielfältigungen dieser VS durch die VS-Registratur zu fertigen. Die Arbeiten sind in Gegenwart einer weiteren entsprechend ermächtigten Person durchzuführen (Vier-Augen-Prinzip).

(6) Bei Nutzung von Kopiergeräten und Multifunktionsgeräten mit nichtflüchtigem Speicher [6] sind die Festlegungen in § 26 Abs. 4 sowie der Hinweise des BSI zu berücksichtigen.

Zu Absatz 1:
Vervielfältigungen von VS, auch elektronische Dateien oder Auszüge davon ab VS-VERTRAULICH oder höher, werden grundsätzlich von der VS-Registratur hergestellt. Werden Inhalte einer VS-Datei zur Erstellung einer neuen VS-Datei benötigt, ist wie unter § 14 Abs. 1 und 2 beschrieben zu verfahren. Die ursprüngliche VS-Datei darf nicht verändert werden.

Zu Absatz 2:
Die Zustimmung kann schriftlich oder mündlich eingeholt werden.
Nach Satz 2 hat der Herausgeber auch bei VS des Geheimhaltungsgrades VS-VERTRAULICH oder GEHEIM die Möglichkeit, die Herstellung von Vervielfältigungen zu untersagen bzw. von seiner Zustimmung abhängig zu machen.

Zu Absatz 3:
Das Auftragsformular ist durch die ausführende Stelle an die VS-Registratur zu leiten. Damit soll ein Nachweis über die Kopien gewährleistet werden. Andernfalls könnte z.B. jemand Kopien herstellen lassen und anschließend das Auftragsformular vernichten oder die Kopien unbemerkt an Unbefugte weitergeben.
Werden nur einzelne Seiten vervielfältigt und ist die Ausfertigungsnummer (ggf. mit ergänzender Kopiernummer, vgl. Beispiel 6b zur VSA) darauf nicht bereits enthalten, so ist sie nachzutragen. Dies ist nur dann entbehrlich, wenn die vervielfältigten Seiten ausnahmsweise zur Herstellung einer neuen (anderen) VS verwendet werden (z.B. bei Änderung umfangreicher Pläne).
Durch die unverzügliche Registrierung von Vervielfältigungen soll eine Kontrollmöglichkeit über Kenntnisnahme und Verbleib der VS geschaffen werden.

Zu Absatz 5:
Kopier- oder Druckarbeiten zur Herstellung von VS-VERTRAULICH oder höher eingestuften VS sind nur an den hierfür bestimmten Stellen zulässig (z. B. zentrale Kopierstelle, Administrator bei Fertigung von z. B. CD oder

DVD usw.). Die Zahl der hergestellten Ausfertigungen und evtl. angefallenes VS-Zwischenmaterial sind durch Unterschrift der Beteiligten auf dem Entwurf oder dem Auftragsformular zu bestätigen.
Das Vieraugenprinzip ist auch bei Fertigung von Vervielfältigungen durch VS-Verwalter oder entsprechend Beauftragte sicherzustellen.

§ 16 Kennzeichnung von VS

(1) Der Geheimhaltungsgrad ist gut sichtbar ungekürzt in Großbuchstaben und so auf der VS anzubringen, dass er sich deutlich von der übrigen Beschriftung abhebt. Befinden sich in einem Behältnis oder auf einem Datenträger mehrere VS, so ist entsprechend der höchsten Einstufung zu kennzeichnen. Im Einzelnen gilt die Anlage 2 zur VS-Anweisung.

(2) ***Bei der Darstellung von VS auf Sichtgeräten soll sich der Geheimhaltungsgrad auf jeder Dokumentenseite deutlich vom dargestellten Inhalt abheben (z. B. durch größere Schrift und Fettdruck). Absatz 1 gilt entsprechend.***

(3) ***Wird der Geheimhaltungsgrad einer VS geändert oder aufgehoben, so ist die VS-Kennzeichnung durch die verantwortlichen VS-Bearbeiter oder VS-Registraturen der herausgebenden Stelle und des Empfängers zu ändern oder zu streichen. Die Änderung oder Streichung ist mit Namenszeichen und Datum der handelnden Person zu versehen und im VS-Bestandsverzeichnis zu vermerken. Bei mobilen Datenträgern und gebundenem Schriftgut erfolgt die Änderung oder die Streichung auf dem Objekt, dem Einband oder dem Titelblatt.***

(4) ***Lässt die Beschaffenheit einer VS die Kennzeichnung nach den Absätzen 1 bis 3 nicht zu (z. B. bei miniaturisierten Bauelementen), ist sinngemäß zu verfahren oder die Kennzeichnung auf der zugehörigen Dokumentation zu vermerken.***

(5) ***VS-Zwischenmaterial, das nicht an Dritte weitergegeben und das unverzüglich vernichtet wird, braucht nicht als VS gekennzeichnet und nicht nachgewiesen zu werden.***

(6) ***Zwischenmaterial von VS-VERTRAULICH oder höher eingestuften VS, das nicht unverzüglich vernichtet wird, ist mit dem entsprechenden Geheimhaltungsgrad und dem Zusatz "VS-Zwischenmaterial" zu kennzeichnen. Bei Weitergabe an Dritte ist ein Nachweis erforderlich; dies gilt nicht bei Weitergabe an die VS-Registratur.***

(7) ***Für die Kennzeichnung ausländischer oder zwischenstaatlicher VS-Einstufungen gilt die Anlage 4.***

Zu Absatz 1:
Enthält eine VS unterschiedlich eingestufte Teile (vgl. Abschn. 1 der Anlage 1 zur VSA und Beispiel 5 zur VSA), so sind unabhängig davon alle Seiten mit dem Geheimhaltungsgrad zu kennzeichnen, der der Gesamteinstufung entspricht. Anfang und Ende der unterschiedlich eingestuften Teile müssen klar erkennbar sein.
Der Begriff "Seitenzahl" wurde gewählt, weil sich die Blattzahl im Falle beidseitiger Beschriftung bei Kopien ändern kann.
Sind einzelne Teile eines höher eingestuften Schriftstückes VS-NUR FÜR DEN DIENSTGEBRAUCH oder nicht eingestuft, so kann es zweckmäßig sein, diese gesondert als Anlage beizufügen.
Die Kennzeichnung von Schriftgutbehältern soll auf die Schutzbedürftigkeit der Unterlagen beim Transport und bei der Aufbewahrung hinweisen.
Schriftgutbehälter, die VS unterschiedlicher Geheimhaltungsgrade enthalten, sind entsprechend dem jeweils höchsten Geheimhaltungsgrad zu kennzeichnen.
Eine besondere Kennzeichnung der Schriftgutbehälter, die VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH enthalten, ist nicht vorgeschrieben.

Von einer äußeren Kennzeichnung sind VS-Transportbehälter ausgenommen, vgl. Abschnitt 7 der Anlage 6 zur VSA.

Zu Absatz 3:
Nur die Änderung oder Aufhebung der Einstufung von VS-VERTRAULICH oder höher eingestuften VS ist im VS-Bestandsverzeichnis zu vermerken.

Zu Absatz 4:
Die Beschaffenheit kann sich auch darin äußern, dass die VS mehrere Teil- oder verschiedene Betriebszustände einnehmen kann.
Bei Verschlüsselungsgeräten (z. B. VS-Schlüsselgerät Elcrodat 6-2 (E-Dat 6-2)) ist u. U. zwischen einer Grundeinstufung (bei E-Dat 6-2 VS-NfD) und der Einstufung im funktions- bzw. betriebsbereiten Zustand (beim im Geheimschutz eingesetzten E-Dat 6-2 GEHEIM) zu unterscheiden.
Eine solche Besonderheit ist bei der Kennzeichnung aufzuführen. z. B. durch einen Aufkleber:

VS-NUR FÜR DEN DIENSTGEBRAUCH

im betriebsbereitem Zustand

GEHEIM
amtlich geheimgehalten

Zu Absatz 5 und 6:
Diese Bestimmungen stellen auf den Regelfall ab. Eine Schreibkraft fertigt z.B. eine VS des Geheimhaltungsgrades GEHEIM und übergibt das Basismaterial (z. B. handschriftlicher Entwurf, Speichermedium mit Diktat, etc.) sowie ggf. Fehldrucke und Speichermedien der VS-Registratur oder dem Verfasser zur entsprechenden geschäftsmäßigen Behandlung (Vernichtung, Aufbewahrung). In diesem Fall brauchen die Unterlagen weder gekennzeichnet noch nachgewiesen zu werden. Diese Unterlagen dürfen jedoch nicht an Dritte weitergegeben werden.

Als Dritter gilt grundsätzlich jeder, der nicht unmittelbar mit der Herstellung befasst ist, ausgenommen der VS-Verwalter (vgl. Abs. 6 Satz 2). Innerhalb einer Arbeitsgruppe kann VS-Zwischenmaterial jedoch ohne Kennzeichnung und ohne Nachweis weitergegeben werden; ebenso zwischen der Schreibkraft oder anderen mit der Herstellung/Vervielfältigung befassten Personen und dem jeweiligen Auftraggeber, vgl. § 2 Abs. 2 VSA.

Zu Absatz 6:
VS-Zwischenmaterial, dass über einige Zeit aufbewahrt wird (z. B. über das Dienstende hinaus zum nächsten Werktag), muss als solches erkennbar sein, damit z.B. im Krankheitsfall des VS-Bearbeiters der Vertreter die Unterlagen auch entsprechend behandelt.
Die Kennzeichnung des VS-Zwischenmaterials (Geheimhaltungsgrade mit dem Zusatz „VS-Zwischenmaterial“) erfolgt entsprechend § 16 VSA; verbleibt es im eigenen Gewahrsam, genügt die Kennzeichnung am oberen Rand bzw. bei gehefteten Unterlagen auf der ersten Seite.

Bei Weitergabe an Dritte entfallen die für VS-Zwischenmaterial vorgesehenen Ausnahmen (vgl. § 16 Absatz 2 und 3 VSA und § 28 Abs. 4 VSA); in diesem Falle kann deshalb die Kennzeichnung als VS (unter Wegfall des Zusatzes „VS-Zwischenmaterial“) angezeigt sein.

§ 17 Aufbewahrung von VS

(1) VS-VERTRAULICH oder höher eingestufte VS sind in VS-Registraturen aufzubewahren. Eine Aufbewahrung außerhalb der VS-Registratur ist nur zulässig, soweit dies aus dienstlichen Gründen unerlässlich ist.

(2) VS-VERTRAULICH oder höher eingestufte VS sind bei Nichtgebrauch in VS-Verwahrgelassen einzuschließen. Dies gilt für STRENG GEHEIM oder GEHEIM eingestufte VS bereits bei kürzerer Abwesenheit der die VS bearbeitenden oder verwaltenden Personen. VS-VERTRAULICH eingestufte VS können bei kurzer Abwesenheit der VS bearbeitenden oder verwaltenden Personen während der Arbeitszeit im Dienstzimmer liegen bleiben, sofern die Zimmertür mit einem Sicherheitsschloss verschlossen wird.

(3) VS-Verwahrgelasse sind Stahlschränke, Aktensicherungsräume u. Ä., die besonderen Sicherheitsanforderungen entsprechen. Näheres über VS-Verwahrgelasse, ihre Bewachung oder technische Überwachung bestimmen die §§ 30 ff.

(4) Außerhalb der Arbeitszeit sind diese VS-Verwahrgelasse zu bewachen oder durch eine Alarmanlage technisch zu überwachen. Bei GEHEIM oder VS-VERTRAULICH eingestuften VS kann eine Bewachung bzw. technische Überwachung des VS-Verwahrgelasses unterbleiben, wenn das Gebäude oder der

Gebäudeteil, in dem sich das Verwahrgelass befindet, ständig bewacht oder technisch überwacht ist und die VS nur vorübergehend in dem VS-Verwahrgelass aufbewahrt werden.

(5) Ist eine Aufbewahrung nach den Absätzen 2 und 3 nicht möglich, so sind die VS bei einer anderen Dienststelle unterzubringen, die die erforderlichen Voraussetzungen erfüllt. Außer bei STRENG GEHEIM eingestuften VS ist die Aufbewahrung in einem Bankschließfach zulässig, wenn sichergestellt ist, dass nur befugte Personen der Dienststelle dazu Zugang erhalten.

(6) Bei GEHEIM oder VS-VERTRAULICH eingestuften VS kann auf Antrag der Dienststellenleitung nach Beratung durch das BSI die zuständige Oberste Bundesbehörde zulassen, dass von der vorgeschriebenen Bewachung bzw. technischen Überwachung abgewichen wird, wenn die damit verbundenen Maßnahmen unangemessen wären. Bei GEHEIM eingestuften VS muss in diesem Fall jedoch mindestens sichergestellt sein, dass ein unbefugter Zugriff auf das VS-Verwahrgelass unmittelbar erkennbar ist.

(7) Ein VS-Verwahrgelass kann von mehreren Personen benutzt werden. Soweit es der Grundsatz „Kenntnis nur, wenn nötig“ erfordert, sind VS-Verwahrgelasse zu unterteilen, z. B. Stahlschränke mit verschließbaren Innenfächern auszustatten.

(8) Ein VS-Verwahrgelass, dessen Benutzer nicht rechtzeitig erreicht werden kann, ist bei Notwendigkeit durch die Geheimschutzbeauftragte oder den Geheimschutzbeauftragten oder eine damit beauftragte ermächtigte Person in Gegenwart von Zeugen zu öffnen. Die Entnahme von VS ist aktenkundig zu machen.

Zu Absatz 1:
Die angestrebte Aufbewahrung von VS an nur einer Stelle erleichtert ihre Sicherung sowie eine Verbleibskontrolle. Die aus vielen Spionagefällen bekannte unbefugte Mitnahme von VS (z.B. abends mitnehmen und morgens zurückbringen) wird erschwert.

Der Grundsatz "Kenntnis nur, wenn nötig" kann es im Einzelfall erfordern, wegen des Umfangs oder der Bedeutung von VS in einer Behörde eine Abschottung innerhalb der VS-Registratur vorzunehmen oder mehrere (getrennte) VS-Registraturen zu bilden.

Für VS, die zumindest vorübergehend auch dem VS-Verwalter nicht zugänglich sein sollen (vgl. auch Abschn. 2.6 der Anlage 6 der VSA), müssen innerhalb oder außerhalb der VS-Registratur sichere Aufbewahrungsmöglichkeiten bestehen, z.B.

- gesondertes VS-Verwahrgelass,
- Schließfach in einem VS-Verwahrgelass oder
- Klebemappe oder VS-Transportbehälter in einem VS-Verwahrgelass.

Nichtdeutsche VS des vergleichbaren Geheimhaltungsgrades GEHEIM und höher (siehe Anlage 4) sind von nationalen VS grundsätzlich getrennt aufzubewahren. Das Trennungsgebot beinhaltet nicht die unmittelbar zum Vorgang zugehörigen nationalen VS.

Zu Absatz 2:
Satz 1 ("in VS-Verwahrgelassen einzuschließen") schließt grundsätzlich eine Benutzung beider Schlösser des VS-Verwahrgelasses - d.h. des Schlüssel- und Zahlenkombinationsschlosses (ZKS)- ein. Es hieße allerdings, die Anforderungen an die Praxis zu überspannen, wollte man verlangen, auch bei kürzester Abwesenheit das ZKS zu verwerfen und anschließend wieder neu einzustellen. Während der Arbeitszeit bleibt, soweit die Dienststelle nichts Näheres bestimmt hat, das Verwerfen des ZKS in das Ermessen der jeweiligen VS-Verwalter oder -Bearbeiter gestellt. Bei Dienstende ist das ZKS in jedem Falle zu verwerfen.

Unter "kürzerer Abwesenheit“ sind mehr als ca. 5 Minuten, unter "kurze Abwesenheit" bis maximal eine Stunde zu verstehen.
Soweit VS-Bearbeiter nicht über ein VS-Verwahrgelass verfügen, ist dies so auszulegen, dass bei "kürzester Abwesenheit“ (maximal ca. 5 Minuten) die VS auch im Zimmer - ein Sicherheitsschloss vorausgesetzt - eingeschlossen werden können. Ein anderes Verfahren wäre praxisfremd.
Die Türschlüssel (einschließlich evtl. Gruppen- und Generalhauptschlüssel) sollen unter Kontrolle gehalten werden.

Zu Absatz 3:
VS-Verwahrgelasse müssen insbesondere gegen konspirativen Zugriff sicher sein und besonderen Sicherheitsanforderungen entsprechen.

Zu Absatz 4:
Zu Bewachung siehe § 31.

Zu Absatz 6:
Mit dieser Ausnahmeregelung soll insbesondere für Dienststellen mit geringer Anzahl von VS sowie bei abgelegenen Dienststellen der Grundsatz der Verhältnismäßigkeit gewahrt werden. In Zusammenarbeit mit dem BSI sind im Einzelfall u. a. folgende Fragen zu prüfen:

1. Welche Folgen kann ein Zugriff auf die VS durch Unbefugte haben?

2. Können die Folgen eines solchen Zugriffs durch geeignete Maßnahmen gemildert oder aufgehoben werden? Nutzen die VS Dritten auch dann noch, wenn bekannt wird, dass sie in ihrem Besitz sind?

3. Können die Sicherungsmaßnahmen so reduziert werden, dass für einen Angreifer dennoch ein nicht kalkulierbares Risiko bleibt?

Wenig sinnvoll sind Bewachungsmaßnahmen, die ein Angreifer vorher genau analysieren und in seine Tatplanung einbeziehen kann (z.B. regelmäßige Kontrollen in einem bestimmten zeitlichen Abstand). Eine solche Bewachung sollte durch eine technische Überwachung ersetzt werden. Zwar sind nicht alle technischen Maßnahmen überwindungssicher, doch das Entdeckungsrisiko für einen Angreifer (durch Fehler oder Unachtsamkeit) ist weniger kalkulierbar, so dass ein höherer Abschreckungseffekt besteht.
Von der Ausnahmeregelung sollte bei VS-VERTRAULICH eingestuften VS großzügig Gebrauch gemacht werden. Bei einer geringen Anzahl von VS-VERTRAULICH eingestuften VS kann ggf. auf eine Bewachung oder technische Überwachung ganz verzichtet werden.
Die Anforderung des „unmittelbaren Erkennens“ eines unbefugten Zugriffs bei GEHEIM eingestuften VS beinhaltet jedoch in jedem Fall eine Bewachung oder technische Überwachung.

Zu Absatz 7:
Ein VS-Verwahrgelass kann auch von mehreren Personen benutzt werden. Soweit es der Grundsatz “Kenntnis nur, wenn nötig” erfordert, sind VS-Verwahrgelasse zu unterteilen, z.B. Stahlschränke mit verschließbaren Innenfächern auszustatten.
Bei Nutzung eines VS-Verwahrgelasses durch mehrere Personen empfiehlt es sich, einen Hauptverantwortlichen zu bestimmen, der z.B. auch das Zahlenkombinationsschloss umstellt.

Zu Absatz 8:
Hier wird der Fall geregelt, dass eine VS aus einem VS-Verwahrgelass dringend benötigt wird, deren Benutzer (VS-Bearbeiter oder VS-Verwalter) nicht rechtzeitig erreicht werden kann (z.B. infolge Krankheit, Dienstreise). Die oder der Geheimschutzbeauftragte hat nach Öffnung des VS-Verwahrgelasses sicherzustellen, dass nach § 34 Abs. 3 und 4 VSA verfahren wird.
Soweit es sich um das VS-Verwahrgelass eines VS-Verwalters handelt und eine Vertretung erforderlich wird, ist § 20 Abs. 5 VSA anzuwenden.

§ 18 Nachweis von VS-VERTRAULICH oder höher eingestuften VS

(1) VS-VERTRAULICH oder höher eingestufte VS sind in VS-Registraturen zu verwalten. Kenntnisnahme und Verbleib sind durch VS-Bestandsverzeichnisse, VS-Quittungsbücher, VS-Begleitzettel, VS-Empfangsscheine, VS-Übergabe- und VS-Vernichtungsprotokolle nachzuweisen (z. B. Muster nach Anlage 3).

(2) Die Führung dieser Nachweise kann auch in elektronischer Form entsprechend § 6 Abs. 3 erfolgen. Hierbei sollen möglichst vom BSI zugelassene VS-Registratur-Systeme eingesetzt werden. Zur Beweissicherung ist mindestens Folgendes automatisch revisionssicher zu protokollieren:

1. Zugriffe auf die VS-Daten,

2. Abgewiesene Zugangs- und Zugriffsversuche,

3. Übertragung von VS-Daten über Leitungen.

Der Zugriff auf die Protokolle und insbesondere ihre Löschung bedürfen der Zustimmung der Geheimschutzbeauftragten.

(3) VS-Datenträger, ihr Verbleib und ihre Vernichtung sind in einem gesonderten VS-Bestandsverzeichnis nachzuweisen. Zur Erfassung genügt die Angabe eines Ordnungskriteriums (z. B. fortlaufende Nummer) sowie des Einsatzbereichs (Organisationseinheit, IT-Nutzer) und eine Kurzangabe des Aufgabengebiets. VS-Datenträger sind grundsätzlich nur gegen Quittung weiterzugeben. Mehrere auf einem Datenträger gespeicherte VS-VERTRAULICH oder höher eingestufte VS, die nicht weitergegeben werden, brauchen nicht einzeln nachgewiesen zu werden.

(4) Ausdrucke sind unverzüglich der VS-Registratur zuzuleiten und im VS-Bestandsverzeichnis zu registrieren. Dies gilt nicht für VS-Zwischenmaterial, das nicht an Dritte weitergegeben wird.

(5) VS-Nachweise sind mindestens 5 Jahre aufzubewahren. Für VS-Bestandsverzeichnisse beginnt die Frist mit Herabstufung auf den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH, Aufhebung der VS-Einstufung, Abgabe oder Vernichtung aller in ihnen nachgewiesenen VS. Für VS-Quittungsbücher, VS-Empfangsscheine, VS-Übergabeprotokolle und VS-Vernichtungsprotokolle beginnt die Frist mit der Ausstellung bzw. der letzten Eintragung.

(6) Auf Datenträgern vorliegende Sicherheitskopien von VS sind wie die ursprüngliche VS im Sinne dieser Anweisung zu behandeln, Schlüssel für die Kryptierung sind getrennt zu speichern.

Zu Absatz 1:
STRENG GEHEIM, GEHEIM oder VS-VERTRAULICH eingestufte VS sind i.d.R. von offenen Akten getrennt in besonderen VS-Registraturen zu verwalten. Ausnahmen kommen z.B. bei den Nachrichtendiensten in Betracht, bei denen fast alle Akten – unabhängig von der VS-Einstufung – geheimhaltungsbedürftig sind. Hier kann die gemeinsame Verwaltung von VS und nicht eingestuften Akten angezeigt sein.

In der Anlage 3 der VSA sind die Geheimschutzforderungen aufgeführt, die beim Führen des VS-Bestandsverzeichnisses zu beachten sind. Aus dem VS-Bestandsverzeichnis muss jedes einzelne Schriftstück (Schreiben, Anlagen, Kopien, Abschriften usw.) ersichtlich sein. Im Übrigen wird die Gestaltung des VS-Bestandsverzeichnisses den einzelnen Behörden überlassen.

Zu Absatz 2:
Ein Protokoll gilt als revisionssicher, wenn es eine nachträgliche Prüfung der durchgeführten Verarbeitungsprozesse gewährleistet und unveränderbar ist. Deshalb muss die Protokollierung besonderen Integritäts- und Verfügbarkeitsanforderungen (Sicherung der Aufzeichnungen gegen Verlust) genügen.
Eine entsprechende Lösung kann z. B. durch einen laufend mitschreibenden „Protokolldrucker“ oder durch permanente Speicherung auf einem nur einmalig beschreibbaren Massenspeicher (z. B. CD, DVD etc.) oder in einer mittels elektronischer Signatur abgesicherten Datenbank erfolgen.
Als Beweissicherung ist mindestens Folgendes automatisch aufzuzeichnen:
abgewiesene Zugangs-/Zugriffsversuche,
Ausdrucke, Ausgaben von VS auf Datenträger und Übermittlung von VS ,
Zugriffe auf VS-Daten (wer hat zu welchem Zeitpunkt welche Rechte ausgeübt.
Es soll grundsätzlich möglich sein, bezogen auf einzelne Benutzer, Benutzergruppen und zugriffsgeschützte Objekte sowie sicherheitserhebliche Ereignisse zuverlässig und nachvollziehbar aufzubereiten.

Zu Absatz 5:
Sind alle VS abgegeben, vernichtet oder ist ihr Geheimhaltungsgrad aufgehoben und bedürfen die Eintragungen keiner VS-Einstufung mehr, so genügt es, das VS-Bestandsverzeichnis unter Verschluss zu nehmen.

Zu Absatz 6:
Die Geheimschutzmaßnahmen sind erforderlich, sofern die auf den Sicherungskopien befindlichen VS unverschlüsselt gespeichert sind. Sind die Daten verschlüsselt (§ 21 Abs. 3) gespeichert, sind die üblichen,

allgemeinen Sicherheitsmaßnahmen zur Behandlung und Aufbewahrung von Datensicherungsdatenträgern ausreichend.

§ 19 Verwaltung von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS

(1) Als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS sowie offene Akten und Vorgänge können, soweit sie nicht Bestandteil höher eingestufter VS sind, von diesen getrennt verwaltet und aufbewahrt werden.

(2) Als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS sind bei Nichtgebrauch in verschlossenen Räumen oder Behältern (Schränke, Schreibtische u. Ä.) aufzubewahren. Innerhalb von Sicherheitsbereichen kann hiervon abgesehen werden.

(3) ***Weiteres zur Arbeit mit VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS regelt Anlage*** 7.

Zu Absatz 1:
Die Aufbewahrung von als VS-NfD eingestuftem Schriftgut zusammen mit offenem Schriftgut in einer offenen Registratur ist zulässig. Dabei ist jedoch weiterhin der Grundsatz „Kenntnis nur wenn nötig“ zu beachten. Die dabei zu berücksichtigenden Anforderungen sind in der Anlage 7 zur VSA aufgeführt.

Zu Absatz 2:
Wenn auch besondere Sicherheitsanforderungen an die Schließeinrichtungen der Räume oder Behälter, in denen VS-NfD eingestufte Informationen aufbewahrt werden, nicht erhoben werden, so sollten zumindest bei einer Häufung dieser VS Sicherheitsschlösser vorhanden sein.
Auch in Sicherheitsbereichen ist der Grundsatz „Kenntnis nur, wenn nötig“ zu beachten.

Zu Absatz 3:
Das VS-NfD-Merkblatt (Anlage 7) ist als Ergänzung zu den Bestimmungen der VSA zu sehen. Die weiteren Bestimmungen der VSA finden Anwendung.

§ 20 Verwaltungspersonal

(1) Die Verwalter von VS-VERTRAULICH oder höher eingestuften VS (VS-Verwalter) haben in besonderem Maße auf die Einhaltung der VS-Vorschriften zu achten und bei Verstößen oder Verdachtsmomenten die Geheimschutzbeauftragten zu unterrichten.

(2) Die VS-Verwalter prüfen täglich, ob alle ausgegebenen VS-VERTRAULICH oder höher eingestuften VS zurückgegeben wurden. Soweit eine tägliche Rückgabe nicht erfolgt, fordern sie mindestens halbjährlich alle VS an, die länger als drei Monate ausstehen, oder überzeugen sich auf andere Weise, dass die ausgegebenen VS vorhanden sind. Wird nach zweimaliger Aufforderung der Verbleib der VS nicht nachgewiesen, so unterrichten sie die Geheimschutzbeauftragten.

(3) Wechseln VS-Verwalter ihr Arbeitsgebiet, so haben die Nachfolger die Vollzähligkeit der Schlüssel zu den VS-Verwahrgelassen und Alarmanlagen sowie der Registraturhilfsmittel zu prüfen und sich stichprobenartig davon zu überzeugen, dass die VS richtig nachgewiesen und vorhanden sind. Zahlenkombinationen und andere Zugangsinformationen sind zu ändern. Es ist ein VS-Übergabeprotokoll nach Anlage 3 zu fertigen.

(4) Bei vorübergehender Vertretung von VS-Verwaltern (z. B. bei Urlaub oder Krankheit) ist nach Absatz 3 Satz 1 zu verfahren. Es reicht aus, die Übergabe aktenkundig zu machen.

(5) Können VS-Verwalter die Übergabe nicht vornehmen, so haben die Geheimschutzbeauftragten oder von diesen beauftragte Personen Schlüssel und Zahlenkombinationen zu den VS-Verwahrgelassen und Alarmanlagen zu beschaffen und diese den Vertretern oder Nachfolgern zusammen mit den Registraturhilfsmitteln zu übergeben. Dabei ist die Vollständigkeit in Gegenwart eines Zeugen zu prüfen; dasselbe gilt für die stichprobenartige Prüfung, ob die VS vorhanden sind.

Zu Absatz 2:

Die Sätze 1 und 2 eröffnen zwei Alternativen. Dienststellen, die aufgrund der großen Zahl von VS nicht nach Satz 1 verfahren können, wenden Satz 2 an.
Vgl. auch Erläuterungen zu § 17 Abs. 1 VSA.
Die Fristen in Satz 2 stehen im Einklang mit der GGO (vgl. § 14 Abs. 5 RegA).

Zu Absatz 4:
Auf ständige Vertretungen (z.B. im Schichtdienst oder während der Mittagspause) ist diese Bestimmung nicht anzuwenden.
Die Übergabe in den Fällen des Absatzes 2 kann z.B. auf einer fortlaufend geführten Liste oder in einem Buch aktenkundig gemacht werden.

§ 21 Grundsätze zu Weitergabe und Versand von VS

(1) Jeder hat sich vor der Weitergabe oder dem Versand von VS oder ihrem Inhalt zu vergewissern, dass der vorgesehene Empfänger zur Annahme oder Kenntnisnahme berechtigt ist. Die Weitergabe ist nachzuweisen und soll bei VS-VERTRAULICH oder höher eingestuften VS grundsätzlich - auch bei Übertragung über Telekommunikationsverbindungen - über die VS-Registratur erfolgen (Anlage 3, Muster 8).

(2) Zum Versand von VS ist anstelle der postalischen Form nach Möglichkeit die Übertragung über Telekommunikationsverbindungen nach § 40 zu nutzen. Benutzer dieser Systeme haben Teilnehmerverzeichnisse vor dem Versand auf aktuellen Stand zu kontrollieren und ein schriftliches oder elektronisches Protokoll über den Versand zu erzeugen und zum Vorgang zu nehmen.

(3) VS, die mit einem vom BSI für den betreffenden Geheimhaltungsgrad zugelassenen Kryptosystem verschlüsselt wurden, bedürfen keines weiteren Schutzes gegen unbefugte Kenntnisnahme. Dies gilt nicht für zum Dekryptieren von verschlüsselten VS benötigte kryptographische Schlüssel. Diese sind getrennt einzustufen und zu schützen.

(4) Für die Weitergabe von VS an Unternehmen gilt Folgendes:

1. ***Den Geheimschutz im Bereich der Wirtschaft regelt das Bundesministerium für Wirtschaft und Technologie.***

2. ***Bei ihm sind vor Weitergabe VS-VERTRAULICH oder höher eingestufter VS Sicherheitsbescheide über die beteiligten Unternehmen anzufordern.***

3. ***In begründeten Ausnahmefällen kann bei ihm vor Auftragsvergabe zusätzlich eine abschließende Beurteilung angefordert werden, in der ausdrücklich bestätigt wird, dass die beteiligten Unternehmen die für den bestimmten Auftrag erforderlichen Voraussetzungen erfüllen.***

4. ***Bei VS-NUR FÜR DEN DIENSTGEBRAUCH ist Anlage 7 zu beachten.***

Soweit besondere Gründe es erfordern, kann im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie für bestimmte Bereiche auch eine andere Oberste Bundesbehörde die vorstehenden Aufgaben übernehmen.

(5) Vorzimmerberechtigte sollen VS-VERTRAULICH oder höher eingestufte VS grundsätzlich persönlich entgegennehmen. Die Geheimschutzbeauftragten können mit Zustimmung der zuständigen obersten Bundesbehörde Ausnahmen zulassen, z. B. bei hohem Aufkommen an VS die Annahme durch Vorzimmerkräfte erlauben, wenn der Vorzimmerberechtigte anwesend ist und die VS bis zur Übergabe in persönlichem Gewahrsam oder nach § 17 Abs. 2 aufbewahrt wird. Die Ausnahmeregelung ist in der Geheimschutzdokumentation nachzuweisen.
(6) Die Hinweise der Anlage 6 zu Weitergabe und Versand von VS sind zu beachten.

Zu Absatz 1:

Arten der Weitergabe sind: Weitergabe von Hand zu Hand, Beförderung durch Boten, Versand durch Kurier, Versand durch privaten Zustelldienst, mündliche Mitteilung, Übertragung über Telekommunikations- oder andere technische Kommunikationsverbindung, Bereitstellung in einem Intranet (abgeschlossenem Netz) zur Einsicht (z. B. ATD, BPOL-Infothek u. Ä.)

Zu Absatz 2:
Unter Sicherheitsaspekten gilt für die unterschiedlichen Beförderungsarten von VS folgende Prioritätenfolge:

1. Elektronische Übermittlung von VS
   VS sollten möglichst elektronisch (in kryptierter Form, vgl. § 40 VSA) übermittelt werden. Sie sollten nur dann in Papierform versandt werden, wenn eine elektronische Übermittlung in kryptierter Form nicht möglich ist.

2. Versendung durch Kurier
   Die Versendung in Papierform sollte nach Möglichkeit durch Kurier erfolgen.

3. Private Zustelldienste
   Sie sollten für eine Versendung nur eingesetzt werden, wenn ein Kurier nicht zur Verfügung steht oder dessen Einsatz unwirtschaftlich wäre.

Bei der Versendung oder dem Empfang von VS-Sendungen, die durch private Zustelldienste befördert werden, ist auch das Verfahren in der Behörde beim Postausgang und Posteingang zu regeln (siehe auch Anlage 5 Nr. 2).
Um innerhalb der Behörden eine unverzügliche Beförderung und einen lückenlosen Nachweis von Sendungen mit VS des Geheimhaltungsgrades VS-VERTRAULICH oder GEHEIM zu gewährleisten und keine Hinweise auf den Inhalt zu geben, wird folgendes Verfahren empfohlen:
Bei eingehenden Sendungen wird von der für die üblichen Postsendungen zuständigen Posteingangsstelle nur der äußere Umschlag geöffnet.
Danach werden Sendungen mit VS gegen Empfangsbestätigung der VS-Registratur übergeben, die den inneren Umschlag auf Unversehrtheit prüft und öffnet.
Zur Versendung werden VS nach Abschnitt 6 der Anlage 6 verpackt und gegen Empfangsbestätigung der für die üblichen Postsendungen zuständigen Postausgangsstelle übergeben, die das weitere veranlasst. Die VS-Registratur überprüft anhand des VS-Empfangsscheines (vgl. Abschnitt 6.7, Anlage 6) die unverzügliche Zustellung der VS-Sendungen.

Die rechnergestützte Sendungsverfolgung bietet auch die Möglichkeit, sich über das Internet über den Lauf einer Sendung (z.B. den Zeitpunkt der Auslieferung) aktuell zu informieren.

Bei einer verschlüsselten Übertragung von VS über Telekommunikations- oder andere technische Kommunikationsverbindungen (siehe § 40) bedarf es keines VS-Empfangsscheins.

Zu Absatz 3:
Die Verschlüsselung mit einem vom BSI für den betreffenden Geheimhaltungsgrad zugelassenen Kryptosystem ist eine ausreichende Maßnahme zum Schutz der Vertraulichkeit und Integrität der VS. Zusätzlich sind Maßnahmen zur Verfügbarkeit der VS zu berücksichtigen.

Zu Absatz 4:
Im Regelfall reicht ein Sicherheitsbescheid für ein Unternehmen für eine VS-Auftragsvergabe aus. Eine zusätzliche Einschaltung des Bundesministeriums für Wirtschaft (BMWi) (vgl. Nummer 3) ist nur in Ausnahmefällen (z.B. bei hochsensitiven VS-Aufträgen mit „Schutzwort“) geboten, wenn (zusätzlich zu den ohnehin bestehenden Kontrollmechanismen gegenüber den Unternehmen) noch einmal speziell für den bestimmten Auftrag die erforderlichen Geheimschutzvorkehrungen überprüft werden sollen. Die beauftragten Unternehmen können in diesen Fällen im Rahmen des VS-Auftrages verpflichtet werden, bei Vergabe von Unteraufträgen entsprechend zu verfahren.

Sollen nur einzelne Privatpersonen Zugang zu VS oder Tätigkeiten nach § 10 Abs. 3 und 4 VSA erhalten (z.B. Gutachter oder Reinigungskräfte in Sicherheitsbereichen), ohne dass ein Unternehmen insgesamt oder in Teilen einer Überprüfung bedarf, so hat die jeweilige Behörde die erforderlichen Geheimschutzmaßnahmen selbst zu veranlassen (s. Absatz 1).

Die Aufnahme eines Unternehmens in die Geheimschutzbetreuung des BMWi kann grundsätzlich nur dann beantragt werden, wenn eine Weitergabe von VS-VERTRAULICH oder höher eingestuften VS beabsichtigt ist, so

dass beim Unternehmen die Voraussetzungen für einen entsprechenden VS-Schutz gegeben sein müssen. In den übrigen Fällen (z.B. bei Wartungsfirmen für bestimmte VS-Sicherungseinrichtungen) kommt eine Aufnahme in die Geheimschutzbetreuung des BMWi nur in Betracht, wenn mit dem BMWi Einvernehmen darüber erzielt wurde, dass neben einzelnen Personen auch Verantwortungsträger der Unternehmen (z.B. Geschäftsführer oder Aufsichträte wegen deren Einwirkungsmöglichkeiten auf überprüfte oder ermächtigte Personen) mit überprüft werden müssen.

Abweichende Zuständigkeiten für Sonderfälle (z.B. Flugsicherung oder Deutsche Bahn AG) sind in der „Allgemeinen Verwaltungsvorschrift des Bundesministeriums für Wirtschaft zur Ausführung des fünften Abschnitts (§§ 24 bis 31) des SÜG“ vom 21.4.1994 (BGBl. I. S. 867 ff.) geregelt.

Soweit regierungsnahe Stiftungen oder Forschungseinrichtungen nicht durch das BMWi, sondern durch ein anderes Ressort geheimschutzmäßig betreut werden, hat das zuständige Ressort diese in geeigneter Weise (z.B. durch Vertrag) zur Beachtung der VS-Vorschriften zu verpflichten. Die Einhaltung der Verpflichtung ist in angemessenen Zeitabständen zu kontrollieren.

Die politischen Parteien nach Artikel 21 des Grundgesetzes erhalten VS nur, soweit sie sich freiwillig zur Beachtung der VS-Vorschriften verpflichtet haben (Auskunft erteilt auf Anfrage des Bundesministeriums des Innern). Die Realisierung der VS-Vorschriften liegt in der Eigenverantwortung der Parteien (vgl. auch § 3 Abs. 1 Nr. 3 SÜG).

Zu Absatz 5:
Die Bestimmung geht auf Erfahrungen aus Spionagefällen zurück. Oft wurde der Verrat von VS erst dadurch möglich, dass Vorzimmerberechtigte (nicht selten aus Bequemlichkeit) gegen den Grundsatz „Kenntnis nur, wenn nötig“ verstoßen haben.

Vorzimmerberechtigte können VS durch Mitarbeiter oder VS-Verwalter persönlich vorlegen und abholen oder weiterleiten lassen. Die Mitarbeiter oder VS-Verwalter können auch die Eintragungen in den Quittungsbüchern vornehmen, so dass der Vorzimmerberechtigte nur noch quittieren muss.

Bei Vorzimmerberechtigten, die über einen eigenen Referenten verfügen, kann dieser unter der Vorraussetzung der Einhaltung der Vorgaben gemäß § 10 Abs. 3 VSA die VS für die Vorzimmerberechtigten annehmen und weiterleiten.

Die Regelung beschränkt sich auf die Annahme und Weitergabe von VS. Bei der übrigen geschäftsmäßigen Behandlung (z.B. bei Schreibarbeiten) entscheiden die Vorzimmerberechtigten selbst, ob die entsprechend ermächtigte Vorzimmerkraft Zugang erhält.

In den Fällen von Satz 2 ist es Aufgabe der Dienststellenleitung, zwischen arbeitsökonomischen Interessen einerseits und Geheimschutzinteressen andererseits abzuwägen und zu entscheiden. Dabei soll an der restriktiven Handhabung festgehalten und die praktische Handhabung der Annahme und Weiterleitung von VS durch die Vorzimmerkraft mit dieser eingehend erörtert werden. Vorausgesetzt, einer Ausnahmeregelung wird zugestimmt, sind folgende Punkte zu beachten:

- Die Ausnahmegenehmigung ist schriftlich zu erteilen.
- Eine Vorzimmerkraft darf VS-VERTRAULICH eingestufte VS für einen Vorzimmerberechtigten nur bei dessen Anwesenheit oder kurzfristiger Abwesenheit annehmen. Sie hat diese VS, die sie für den Vorzimmerberechtigten annimmt oder von ihm zur Weitergabe erhält, unverzüglich weiterzuleiten. Sie weist den Ein- und Ausgang dieser VS in einem VS-Quittungsbuch nach; ein Nachweis durch den Vorzimmerberechtigten kann entfallen.
- Anlage 6 Abschn. 1.1 Satz 2 und Abschn.1. 2 bleibt unberührt.
- Der Vorzimmerberechtigte prüft durch Stichproben die unverzügliche Weitergabe dieser VS**.**

§ 22 Eingehende Sendungen

(1) Elektronisch oder postalisch eingehende Sendungen mit VS-VERTRAULICH oder höher eingestuften VS sind der VS-Registratur umgehend zuzuleiten. Jede Sendung ist zu prüfen, ob sie unbeschädigt und vollständig ist. Zeigen sich Spuren unbefugter Kenntnisnahme oder ist die Sendung

unvollständig, so sind die Geheimschutzbeauftragten und die Absender unverzüglich zu benachrichtigen.

(2) Auf den VS-Empfangsscheinen nicht elektronisch eingehender Sendungen vermerkt die VS-Verwaltung das Datum des Empfangstages und sendet die Empfangsscheine mit Unterschrift und Dienststempelabdruck versehen unverzüglich an den Absender zurück. Bei ausgehenden Sendungen überwacht die VS-Verwaltung den Rücklauf der VS-Empfangsscheine.

(3) Bei elektronischer Übermittlung von VS genügt eine elektronische Empfangsbestätigung. Sofern mehrere VS übermittelt werden oder auf Datenträgern eingehen, sind diese einzeln nachzuweisen (z. B. in einem Verzeichnis der Dateinamen oder als FAX-Sendebericht).

Zu Absatz 1:
Die Posteingangsstellen sind anzuweisen, Briefe und Pakete, die VS-VERTRAULICH oder höher eingestufte VS enthalten, verschlossen (d.h. ohne Öffnung des inneren Umschlages) der VS-Registratur zuzuleiten, vgl. auch Ziffer 1 des Teils II der Anlage 1 zu § 13 Abs. 2 GGO.
Sendungen mit STRENG GEHEIM, GEHEIM oder VS-VERTRAULICH eingestuften VS, die auf dem inneren Umschlag den Vermerk „Persönlich“ (Abschn. 6.4 der Anlage 6 zur VSA) oder „Nicht durch die Registratur zu öffnen“ tragen, sind dem Empfänger oder ggf. dem Vertreter im Amt ungeöffnet mit einem VS-Begleitzettel (Anlage3, Muster 5) zuzuleiten. Der Empfänger kann eine solche VS von der Weitergabe in den Geschäftsgang ausschließen, wenn es der Grundsatz „Kenntnis nur, wenn nötig“ erfordert. In diesem Falle werden der zuständigen VS-Registratur nur der ausgefüllte VS-Begleitzettel und der unterschriebene VS-Empfangsschein zugeleitet.

Zu Absatz 2:
Der Abdruck eines üblichen Dienststempels genügt; ein Dienstsiegelabdruck ist nicht erforderlich.

§ 23 Austausch von VS mit ausländischen Staaten

(1) Die Weitergabe von deutschen VS an Dienststellen ausländischer Staaten und internationaler Organisationen setzt ein Geheimschutzabkommen bzw. Geheimschutzübereinkommen voraus, das die Bestimmungen für den Austausch regelt (siehe Anlage 4 zur VSA).

(2) Deutsche VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH können an Dienststellen ausländischer Staaten auch ohne Geheimschutzabkommen weitergegeben werden, sofern

1. ***eine dienstliche Notwendigkeit für die Weitergabe besteht,***
2. ***der Empfänger über die Geheimhaltungspflicht informiert wurde und***
3. ***die ausländische Dienststelle der deutschen Dienststelle schriftlich zusichert, die VS entsprechend nationaler Vorschriften zu schützen.***

Sofern die Weitergabe von VS an Dienststellen eines anderen Staates häufiger erfolgt, ist das Bundesministerium des Innern zum Abschluss eines Geheimschutzabkommens in Kenntnis zu setzen.

(3) In Ausnahmefällen dürfen VS-VERTRAULICH und höher eingestufte VS an Dienststellen ausländischer Staaten weitergegeben werden, mit denen kein Geheimschutzabkommen besteht, sofern

1. ***die Voraussetzung von Absatz 2 Nummern 1 bis 3 erfüllt sind,***
2. ***der Empfänger schriftlich erklärt, dass nur sicherheitsüberprüftes Personal Zugang zu den VS erhält,***
3. ***die deutsche Dienststelle einen Nachweis über die nach diesem Absatz ausgetauschten Informationen führt und***
4. ***die deutsche Dienststelle dem Bundesministerium des Innern die schriftliche Zusicherung in Kopie übersendet.***

(4) Die Weitergabe von GEHEIM oder STRENG GEHEIM eingestuften VS an Dienststellen ausländischer Staaten bedarf der Zulassung im Einzelfall durch die zuständige Oberste Bundesbehörde.

(5) Bei Gefahr im Verzug dürfen die Voraussetzungen in Absatz 2 Nr. 3, Absatz 3 Nr. 4 und Absatz 4 nachgeholt werden.

(6) Beim Erhalt ausländischer VS von Staaten, mit denen Deutschland kein Geheimschutzabkommen geschlossen hat, dürfen deutsche Dienststellen Zusicherungen entsprechend Absatz 2 Nummer 3 und Absatz 3 Nummer 2 gegenüber der ausländischen Dienststelle abgeben (Anlage 3, Muster 8d und 8e). Diese sind mindestens so lange aufzubewahren, wie die VS, auf die sie sich beziehen.

Zur Erleichterung der internationalen Zusammenarbeit wird der Austausch von VS mit Staaten, mit denen kein Geheimschutzabkommen besteht, unter bestimmten Bedingungen erlaubt. Die Zusammenarbeit der Sicherheitsbehörden hat sich insbesondere bei der Bekämpfung des internationalen Terrorismus intensiviert. Die Ausarbeitung von Geheimschutzabkommen ist jedoch oft langwierig, so dass eine Übergangslösung erforderlich ist.
Beim Bundesministerium des Innern, Ref. IS 4, sowie innerhalb des IVBB auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (http://www.bsi.bund.de/geheimschutz/index.htm) ist das Formblatt 8a „Vereinbarung zu Sicherheitsbestimmungen für Verschlusssachen“ sowie das Muster 8d der VSA (Formblatt für den VS-Austausch) in deutscher Sprache sowie in fremdsprachlicher Ausfertigung erhältlich.

§ 24 Mitnahme von VS außerhalb des Dienstgebäudes

(1) VS-VERTRAULICH oder höher eingestufte VS dürfen außerhalb des Dienstgebäudes oder einer geschlossenen Gebäudegruppe nur auf Dienstreisen und zu Konferenzen, Sitzungen, Besprechungen usw. mitgenommen werden. Ihre Mitnahme aus anderem Anlass (z. B. zur Bearbeitung in der Privatwohnung) ist unzulässig. In besonderen Fällen können die Geheimschutzbeauftragten Ausnahmen zulassen.

(2) Die Mitnahme von VS auf Dienstreisen und zu Konferenzen, Sitzungen, Besprechungen usw. außerhalb des Dienstgebäudes bzw. einer geschlossenen Gebäudegruppe ist auf notwendige Fälle zu beschränken. Die Regelungen der Anlage 6, Nr. 3 gelten entsprechend. Sie bedarf bei STRENG GEHEIM oder GEHEIM, bei Auslandsdienstreisen auch bei VS-VERTRAULICH eingestuften VS der Genehmigung der Dienststellenleitung, bei den in § 5 Abs. 3 Satz 1 genannten Behörden des Abteilungsleiters oder Unterabteilungsleiters.

(3) Innerhalb des Bundesgebietes sind VS-VERTRAULICH oder höher eingestufte VS nach Möglichkeit an eine Dienststelle am Zielort, die selbst VS verwaltet oder aufbewahrt, voraus zu senden. Auf Datenträgern verschlüsselt gespeicherte VS und zugehörige Schlüssel für die Kryptierung sind möglichst getrennt zu transportieren. Die persönliche Mitnahme ist auch gestattet, wenn sich die VS auf einem vom BSI zugelassenen IT-System oder einem entsprechend geschützten VS-Datenträger befinden.

(4) Nach außerhalb des Bundesgebietes sind VS-VERTRAULICH oder höher eingestufte VS möglichst an die zuständige Auslandsvertretung voraus zu senden und nach Erledigung des Dienstgeschäftes durch diese zurückzusenden. Ist dies nicht möglich, so versiegelt das Auswärtige Amt bzw. die zuständige Auslandsvertretung die verpackten VS und stellt eine Bescheinigung aus, nach der ihr Inhaber zur Mitnahme des versiegelten Stückes als „Kuriergepäck“ berechtigt ist. Die VS sind ständig in persönlichem Gewahrsam zu halten oder bei der Auslandsvertretung zu hinterlegen. Die persönliche Mitnahme ist ohne Mitwirkung des Auswärtigen Amtes gestattet, wenn sich die VS auf einem vom BSI zugelassenen IT-System oder einem entsprechend geschützten VS-Datenträger befinden. Die persönliche Mitnahme von STRENG GEHEIM eingestuften VS im grenzüberschreitenden Verkehr ist unzulässig. Die Geheimschutzbeauftragten können Ausnahmen zulassen.

(5) VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS können im verschlossenen Umschlag unversiegelt und ohne VS-Kurierausweis mitgeführt werden.

(6) Die Aufbewahrung von VS in Hotelzimmern bei persönlicher Abwesenheit, Hotelsafes, Gepäckschließfächern oder in unbesetzten Fahrzeugen ist grundsätzlich unzulässig.

Zu Absatz 1:
Die Erteilung von Ausnahmen (Satz 3) wurde der oder dem Geheimschutzbeauftragten (GB)übertragen, weil neben einer Prüfung der dienstlichen Notwendigkeit – z.B. durch Rückgabe beim zuständigen Vorgesetzen – auch sicherzustellen ist, dass die VS gemäß der VSA befördert und aufbewahrt werden (VS-Verwahrgelass oder ständiger persönlicher Gewahrsam).

VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS können in Einzelfällen, soweit der Dienststellenleiter nichts anderes bestimmt, ohne Genehmigung zur Bearbeitung in die Privatwohnung mitgenommen werden (eine Aufbewahrung nach Anlage 7 VSA vorausgesetzt).
Begründung: Eine regelmäßige Mitnahme entspricht einer Heim- bzw. Telearbeitstätigkeit und sollte durch eine entsprechende Anlage zum VS-NfD-Merkblatt wie im Bereich der geheimschutzbetreuten Unternehmen geregelt werden.

Zu Absatz 2:
Die Genehmigung soll vor Mitnahme der VS eingeholt werden.

Zu Absatz 3
Soweit VS zu Besprechungen bei Behörden oder Unternehmen mit VS-Aufträgen mitgeführt werden, werden dort in der Regel auch entsprechende Aufbewahrungsmöglichkeiten für VS bestehen. Besprechungsorte und –termine sollten insbesondere bei größeren Tagungen so gelegt werden, dass eine sichere Aufbewahrung der VS von Besprechungsteilnehmern gewährleistet ist. In Sonderfällen ist die Möglichkeit der Aufbewahrung bei einer Polizeidienststelle zu prüfen und ggf. zu nutzen.

Zu Absatz 4:
Besteht ein erhöhtes Risiko beim Transport von VS, so ist diesem Umstand im Einzelfall unter Berücksichtigung der speziellen Gegebenheiten und in Absprache mit dem Auswärtigen Amt Rechnung zu tragen.

Der nach den Bestimmungen des Wiener Übereinkommens (s. BGBl. 1964 II. Seite 957) für Kuriere und Kuriergepäck vorgesehene Schutz gilt nur für diplomatische Kuriere und diplomatisches Kuriergepäck im Verkehr zwischen dem Entsendestaat und den fremden Missionen im Empfangsstaat sowie zwischen den fremden Missionen untereinander. Denn gem. Artikel 27 Abs. 1 des Übereinkommens schützt der Empfangsstaat nur den freien Verkehr der Mission für alle amtlichen Zwecke. Kuriere, die amtliches Gepäck an einen anderen Ort im Ausland befördern als an den Sitz der deutschen Auslandsvertretung (z.B. anlässlich von Tagungen oder Besprechungen im Ausland an den Tagungsort außerhalb des Sitzes der deutschen Auslandsvertretung), genießen keinen nach dem Wiener Übereinkommen gesicherten völkerrechtlichen Schutz. Jedoch lässt sich für amtliche Kuriere, die zu einem Konferenzort außerhalb des Sitzes der deutschen Auslandsvertretungen entsandt werden, aus den allgemeinen Regeln des Völkerrechts ein besonderer Rechtsstatus mit einem Mindestmaß an Schutzrechten herleiten. Nähere Auskunft erteilt bei Bedarf das Auswärtige Amt.

Bei Tagungen und Besprechungen im Ausland außerhalb der jeweiligen Regierungshauptstadt ergeben sich bei Mitnahme von VS teilweise Probleme der Art, dass zur Versiegelung des Kuriergepäcks und Ausstellung eines Kurierausweises für die Rückreise u. U. erst eine weite Reise zur nächsten deutschen Auslandsvertretung erforderlich ist. Probleme können sich im Einzelfall auch bei der Hinreise ergeben, wenn in außergewöhnlich dringenden Angelegenheiten das AA nicht mehr rechtzeitig eingeschaltet werden kann. Das Bundesministerium des Innern stimmt deshalb gemäß § 46 Abs. 4 VSA zu, dass in den o. a. Fällen mit Zustimmung des Dienststellenleiters oder Geheimschutzbeauftragten VS auch unversiegelt und ohne Kurierausweise mitgeführt werden können. Soweit es sich nicht um Anliegerstaaten handelt, ist der Luftweg (deutsche Fluggesellschaft bzw. Fluggesellschaft des besuchten Landes) zu benutzen. Bei GEHEIM eingestuften VS soll von der Ausnahmemöglichkeit restriktiv Gebrauch gemacht werden.

Die persönliche Mitnahme von STRENG GEHEIM eingestuften VS im grenzüberschreitenden Verkehr ist (auch aufgrund von NATO-Bestimmungen) unzulässig.
Die Anmerkung zu Absatz 3 zu elektronisch vorliegenden VS gilt entsprechend.

Sofern die VS an ausländische Dienststellen und Institutionen gehen sollen, können mit deren Einverständnis von diesen bereit gestellte Kryptoprodukte auch für deutsche VS verwendet werden.

Zu Absatz 6:

Die VS sind ständig in persönlichem Gewahrsam zu halten. Können mitgeführte VS-VERTRAULICH oder höher eingestufte VS nicht ständig in persönlichem Gewahrsam gehalten werden, sind sie nach § 17 der VSA aufzubewahren. Ist dies nicht möglich, sind sie verschlossen einer Polizeidienststelle zur sicheren Aufbewahrung zu übergeben. Hierbei ist zu beachten, dass eine entsprechende Amtshilfe (Art. 35 GG, § 4 Abs. 1 VwVfG) durch eine Polizeidienststelle nur erfolgen kann, wenn diese auch die für eine Aufbewahrung erforderlichen materiellen Geheimschutzanforderungen erfüllt. Dies erfordert, dass die Dienststelle entweder „rund um die Uhr" mit mindestens 2 Polizeivollzugsbeamten besetzt ist oder außerhalb der Dienstzeit die VS in einem VS-Verwahrgelass (§ 17 Abs. 3)aufbewahrt und das Dienstgebäude technisch überwacht wird.

§ 25 Erörterung von VS in Konferenzen, Sitzungen, Besprechungen usw.

(1) Sollen VS-VERTRAULICH oder höher eingestufte VS in Konferenzen, Sitzungen, Besprechungen usw. erörtert werden, so ist darauf bei der Einladung unter Angabe des Geheimhaltungsgrades hinzuweisen.

(2) Die entsendenden Dienststellen gewährleisten, dass nur ausreichend ermächtigte Teilnehmer entsandt werden und stellen bei VS-VERTRAULICH oder höher eingestuften VS darüber eine Konferenzbescheinigung (z. B. Anlage 3, Muster 9) aus, soweit die einladende Stelle dies aus besonderen Gründen für erforderlich hält.

(3) Vor Beginn der Konferenz, Sitzung, Besprechung usw. hat der Leiter/Besprechungspartner auf die Geheimhaltungsbedürftigkeit der Erörterungen hinzuweisen und sich zu vergewissern, dass alle teilnehmenden Personen ausreichend ermächtigt sind. Aufzeichnungen bedürfen der Genehmigung und sind ggf. als VS zu behandeln. Das Mitführen von Bild- und Tonaufzeichnungsgeräten, mobilen Telekommunikationsendgeräten (z. B. Mobiltelefone, PDA usw.) und sonstiger Informationstechnik soll vom Leiter der Veranstaltung vorher erlaubt oder untersagt werden.

(4) Bei Erörterungen von STRENG GEHEIM oder GEHEIM eingestuften VS sollen, soweit vorhanden, abhörsichere oder abhörgeschützte Räume benutzt werden. Vor Konferenzen auf hoher Ebene oder von besonderer Bedeutung ist bezüglich der notwendigen Abhörschutzmaßnahmen das BSI rechtzeitig beratend hinzuzuziehen.

Zu Absatz 2:
Eine Konferenzbescheinigung ist im Behördenbereich nur zu verlangen, wenn „besondere Gründe" im Sinne von Absatz 2 vorliegen (z.B. eine große Zahl persönlich nicht bekannter Konferenzteilnehmer). In der Regel genügt es, die Dienststellen nach Absatz 1 zu unterrichten, so dass diese die Entsendung entsprechend ermächtigter Teilnehmer gewährleisten. Eine Identitätsprüfung der Teilnehmer an Konferenzen, Sitzungen, Besprechungen usw. kann bei Bedarf anhand des Dienstausweises vorgenommen werden.

Die Konferenzbescheinigungen gelten auch für NATO- und andere nichtdeutsche VS bis einschließlich GEHEIM. Vgl. auch Erläuterungen zu Anlage 4 VSA und § 11 Abs. 1 VSA.

Konferenzbescheinigungen können auch bei Abordnung VS-ermächtigter Personen zu anderen Dienststellen ausgestellt werden.

Mit der Konferenzbescheinigung wird die Ermächtigung lediglich formal bescheinigt. Damit erhält z.B. der Leiter einer Konferenz eine Bestätigung, dass er dem Inhaber der Bescheinigung (der eine andere Dienststelle vertreten soll) Zugang zu VS gewähren kann. Die Konferenzbescheinigung begründet für den Inhaber der Konferenzbescheinigung keinen Anspruch auf Zugang zu VS in einer anderen Dienststelle. Vielmehr entscheidet jede Dienststelle bzw. deren Vertreter in jedem Einzelfall, ob und inwieweit sie oder er dem Inhaber einer Konferenzbescheinigung Zugang zu VS gewähren will.

Die VS-Verwalter sind ggf. darauf hinzuweisen, dass sie nur den (in einer vorliegenden Liste erfassten) VS-Ermächtigten der eigenen Dienststelle Einsicht in VS geben dürfen bzw. dass eine darin erfasste zuständige Person ausdrücklich zustimmen muss, bevor eine fremde Person Einsicht erhält.

III. Aussonderung von VS

§ 26 Grundsätze der Aussonderung von VS

(1) Nicht mehr benötigte VS-VERTRAULICH oder höher eingestufte VS sind aus dem Bestand der Dienststelle zur Archivierung oder Vernichtung nach §§ 27 und 28 auszusondern.

(2) Zugelassenes Kryptomaterial (Geräte, Schlüssel) ist unter Mitwirkung des BSI auszusondern.

(3) Als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS werden wie nicht eingestuftes Material entsprechend dem Bundesarchivgesetz ausgesondert. Die Vernichtung erfolgt nach § 28.

(4) Bei Aussonderung von Gerätschaft zur weiteren Verwendung außerhalb des VS-Bereichs sind VS auf enthaltenen nichtflüchtigen Speichern (z. B. Festplatten) entsprechend § 28 zu vernichten.

Zu Absatz 2:
Hier ist Kryptomaterial in Zuständigkeit des BSI gemeint. Für Kryptomaterial der NATO, EU und Bundeswehr ist das BSI nicht zuständig.

§ 27 Archivierung von VS

(1) Die Stellen des Bundes bieten, soweit nicht Absatz 3 gilt, ihre nicht mehr benötigten VS dem Bundesarchiv (Geheimarchiv) gemäß der „Richtlinie für die Abgabe von VS an das Geheimarchiv des Bundesarchivs“ (VS-Archivrichtlinie, Anlage 8) zur Archivierung an.

(2) Die Bundesbehörden, die das Zwischenarchiv des Bundesarchivs gemäß § 20 der Registraturrichtlinie der Bundesregierung nutzen, sollen ihre nicht mehr laufend benötigten VS dem Bundesarchiv (Geheimarchiv) zur weiteren Aufbewahrung gemäß der VS-Archivrichtlinie übergeben.

(3) Nachgeordnete Stellen des Bundes mit regionaler Zuständigkeit, für deren Schriftgut ein Landesarchiv in Anwendung von § 2 Abs. 3 des Bundesarchivgesetzes vom 6. Januar 1988 (BGBl. I S. 62) in der jeweils geltenden Fassung zuständig ist, bieten ihre nicht mehr benötigten VS dem Landesarchiv (Geheimarchiv) zur Archivierung an. Die VS-Archivrichtlinie ist sinngemäß anzuwenden. Soweit kein Geheimarchiv besteht, sind die VS bis zur Aufhebung der VS-Einstufung bei der Stelle zu verwahren.
(4) Elektronisch vorliegende VS sind dem Bundesarchiv – in Fällen des Absatzes 3 dem zuständigen Landesarchiv – in entsprechender Anwendung der VS-Archivrichtlinie zur Übernahme anzubieten. Das technische Verfahren der Übergabe ist zuvor mit dem Archiv abzusprechen.

Die VS-Archivrichtlinien erstrecken sich nur auf STRENG GEHEIM, GEHEIM und VS-VERTRAULICH eingestufte VS.
Für VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS gelten die Richtlinien nicht; sie sind wie offenes Schriftgut an das Bundesarchiv abzugeben.

§ 28 Vernichtung von VS

(1) VS, die das zuständige Archiv nicht übernimmt, sind zu vernichten. VS sind so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.

(2) VS-VERTRAULICH oder höher eingestufte VS dürfen nur auf Weisung eines zeichnungsbefugten VS-Bearbeiters vernichtet werden. Der zuständige VS-Verwalter prüft diese VS auf Vollständigkeit und vernichtet sie in Gegenwart eines entsprechend ermächtigten Zeugen.

(3) Im VS-Bestandsverzeichnis ist zu vermerken, an welchem Tag welche VS oder welche Teile davon vernichtet wurden (bei STRENG GEHEIM und GEHEIM mit Angabe der Ausfertigungsnummer und Seitenzahl) und wer die Weisung zur Vernichtung erteilt hat. Der Vermerk ist vom ausführenden VS-Verwaltungspersonal und vom Zeugen zu unterschreiben. Wird über die Vernichtung der VS ein VS-Vernichtungsprotokoll gefertigt, so genügt es, wenn dies vom VS-Verwalter und vom Zeugen

unterschrieben und unter Angabe der laufenden Nummer des Vernichtungsprotokolls im VS-Bestandsverzeichnis darauf verwiesen wird.

(4) Zwischenmaterial von STRENG GEHEIM eingestuften VS, das nicht nachgewiesen ist, ist durch die zuständige VS-Verwaltung unter Aufsicht des Herstellers (bei Abschriften des Auftraggebers, bei Ablichtungen/Abdrucken der überwachenden Person) zu vernichten. Zwischenmaterial von GEHEIM oder VS-VERTRAULICH eingestuften VS ist, soweit von der Dienststellenleitung nichts anderes bestimmt ist, der zuständigen VS-Verwaltung zur Vernichtung zu übergeben; einer Aufsicht bedarf es nicht.

(5) VS auf Datenträgern sind mittels vom BSI dafür zugelassener Produkte zu löschen. Sofern keine zugelassenen Produkte verfügbar sind, können bis zu deren Bereitstellung handelsübliche, für den Zweck der sicheren Löschung entwickelte Produkte verwendet werden. Ist die sichere Löschung elektronisch nicht möglich (z. B. wegen Defekts), so sind die Datenträger physikalisch so zu zerstören, dass eine Rekonstruktion der enthaltenen Information nicht möglich ist.

Zu Absatz 1:
Das BSI legt auf der Grundlage des Standes der Technik, eigener sowie ggf. nachrichtendienstlicher Erkenntnisse die Anforderungen fest, die zur Erfüllung der Forderungen gemäß Satz 2 erforderlich sind.
Für die Vernichtung von VS dürfen nur Produkte eingesetzt werden, die vom BSI als dafür geeignet benannt wurden.

Zu Absatz 4:
Die Regelung in Satz 2 soll eine Kontrolle des VS-Zwischenmaterials ermöglichen. In Bereichen, in denen häufig größere Mengen VS-Zwischenmaterial anfallen (z.B. in Druckereien), ist eine Vernichtung an Ort und Stelle angezeigt

IV. Materielle und technische Maßnahmen

§ 29 Räumliche Sicherheitsmaßnahmen

(1) VS-IT-Räume und andere Räume, in denen VS-VERTRAULICH und höher eingestufte VS unkryptiert verarbeitet werden, sind gegen unbemerkten Zutritt Unbefugter zu schützen.

(2) Mit der Verwaltung, Bearbeitung oder sonstigen Behandlung von VS befasste Organisationseinheiten und Personen sind nach Möglichkeit räumlich zusammenzufassen.

(3) Sofern Umfang und Bedeutung der VS es erfordern, sind mit Zustimmung der zuständigen Obersten Bundesbehörde Sicherheitsbereiche zu bilden. Diese sind durch personelle, organisatorische und technische Maßnahmen gegen den Zutritt durch Unbefugte zu schützen. Zutritt zu diesen Bereichen darf nur an Stellen möglich sein, an denen eine zuverlässige Prüfung der Zutrittsberechtigung stattfindet. Als Sicherheitsbereiche kommen sowohl einzelne oder mehrere Räume als auch Gebäude oder Gebäudegruppen in Betracht.

(4) Für VS-IT-Räume gilt die Zustimmung der zuständigen Obersten Bundesbehörde nach Absatz 3 als gegeben.

(5) Die in einem Sicherheitsbereich tätigen Personen sind beim Betreten des Sicherheitsbereiches anhand des Dienstausweises oder auf andere geeignete Weise zu identifizieren. Besucher sind nach Identitätsfeststellung während des Aufenthalts im Sicherheitsbereich zu beaufsichtigen. Bei Besuchern, die nachweislich (z. B. durch eine Konferenzbescheinigung nach Anlage 3, Muster 9) nach dem Sicherheitsüberprüfungsgesetz und den allgemeinen Verwaltungsvorschriften zur Durchführung von Sicherheitsüberprüfungen überprüft sind, kann die Beaufsichtigung entfallen. Fremdpersonal (Handwerker, Reinigungskräfte usw.) ist gemäß dem Sicherheitsüberprüfungsgesetz und den allgemeinen Verwaltungsvorschriften zur Durchführung von Sicherheitsüberprüfungen zu überprüfen und, soweit erforderlich, zu beaufsichtigen. In Ausnahmefällen genügt eine Beaufsichtigung.

(6) Das Kontrollpersonal ist über alle Arten von Ausweisen, die zum Betreten des Sicherheitsbereiches berechtigen, zu unterrichten. Die Aufgaben sind in einer Dienstanweisung festzulegen. Besucherausweise und ähnliche Aufzeichnungen sind zwei Jahre aufzubewahren.

(7) Verfügt eine Dienststelle über einen Sicherheitsbereich nach Absatz 3, sollen (soweit erforderlich) abhörgeschützte und abhörsichere Besprechungsräume möglichst in diesem Sicherheitsbereich eingerichtet werden.

Zu Absatz 1:
Die materiellen und organisatorischen Vorkehrungen zum Schutz von VS-IT-Räumen in den Hinweisen des BSI sind zu beachten.

Zu Absatz 3:
In der Regel ist die Aufbewahrung und Sicherung von VS gemäß § 17 VSA ausreichend. Die Bildung von Sicherheitsbereichen wird erst erforderlich, wenn dem Risiko von Verstößen (nicht verschlossenes Zimmer oder VS-Verwahrgelass) sowie von Angriffen technischer Art (Manipulation von Geräten, Abhören) aufgrund der hohen Konzentration von VS und ihrer Bedeutung durch zusätzliche Maßnahmen (Besucherkontrolle usw.) begegnet werden soll.
Die für die Bildung von Sicherheitsbereichen erforderliche Zustimmung der obersten Bundesbehörden im Einvernehmen mit dem Bundesministerium des Innern ist bereits durch § 1 Abs. 2 Nr. 3 SÜG vorgegeben.

Zu Absatz 5:
Eine Identifizierung „auf andere geeignete Weise“ ist z.B. gegeben, wenn Personen dem Kontrollpersonal als Dienststellenangehörige persönlich bekannt sind.

Das „Beaufsichtigen“ von Besuchern hat zum Ziel, zu verhindern, dass diese sich unbefugt Zugang zu VS verschaffen (z.B. durch Mitnahme oder Fotografieren unbeaufsichtigter VS oder den Einbau von Abhörvorrichtungen). Bei der Form der Beaufsichtigung bleibt unter Berücksichtigung der örtlichen Gegebenheiten ein Ermessensspielraum. So kann es z.B. genügen, durch Voranmeldung von Besuchern (ggf. i. V. m. einem Besucherschein) deren Aufenthalt im Sicherheitsbereich zu kontrollieren.
Als „Besucher“ ist jede Person anzusehen, deren ständiger Arbeitsbereich nicht innerhalb des Sicherheitsbereichs liegt. Dies gilt für Angehörige fremder Dienststellen und denen der eigenen Dienststelle gleichermaßen.
Auf das „Beaufsichtigen“ kann nur verzichtet werden, wenn die betreffende Person sicherheitsüberprüft ist. Der (auch wiederholte) Besuch in einem Sicherheitsbereich bildet jedoch keine Voraussetzung, um - zur Vermeidung der Beaufsichtigung – eine Sicherheitsüberprüfung durchzuführen.

Um Mehrfachüberprüfungen von Fremdpersonal zu vermeiden, sollte beim Bundesministerium für Wirtschaft oder bei den jeweiligen Firmen oder den betroffenen Personen nachgefragt werden, ob und ggf. durch welche Behörde bereits eine Sicherheitsüberprüfung veranlasst wurde. Es genügt dann eine Bestätigung durch die Stelle, welche die Sicherheitsüberprüfung veranlasste, dass diese ohne negative Erkenntnisse durchgeführt wurde.

§ 30 Technische Sicherung von VS

(1) Technische Mittel zur Sicherung von VS müssen vom BSI auf die Erfüllung der in Absatz 2 genannten Anforderungen geprüft und für geeignet befunden worden sein. Im Einzelfall kann das BSI auch dem Einsatz anderer technischer Mittel zustimmen, soweit diese einen vergleichbaren Schutz bieten.

(2) Die nachstehend genannten technischen Mittel zur Sicherung von VS müssen folgenden Anforderungen entsprechen:

1. VS-Verwahrgelasse und VS-Schlüsselbehälter müssen so beschaffen sein, dass
   a) ein Zugang einer Person zum Inhalt erst nach deren zuverlässiger Identifizierung/Authentisierung durch Besitz und Wissen möglich ist; Besitz (z. B. Schlüssel) soll gegen Nachfertigung durch Unbefugte geschützt sein; anstelle von Besitz oder Wissen oder ergänzend können auch biometrische Merkmale genutzt werden;
   b) ein Zugriff Unbefugter auf den Inhalt erkennbar wird und
   c) ein angemessener Schutz gegen gewaltsamen Zugriff auf den Inhalt gegeben ist.

2. Alarmanlagen müssen so beschaffen und installiert sein, dass

a) sie einen Eindringling sicher erkennen,
b) sie erst nach zuverlässiger Identifizierung/Authentisierung einer Person durch Besitz und Wissen durch diese unscharf geschaltet werden können; anstelle von Besitz oder Wissen oder ergänzend können auch biometrische Merkmale genutzt werden;
c) der Alarm sicher zu der zu alarmierenden Stelle übertragen wird und
d) die Alarmanlage nicht unbemerkt überwunden werden kann.

3. VS-Transportbehälter und Verpackungen für Briefe/Pakete müssen so beschaffen sein, dass ein Zugriff Unbefugter auf den Inhalt erkennbar wird.

4. Türen, Türschlösser oder elektronische Zutrittskontrollsysteme für abhörgeschützte/abhörsichere Räume oder für Zugänge zu nicht ständig besetzten Sicherheitsbereichen müssen so beschaffen sein, dass ein Zutritt Unbefugter erkennbar wird; Schlüssel oder andere Zugangsmittel müssen vor Nachfertigung durch Unbefugte geschützt sein.

(3) Die Dienststelle hat zu veranlassen, dass die zum Schutz von VS eingesetzten technischen Mittel bei der Planung bzw. erstmaligen Nutzung von VS-Aktensicherungsräumen und Alarmanlagen zum Schutz von VS grundsätzlich sowie darüber hinaus gelegentlich stichprobenweise und bei Manipulationsverdacht durch das BSI auf korrekte Ausführung und mögliche Manipulation überprüft werden. Absatz 1 gilt entsprechend.
(4) In Wiederanlauf-Vorkehrungen bei größeren IT-Systemen sind die erforderlichen Geheimschutzmaßnahmen einzubeziehen.

Zu § 30 Abs. 2 Ziffer 1a VSA:
Abweichend von dem Vorschriftentext erfolgt bei VS-Schlüsselbehältern die Identifizierung/Authentisierung nur durch Wissen (Zugelassenes Zahlenkombinationsschloss oder gleichwertige Komponente).

§ 31 Bewachung und technische Überwachung von VS

(1) Die Bewachung eines

1. VS-Verwahrgelasses ist gegeben, wenn mindestens zwei Personen bei Aufenthalt in Sichtweite unmittelbar oder außer Sichtweite mit technischen Hilfsmitteln Angriffe erkennen können und in der Lage sind, entweder selbst einen Angriff abzuwehren (z. B. mit Waffengewalt) oder ihn hilfeleistenden Abwehrkräften sofort zu melden;

2. Gebäudes ist gegeben, wenn während einer Wachschicht mehrfach in unregelmäßigen Zeitabständen kontrolliert wird oder wenn mit technischen Mitteln Angriffe erkannt und mit Abwehrkräften abgewehrt werden können.

(2) Die technische Überwachung eines

1. VS-Verwahrgelasses ist gegeben, wenn es durch eine Alarmanlage überwacht wird, die jeden Angriff erkennt und hilfeleistenden Abwehrkräften sofort meldet;

2. Gebäudes ist gegeben, wenn es durch eine Alarmanlage überwacht wird, die ein Eindringen Unbefugter erkennt und hilfeleistenden Abwehrkräften sofort meldet.

(3) Näheres über Art und Umfang der Bewachung und technischen Überwachung legt der oder die Geheimschutzbeauftragte unter Berücksichtigung des Schutzziels für die jeweiligen VS-Verwahrgelasse und Gebäude fest.

Das Bewachen bzw. technische Überwachen der VS-Verwahrgelasse dient dazu, einen möglichen gewaltsamen Zugriff auf die VS abzuwehren und einen konspirativen Zugriff zusätzlich zu erschweren.
Ist nur das Gebäude oder der Gebäudeteil bewacht oder technisch überwacht, so dürfen die VS nur vorübergehend aufbewahrt werden. Eine Bewachung bzw. technische Überwachung eines Gebäudes kann auch im Hinblick auf mögliche “Innentäter” in der Regel nicht so wirksam wie die eines VS-Verwahrgelasses sein. Bei einer nur vorübergehenden Aufbewahrung (z.B. zur Bearbeitung über einige Tage) weiß ein potentieller Täter in der Regel nicht, ob und ggf. welche VS er vorfindet. “Vorübergehend“ bedeutet, dass sich die einzelnen VS i. d. R. nur für kurze Zeit in dem VS-Verwahrgelass befinden.

Eine Alarmierung über eine Alarmanlage muss einen sofortigen Einsatz von hilfeleistenden Kräften (z. B. Polizei bei Aufschaltung auf den Polizeinotruf) initiieren. Die hilfeleistenden Kräfte müssen in der Lage sein, den Zugriff auf die VS abzuwehren. Bei den mechanischen und technischen Absicherungsmaßnahmen sind die allgemeinen Anmarschzeiten der hilfeleistenden Stellen zu berücksichtigen.

Die Durchführung der Maßnahmen von hilfeleistenden Kräften vor Ort haben sich auch bei privaten Wachdiensten an den einschlägigen Hinweisen zur Eigensicherung (z. B. Leitfaden Nr. 371 zur PDV 100) zu orientieren.

§ 32 Abhörschutzmaßnahmen

(1) Das Bundesministerium des Innern legt im Einvernehmen mit den Obersten Bundesbehörden die Dienststellen fest, in denen aufgrund des Umfangs und der Bedeutung von VS sowie der Aufgabenstellung eine besondere Abhörgefahr besteht. Bei Dienststellen nach § 45 gilt die besondere Abhörgefahr als gegeben.

(2) Dienststellen nach Absatz 1 haben Vorkehrungen zu treffen, damit ihre Telekommunikations- und Informationstechnik nicht dazu missbraucht werden kann, um Raum- und Telefongespräche abzuhören.

(3) In Dienststellen nach Absatz 1 legen die Geheimschutzbeauftragten die Räume fest, in denen aufgrund des Umfangs und der Bedeutung der dort geführten Gespräche eine besondere Abhörgefahr besteht. Bei Räumen, in denen nicht nur ausnahmsweise Gespräche mit GEHEIM oder STRENG GEHEIM eingestuftem Inhalt geführt werden, gilt die besondere Abhörgefahr als gegeben.

(4) Räume nach Absatz 3 müssen abhörgeschützt oder abhörsicher sein. Diese Räume müssen mindestens

1. ***vor unbemerktem Zutritt Unbefugter geschützt sein,***
2. ***eine akustische Dämpfung aufweisen, die ein Mithören von außen ohne technische Hilfsmittel hinreichend ausschließt,***
3. ***bei Ausstattung mit Kommunikationseinrichtungen Vorkehrungen enthalten, damit Raumgespräche nicht über diese Einrichtungen abgehört werden können,***
4. ***so gestaltet sein (Einrichtungen, Installationen usw.), dass Versteckmöglichkeiten für Abhörgeräte nach Möglichkeit beschränkt sind und technische Prüfungen nach Absatz 5 wirksam und in angemessener Zeit durchgeführt werden können und***
5. ***Vorkehrungen enthalten, damit Leitungen, die in diese Räume führen, nicht für Abhörzwecke missbraucht werden können.***

Abhörsichere Räume sind darüber hinaus so zu gestalten, dass auch eine unbefugte Übertragung von Gesprächen mittels technischer Hilfsmittel (Abhörgeräten) nach außen verhindert wird.

(5) In Dienststellen nach Absatz 1 sind nach Fertigstellung und anschließend regelmäßig sowie bei Manipulationsverdacht technische Prüfungen durchzuführen, um festzustellen, ob
1. ***Telekommunikations- oder IT-Einrichtungen für Abhörzwecke missbraucht werden können oder***
2. ***in den Räumen nach Absatz 3 Abhöreinrichtungen vorhanden sind und***
3. ***die Anforderungen der Technischen Leitlinien nach Absatz 8 erfüllt sind.***

(6) Bei Abhörverdacht oder aus Anlass von Konferenzen auf höherer Ebene oder von besonderer Bedeutung sollen ebenfalls technische Prüfungen nach Absatz 5 durchgeführt werden. In diesem Fall ist der Umfang der Prüfung mit dem oder der Geheimschutzbeauftragten bzw. sonstigen Verantwortlichen in Abhängigkeit von den örtlichen und zeitlichen Gegebenheiten und der spezifischen Bedrohungslage abzustimmen.

(7) Für die nach den Absätzen 5 und 6 geforderten technischen Prüfungen haben die Dienststellen die für die Prüfungen erforderliche Unterstützung zu gewähren.

(8) Zu Sicherheitsvorgaben für abhörsichere und abhörgeschützte Räume sowie Konferenzen auf höherer Ebene oder von besonderer Bedeutung und zur Umsetzung der Abhörschutzmaßnahmen gibt das BSI im Einvernehmen mit dem Bundesministerium des Innern Technische Leitlinien heraus.

Zu Absatz 8:
Das BSI ist bereits bei der Planung von abhörgeschützten und abhörsicheren Räumen zu beteiligen.

§ 33 Sicherung von Schlüsseln und sonstigen Zugangsmitteln zu VS

(1) Schlüssel zu VS-Verwahrgelassen, für VS-IT-Räume, abhörgeschützte und abhörsichere Räume und zum Ein- und Ausschalten von Alarmanlagen zur technischen Sicherung von VS sind während des Dienstes in persönlichem Gewahrsam zu halten, sofern sie nicht nach Satz 2 verwahrt werden. Vor Verlassen des Dienstgebäudes sind sie grundsätzlich in einem VS-Verwahrgelass oder VS-Schlüsselbehälter zu verschließen.

(2) VS-Schlüsselbehälter sind möglichst zu bewachen. Wird ein VS-Schlüsselbehälter von mehreren Personen benutzt, so muss er mit Schließfächern ausgerüstet sein, in denen die Benutzer ihre Schlüssel getrennt unterbringen. Dies gilt nicht bei gemeinsamer Benutzung von VS-Verwahrgelassen oder Alarmanlagen. Die Schlüssel zu den Schließfächern verbleiben im persönlichen Gewahrsam der Schließfachbenutzer.

(3) IT-Systeme, die für VS eingesetzt werden, müssen über ein zuverlässiges Zugangs-/Zugriffskontrollsystem verfügen, so dass nur Befugte im Rahmen der ihnen erteilten Rechte Zugang erhalten und auf VS zugreifen können. Wiederholte abgewiesene Zugangs-/Zugriffsversuche sollen für den betreffenden Nutzer zur Systemsperrung führen. Diese darf nur von dem für IT-Geheimschutzmaßnahmen Verantwortlichen oder einer von ihm beauftragten Person aufgehoben werden.

(4) Bei der Vergabe, Änderung und Rücknahme von Rechten muss gewährleistet sein, dass

1. ein dazu erforderlicher Antrag von einer berechtigten Stelle stammt,

2. die zu berechtigende Person eine ausreichende VS-Ermächtigung besitzt,

3. der Grundsatz "Kenntnis nur, wenn nötig" beachtet wird und

4. keine bezüglich der Sicherheit unvereinbare Bündelung von Funktionen entsteht.

Die Übertragung der Befugnis zur Vergabe und Änderung von Rechten ist zu dokumentieren und bedarf der Zustimmung der Geheimschutzbeauftragten. Die Dokumentation ist mindestens 5 Jahre aufzubewahren.

(5) Die Verwendung gegenständlicher Zugangsmittel zu IT-Systemen und Komponenten (Magnet- und Chip-Karten, Dongel[7], Lochstreifen usw.) sowie Einzelheiten über die Auswahl, Vergabe, Kontrolle und den Wechsel von Kennworten/PIN sollen in einer Dienstanweisung festgelegt sein.

Zu Absatz 1:
Mit Satz 1 soll nicht ausgeschlossen werden, dass die dort genannten Schlüssel auch während der Dienstzeit in VS-Schlüsselbehältern verwahrt werden (Satz 2).

Die Formulierung „grundsätzlich“ in Satz 2 lässt in begründeten Fällen Ausnahmen zu. So ist auch eine Aufbewahrung in einem Bankschließfach oder in einem versiegelten Umschlag unter Bewachung (i. S. von § 31 Abs. 1, 1. Halbsatz) möglich.

Zu Absatz 5:
Gegenständliche Zugangsmittel zu IT-Systemen und –Komponenten sollten grundsätzlich wie Schlüssel zu VS-Verwahrgelassen behandelt werden.

§ 34 Zahlenkombinationen als Zugangsmittel zu VS

(1) Die Zahlenkombination zum Zugang eines VS-Verwahrgelasses oder VS-Schlüsselbehälters oder zum Ein- und Ausschalten einer Alarmanlage darf nur den Benutzern bekannt sein. Sie darf nicht aus leicht zu ermittelnden Zahlen oder Zusammenstellungen, z. B. persönlichen Daten, Fernsprechnummern oder arithmetischen Reihen, bestehen.

(2) Die Zahlenkombination ist schriftlich aufzuzeichnen und den mit ihrer Verwaltung Beauftragten in einem versiegelten Umschlag zu übergeben. Die Umschläge sind mindestens wie eine VS-VERTRAULICH eingestufte VS aufzubewahren. Weitere Aufzeichnungen der Zahlenkombination sind unzulässig.

(3) Die Zahlenkombinationen von VS-Verwahrgelassen oder VS-Schlüsselbehältern oder zum Ein- und Ausschalten von Alarmanlagen sind zu ändern:

1. ***nach Beschaffung,***
2. ***bei Wechsel der Benutzer,***
3. ***nach Öffnung in Abwesenheit der Benutzer,***
4. ***wenn der Verdacht besteht, dass die Zahlenkombination Unbefugten bekannt geworden ist,***
5. ***regelmäßig alle 12 Monate oder häufiger.***

Außer den Benutzern können mit Zustimmung der Geheimschutzbeauftragten auch die zuständigen VS-Verwalter in Anwesenheit der Benutzer die Änderungen vornehmen.

(4) Reserveschlüssel und die Aufzeichnungen der Zahlenkombinationen sind in getrennten VS-Verwahrgelassen (Reserveschlüssel auch in VS-Schlüsselbehältern) in beschrifteten und versiegelten Umschlägen aufzubewahren. Sie sind durch verschiedene Personen zu verwalten, wenn die Verwalter nicht ohnehin Zugang zu den gesicherten VS haben (z. B. VS-Verwalter und Vertreter). Die Zahlenkombinationen der VS-Schlüsselbehälter sind getrennt von den Zahlenkombinationen der VS-Verwahrgelasse aufzubewahren und zu verwalten.

(5) Für Kennworte, PIN und andere Zeichenkombinationen für den Zugang zu Computern und elektronischer Informationstechnik, auf denen VS verarbeitet werden, gelten die vorstehenden Absätze sinngemäß. Näheres ist im Geheimschutzkonzept der Dienststelle festzulegen.

Zu Absatz 1:
Benutzer eines VS-Verwahrgelasses können mehrere Personen gleichzeitig sein (vgl. § 17 Abs. 7 VSA). Dies gilt auch für VS-Schlüsselbehälter.

Unter „Zahlenkombination“ fallen auch die Zahlen für elektronische Codeschalter von Alarmanlagen.

Zu Absatz 2:
Ein „Wechsel des Benutzers“ liegt auch vor, wenn im Falle des § 17 Abs. 7 VSA nur einer der gemeinsamen Benutzer ausscheidet oder wechselt.

Satz 2 trägt den praktischen Erfordernissen in Behörden mit einer großen Zahl von VS-Verwahrgelassen Rechnung. Die Regelung ist bezüglich des Geheimschutzes unbedenklich, da der zuständige VS-Verwalter – nur er ist hier angesprochen – ohnehin Zugang zu den VS hat (bis auf wenige Ausnahmen, vgl. § 26 Abs. 2 VSA). Im Übrigen besitzt er nur die Zahlenkombination, nicht aber den Schlüssel zum VS-Verwahrgelass. VS-Verwahrgelasse, die den Geheimschutzanforderungen entsprechen, sind überdies mit einem Zählwerk versehen. Der VS-Bearbeiter kann insoweit kontrollieren, ob sein VS-Verwahrgelass in seiner Abwesenheit geöffnet wurde.

§ 35 Planung, Beschaffung und Abnahmeprüfung

(1) Dienststellen, die VS nicht nur gelegentlich verwenden, haben für sämtliche Geheimschutzmaßnahmen ein gemeinsames Konzept entsprechend Anlage 5 zu erstellen, in dem die spezifischen Gegebenheiten der Dienststelle berücksichtigt sind.

(2) Bei der Planung und Durchführung von Baumaßnahmen sind rechtzeitig die notwendigen Geheimschutzvorkehrungen zu treffen. Näheres bestimmen die „Richtlinien für die Durchführung von Bauaufgaben des Bundes“ (RBBau), Anhang 20/1 (RiSBau).

(3) Bei der Planung und Abnahmeprüfung von VS-Aktensicherungsräumen, Alarmanlagen zum Schutz von VS, Telekommunikationsanlagen und abhörsicheren oder abhörgeschützten Räumen ist das BSI, im Geschäftsbereich des Bundesministeriums der Verteidigung das Amt für den Militärischen Abschirmdienst , beratend hinzuzuziehen.

(4) Ist geplant, IT für VS einzusetzen, so sind die Geheimschutzbeauftragten und deren Verantwortliche mit IT-Fachkenntnissen bereits zu Planungsbeginn zu beteiligen. Bei komplexen IT-Systemen oder besonderen IT-Anwendungen für VS ist das BSI, im Geschäftsbereich des Bundesministeriums der Verteidigung das Amt für den Militärischen Abschirmdienst, bereits bei Planungsbeginn beratend hinzuzuziehen.

(5) Bei der Beschaffung von IT, die für VS eingesetzt werden soll, ist in die Beschaffungsaufträge aufzunehmen, welche IT-Sicherheitsfunktionen das IT-System enthalten muss und welche Sicherheitsleistungen die IT-Hersteller oder Vertreiber zu erbringen haben. Es ist insbesondere sicherzustellen, dass

1. ***Produkte mit IT-Sicherheitsfunktionen die erforderliche Zulassung aufweisen und sicherheitsgerecht implementiert werden,***
2. ***Produkte mit IT-Sicherheitsfunktionen ab dem Zeitpunkt, zu dem feststeht, dass sie für VS eingesetzt werden sollen, geschützt aufbewahrt und transportiert werden,***
3. ***eine sicherheitsgerechte Wartung und Instandsetzung erfolgt,***
4. ***bei Vergabe des IT-Einsatzes an Dritte die erforderlichen Geheimschutzmaßnahmen erfolgen.***

Zu Absatz 2:

Ziel ist es, rechtzeitig festzulegen, inwieweit Sicherheitsüberprüfungen (z.B. bei Bauarbeiten in Sicherheitsbereichen) durchzuführen und/oder bauliche oder technische Sicherheitsvorkehrungen (z.B. Einrichtung abhörgeschützter oder abhörsicherer Räume) zu beachten sind.

V. IT-spezifische Maßnahmen

§ 36 Freigabe und Betrieb von IT-Systemen

(1) Bevor IT-Systeme erstmals für VS eingesetzt werden, haben die Geheimschutzbeauftragten eine Überprüfung zu veranlassen, ob die erforderlichen Geheimschutzmaßnahmen getroffen sind. Zur Unterstützung können die Geheimschutzbeauftragten das BSI hinzuziehen, bei komplexen IT-Systemen oder vielfältigen IT-Anwendungen soll das BSI beratend hinzugezogen werden.

(2) Die Verarbeitung von VS ist nur mit solchen IT-Systemen zulässig, die ausschließlich von der Dienststellenleitung freigegebene Hard- und Software verwenden. Die Freigabe ist zu dokumentieren.

(3) Geheimschutzrelevante Änderungen bei freigegebenen IT-Systemen, insbesondere der Einsatz für höher eingestufte VS, bedürfen der vorherigen Zustimmung der zuständigen Geheimschutzbeauftragten, die vor wesentlichen Änderungen nach Absatz 1 und 2 verfahren.

(4) *Für den Betrieb der IT-Systeme gelten § 4 Absatz 3 und § 18 Absatz 2 sinngemäß*.

§ 37 Produkte mit IT-Sicherheitsfunktionen zur Verwendung für VS

(1) Produkte mit Funktionen zur

1. ***Herstellung von Schlüsselmitteln,***
2. ***Verschlüsselung (Kryptierung),***

3. ***Löschung oder Vernichtung von VS-Datenträgern,***
4. ***Abstrahlsicherheit oder***
5. ***Sicherung von Übertragungsleitungen,***
6. ***Trennung von Netzen mit unterschiedlichen maximalen Einstufungen der verarbeiteten VS***

müssen vom BSI zugelassen sein. Die Zulassung hat auch die erforderlichen Angaben zu den Einsatz- und Betriebsbedingungen zu enthalten. Die Nummern 3 bis 6 gelten nicht für VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS.

(2) Produkte mit Funktionen zur

1. ***Zugangs-/Zugriffskontrolle zu den Systemen,***
2. ***Erstellung von VS,***
3. ***Protokollierung/Beweissicherung und Protokollauswertung oder***
4. ***Abwehr von Manipulationen an IT-Systemen,***
5. ***Registratur und zum Bestandsnachweis,***

die für VS-VERTRAULICH und höher eingestufte VS verwendet werden, sollen vom BSI zugelassen sein. Die Dienststellenleitung kann die Verwendung anderer Produkte freigeben, insbesondere wenn sich Produkte zum Zeitpunkt des Inkrafttretens dieser Vorschrift bereits im Einsatz oder in der Beschaffung befinden oder keine geeigneten zugelassenen Produkte verfügbar sind und eine Bereitstellung nicht oder nicht zeitgerecht veranlasst werden kann. Hierzu zählen insbesondere nach Common Criteria[8] mit nationalen Schutzprofilen durch das BSI zertifizierte Produkte. Bis zur Bereitstellung nationaler Schutzprofile können auch andere durch das BSI zertifizierte Produkte verwendet werden. Zur Auswahl der alternativen Produkte ist der Beschaffungsleitfaden des BSI zu verwenden. Eine Beratung durch das BSI ist empfohlen.

(3) Die Zulassungen erfolgen abgestuft nach der Schutzbedürftigkeit von IT-Anwendungen für VS auf der Grundlage allgemein anerkannter Sicherheitskriterien und Verfahren, die bei Bedarf um besondere Prüfungen zum Schutz vor Angriffen zu ergänzen sind. Die näheren Einzelheiten legt das BSI in einem Zulassungskonzept fest, das der Billigung des Bundesministeriums des Innern bedarf.

(4) Produkte mit IT-Sicherheitsfunktionen sind ab dem Zeitpunkt, zu dem feststeht, dass sie für VS-VERTRAULICH oder höher eingestufte VS eingesetzt werden sollen,

1. ***in Räumen nach § 29 Abs. 1 oder entsprechend geschützten Räumen aufzubewahren,***
2. ***unter ständiger Kontrolle von nach § 10 Abs. 3 und 4 ermächtigtem oder zugelassenem Personal zu transportieren oder so zu verpacken, dass ein Zugriff Unbefugter erkennbar wird,***
3. ***durch nach § 10, Absätze 3 und 4 ermächtigtes oder zugelassenes Personal zu installieren, zu warten und instand zu setzen, soweit nicht durch organisatorische Maßnahmen (z. B. keine Verarbeitung/Übertragung von VS in Anwesenheit der Personen und Beaufsichtigung dieser) ein Zugang zu VS auszuschließen ist, und***
4. ***in einem Bestandsverzeichnis nachzuweisen.***

Zu Absatz 1:
Eine regelmäßig aktualisierte „Liste der zugelassenen IT-Sicherheitsprodukte und –Systeme“ sowie ein weiteres Dokument „Produkte für die materielle Sicherheit“ werden vom BSI herausgegeben.

Zu Absatz 2:
Unter Zulassung versteht man die Prüfung und Bewertung der IT-Sicherheit von IT-Systemen oder -Komponenten für die Verarbeitung und Übertragung von VS unter Berücksichtigung besonderer Belange des staatlichen Geheimschutzes. Grundlage ist das in Absatz 3 definierte Zulassungskonzept des BSI. Der Antrag auf Zulassung kann grundsätzlich nur von einem behördlichen Anwender gestellt werden.
Demgegenüber kann eine Zertifizierung, d.h. eine Prüfung und Bewertung der IT-Sicherheit, für alle IT-Systeme oder -Komponenten durchgeführt werden. Basis sind international anerkannte IT-Sicherheitskriterien. Ziel der Zertifizierung ist, IT-Systeme und –Komponenten hinsichtlich ihrer Sicherheitseigenschaften transparent und vergleichbar zu machen.

Ein nationales Schutzprofil ist eine standardisierte Prüfvorschrift für bestimmte Produktklassen, z.B. Firewalls, wo ein Bedarf der nationalen Sicherheit besteht.

Zu Absatz 4:
Durch die beschriebenen Maßnahmen der Nummern 1 bis 4 soll einer nachträglichen Manipulation der für den VS-Betrieb vorgesehenen Produkte vorgebeugt werden.
Entsprechende Hinweise zur Beförderung von Produkten mit IT-Sicherheitsfunktionen sind den Hinweisen des BSI zu entnehmen.

§ 38 Abstrahlsicherheit

(1) IT-Hardware, die VS-VERTRAULICH oder höher eingestufte VS unkryptiert führt, soll unter Beachtung der Hinweise des BSI zur Abstrahlsicherheit installiert sein.

(2) Es ist durch die Geheimschutzbeauftragten unter Beachtung der Hinweise des BSI zu prüfen und durch die Dienststellenleitung zu entscheiden, inwieweit mit einer erheblichen Gefährdung der Geheimhaltung der VS- VERTRAULICH oder höher eingestuften VS durch Nutzung von kompromittierender Abstrahlung durch Unbefugte zu rechnen ist. Ist mit einer erheblichen Gefährdung zu rechnen, so muss die IT-Hardware in vom BSI zugelassenen abstrahlsicheren Räumen betrieben werden, eine Zulassung des BSI für den Betrieb innerhalb einer bestimmten Sicherheitszone (Zonenmodell) aufweisen und innerhalb einer solchen betrieben werden oder vom BSI als abstrahlsicher zugelassen sein.

Zu Absatz 1:
IT-Systeme senden wie jedes elektronische Gerät Störstrahlung aus. Diese Störstrahlung kann durch die Verarbeitung der Information beeinflusst sein und als sogenannte kompromittierende Abstrahlung die Vertraulichkeit der verarbeiteten Information gefährden. Das Risiko von kompromittierender Abstrahlung besteht zwar insbesondere bei nach dem Zonenmodell eingesetzten Geräten, da hier ein gewisses Maß an Abstrahlung bereits bei der Zulassung toleriert wird, kann jedoch aber auch bei Einsatz von abstrahlsicherer Systemen, insbesondere soweit sie nicht vorschriftsgemäß miteinander verbunden wurden, nicht grundsätzlich ausgeschlossen werden.

Zu Absatz 2:
Eine erhebliche Gefährdung ist anzunehmen, wenn eine kompromittierende Abstrahlung auftritt, die außerhalb des eigenen zutrittsgeschützten Bereichs aufgenommen werden kann und daraus die VS-Informationen weitgehend rekonstruiert werden können und unter den gegebenen Umständen realistisch damit gerechnet werden muss, dass Unbefugte die vorhandene kompromittierende Abstrahlung praktisch nutzen werden.
Bei Beurteilung der Gefahr, dass Unbefugte kompromittierende Abstrahlung erfassen und auswerten, sind folgende Aspekte zu berücksichtigen:
Häufigkeit und Dauer des VS-Einsatzes,
örtliche Gegebenheiten, die eine unbemerkte Erfassung der Abstrahlung ermöglichen oder erleichtern,
Maßnahmen mit Schutzwirkung gegen einen potentiellen Angriff,
Nutzen für Dritte, wenn sie die VS-Information besitzen.
Es ist davon auszugehen, dass bei Dienststellen (oder Teilen davon) die nach Feststellung des Bundesministeriums des Innern in besonderem Maße Ziel von Angriffen auf Vertraulichkeit, Integrität und Verfügbarkeit von VS sind (Dienststellen nach § 45 VSA) die Gefahr der Nutzung der kompromittierenden Abstrahlung durch Unbefugte grundsätzlich besteht und entsprechende Schutzmaßnahmen zu treffen haben.
Bei anderen Dienststellen ist eine solche Gefahr anzunehmen bei

- nicht nur gelegentlichem IT-Einsatz für STRENG GEHEIM eingestuften VS,
- häufigem IT-Einsatz für GEHEIM eingestufte VS oder
- bei besonders exponierter Lage der IT-Betriebsräume (z. B. in einer deutschend Vertretung im Ausland).

Von einer unerheblichen Gefährdung kann ausgegangen werden, wenn aufgrund der Gesamtumstände die Erfolgsaussichten oder der Nutzen eines Angriffs als gering anzusehen ist oder die Wahrscheinlichkeit, dass eine andere Möglichkeit der Informationsbeschaffung genutzt wird, hoch ist.

§ 39 Technische Prüfungen

(1) Geheimschutzbeauftragte haben bei IT-Systemen, die für STRENG GEHEIM oder nicht nur ausnahmsweise für GEHEIM eingestufte VS eingesetzt werden, vor dem erstmaligen Einsatz für VS und danach in angemessenen zeitlichen Abständen folgende technischen Prüfungen durch das BSI zu veranlassen:

1. ***eine Prüfung des IT-Systems unter den spezifischen Einsatzbedingungen, ob die erforderlichen IT-Sicherheitsfunktionen sachgerecht implementiert sind, keine erkennbaren Manipulationen aufweisen und auch nach Implementierung in das jeweilige IT-System wirksam greifen, nicht über einen Systemweg manipuliert oder umgangen werden können und auch bei einem Verbund mit anderen IT-Systemen diese Sicherheit aufweisen,***
2. ***Abstrahlsicherheits- und Manipulationsprüfungen bei abstrahlsicheren Räumen/Behältern, bei zonenvermessenen Räumen und bei für VS eingesetzter Hardware und***
3. ***eine Überprüfung von Sicherheitszonen auf mögliche Einrichtungen zur Erfassung oder Übertragung kompromittierender Nahbereichsabstrahlung.***

(2) Das BSI teilt die Ergebnisse der Prüfungen den Geheimschutzbeauftragten in Form von Prüfberichten mit.

(3) Bei vernetzten IT-Systemen, die für VS eingesetzt werden, ist in den Dienststellen nach § 5 Abs. 3 durch die Geheimschutzbeauftragten ein Penetrationstest[9] zu veranlassen.

Zu Absatz 1:
Die Prüfgrundlagen und die Vorgehensweise zur Überprüfung der Geheimschutzmaßnahmen sind in den Hinweisen des BSI dargestellt.

Zu Absatz 3:
Ein Penetrationstest gehört zu den Administrationstätigkeiten bei Computernetzen. Mit speziellen Diagnoseprogrammen wird geprüft, ob es möglich ist, unbefugt von außen in das Netz einzudringen oder als interner Nutzer höhere als die zugewiesenen Rechte zu erlangen. Dies kann durch Fehler bei der Administration des Computernetzes ermöglicht werden, der Penetrationstest ist daher als Teil der Administration des Computernetzes zu betrachten.
Ein Penetrationstest kann durch nachweisbar qualifizierte eigene Administratoren erfolgen. Das BSI stellt hierzu ein entsprechendes Programm bereit. Die Prüfung kann jedoch auch durch das BSI oder von spezialisierten Firmen mit sicherheitsüberprüftem Personal als Dienstleistung ausgeführt werden.

Das BSI wird eine Technische Leitlinie „Anwendung von Penetrationstests in VS-IT-Umgebungen“ bereitstellen.

§ 40 Übertragung von VS über Telekommunikations- oder andere technische Kommunikationsverbindungen

(1) VS sind bei der Übertragung über Telekommunikations- oder andere technische Kommunikationsverbindungen mit einem vom BSI für den betreffenden Geheimhaltungsgrad zugelassenen Kryptosystem zu verschlüsseln oder durch andere zugelassene Maßnahmen zu sichern. Sofern für die Verwendung bei als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS Programme und Geräte mit BSI-Zulassung nicht verfügbar sind, können auch nach Common Criteria mit nationalen Schutzprofilen durch das BSI zertifizierte Produkte verwendet werden. Bis zur Bereitstellung nationaler Schutzprofile können andere durch das BSI zertifizierte Produkte, Prüftiefe mindestens EAL 3, verwendet werden. Zur Auswahl zertifizierter Produkte ist der Beschaffungsleitfaden des BSI zu verwenden.

(2) Abweichend von Absatz 1 Satz 1 ist in folgenden Fällen eine unkryptierte Übertragung zulässig:

1. ***wenn die Erledigung der Angelegenheit dringlich ist und die schriftliche oder sonstige sichere Übermittlung einen unvertretbaren Zeitverlust bedeuten würde, kann***
   a) ***bei Telefongesprächen mit VS-VERTRAULICH eingestuftem Inhalt eine für VS-NUR FÜR DEN DIENSTGEBRAUCH zugelassene Verbindung nach Absatz 1 Satz 1 und***

b) bei Telefongesprächen mit VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuftem Inhalt eine ungeschützte Verbindung

verwendet werden. Die Gespräche sind möglichst so zu führen, dass der Sachverhalt Dritten nicht verständlich wird. Ist der Gesprächspartner nicht mit Sicherheit zu identifizieren, ist ein Kontrollanruf erforderlich. Besondere Vorsicht ist bei Funkfernsprechanschlüssen (z. B. Mobilfunk, DECT[10], Bluetooth[11]) geboten.

2. bei dringlichen E-Mails, Fernkopien und Fernschreiben des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn zwischen Absender und Empfänger für die erforderliche Übertragungsart keine Kryptiermöglichkeit und auch keine andere Schutzmöglichkeit (z. B. mittels Kennwort) besteht. Die absendende Stelle hat durch geeignete Maßnahmen vor Übertragung zu gewährleisten, dass die Nachricht den berechtigten Empfänger erreicht.

3. in außergewöhnlichen Fällen mit Einwilligung der Dienststellenleitung, bei Behörden nach § 5 Absatz 3 Satz 1 der Abteilungs- oder Unterabteilungsleitung, auch über die vorstehenden Ausnahmen hinaus bei der Übertragung von VS-VERTRAULICH oder GEHEIM eingestuften VS (sofern sie keine besondere VS-Behandlungskennzeichen wie z. B. Krypto aufweisen), wenn

a) zwischen Absender und Empfänger keine Kryptiermöglichkeit besteht und

b) eine rechtzeitige Beförderung der VS auf anderem Wege nicht möglich ist und eine Verzögerung zu einem Schaden führen würde, der den mit einer Preisgabe der VS verbundenen Schaden deutlich überwiegen würde.

Die Nachrichten sind möglichst so abzufassen, dass sie keinen unmittelbaren Rückschluss auf ihren VS-Charakter zulassen. Sie dürfen keine Kennzeichnungen oder Hinweise aufweisen, die sie von einer offenen Nachricht unterscheiden. Die Nachrichtenempfänger sind auf anderem Wege (z. B. über andere Telekommunikationsverbindungen, durch Post oder Kurier) unverzüglich über die VS-Einstufung der Nachricht zu unterrichten, außer, dies ist im Einzelfall nicht möglich oder nicht zweckmäßig.

(3) Bei der Übertragung von VS kann über die bestehenden Ausnahmen nach Absatz 2 hinaus eine Kryptierung unterbleiben

1. innerhalb eines zutrittsgeschützten IT-Betriebsraumes,

2. wenn die Übertragungseinrichtungen so geschützt sind, dass ein Zugriff Unbefugter unverzüglich erkannt wird (approved circuits)[12], oder

3. wenn in einem Netz der Dienststelle
a) VS-NUR FÜR DEN DIENSTGEBRAUCH übertragen werden,
b) nur VS-VERTRAULICH oder ausnahmsweise GEHEIM eingestufte VS übertragen werden,
c) ein Zugriffskontrollsystem nach § 37 Absatz 2 eingesetzt ist und
d) die Übertragungseinrichtungen sich vollständig in einem Bereich mit zuverlässiger Zutrittskontrolle befinden oder außerhalb gegen unmittelbaren Zugriff Unbefugter geschützt sind;

bei Verbindung mit einem anderen Kommunikationsnetz muss dieses und die Verbindung zu diesem mindestens gemäß Buchstabe c) und d) geschützt sein.

(4) Soweit die für den Betrieb eines Kryptosystems benötigten Kryptodaten (Schlüssel) nicht automatisch bereitgestellt werden, dürfen diese nur vom BSI oder durch vom BSI benannte Stellen hergestellt und verteilt werden. Für die Verwaltung von auf dem Kurier-/Postweg bereitgestellte Kryptodaten sind Kryptoverwalter/Vertreter zu bestellen. Die Kryptoverwalter geben die Kryptodaten in die Kryptosysteme ein oder bei Bedarf an die befugten IT-Nutzer aus. Namen und Behördenanschrift der Kryptoverwalter/Vertreter sowie Änderungen sind dem BSI oder den vom BSI benannten Stellen mitzuteilen.

(5) Sicherheitsvorgaben für Telekommunikationsanlagen, über die Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt unkryptiert geführt werden, bestimmt eine Technische Leitlinie, die das BSI im Einvernehmen mit dem Bundesministerium des Innern herausgibt.

(6) Bei der Kommunikation mit ausländischen oder zwischenstaatlichen Stellen (z. B. NATO) gehen die jeweiligen internationalen Bestimmungen und Abkommen vor, sofern nicht nationale Bestimmungen höhere Geheimschutzmaßnahmen erfordern.

Zu Absatz 1:
Unter „andere technische Kommunikationsverbindungen“ fallen z. B. nichtöffentliche Verbindungen außerhalb von Sicherheitsbereichen über Richtfunk, WLAN oder den Kurzstreckenfunk Bluetooth.

Bei Kommunikation zwischen Dienststellen, die über den Informationsverbund Bonn/Berlin (IVBB)erfolgt, besteht zwischen Absender- und Empfängerbehörde eine den Anforderungen an eine Übertragung von VS-NUR FÜR DEN DIENSTGEBRAUCH entsprechende zugelassene Verschlüsselung. Bei Kommunikation mit Dienststellen, die nicht unmittelbar an den IVBB angeschlossen sind, ist außer in Fällen gemäß § 40 Absatz 2 eine Übertragung nur mittels zugelassener Verschlüsselung zulässig.

Zu Absatz 2 Nr. 1b:
Funkverbindungen und drahtlose Telefone aller Art können leicht von Unbefugten empfangen bzw. abgehört werden, auch Bluetooth, WLAN usw. mit entsprechenden Antennen u.U. über einige km. Außerdem kann durch Störsender die Verbindung unterbrochen werden, wodurch der Zugriff auf die VS nicht mehr gesichert ist (siehe „Verfügbarkeit“ in § 4).

Zu Absatz 3 Nr. 3:

Bei unverschlüsselter Übertragung von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS innerhalb einer Liegenschaft von Dienststellen sind für die Zugangs- und Zugriffskontrolle zum IT-System die Regelungen des IT-Grundschutzes anzuwenden. Sofern sich die Dienstgebäude auf unterschiedlichen Liegenschaften befinden, ist die Übertragung zu verschlüsseln.

Zu Absatz 4:
Kryptoverwalter sind auch für die Verwaltung der Kryptotechnik zu bestellen, sofern deren Umfang es erfordert. Anderenfalls nehmen die Geheimschutzbeauftragten diese Aufgabe wahr. Die Pflicht zur Meldung der verantwortlichen Personen an das BSI gilt entsprechend.

§ 41 Wartung und Instandsetzung von Informationstechnik für VS-VERTRAULICH oder höher eingestufte VS

(1) Vor Wartungs- oder Instandsetzungsarbeiten sollen diese VS aus dem IT-System entfernt werden. Ist dies nicht möglich, ist nach § 10 Absätze 3 und 4 ermächtigtes oder zugelassenes Wartungs- oder Instandsetzungspersonal einzusetzen. Während der Verarbeitung oder Übertragung von VS ist eine Wartung oder Instandsetzung des IT-Systems grundsätzlich nicht zulässig.

(2) Eine Fernwartung ist nur zulässig, wenn

1. ***sie durch nach § 10 Abs. 3 und 4 ermächtigtes oder zugelassenes Personal erfolgt,***
2. ***für die Übertragungen im Rahmen der Fernwartung Kryptosysteme eingesetzt sind,***
3. ***eine zuverlässige Zugriffskontrolle, Beweissicherung und Überprüfung der Protokolle erfolgt und***
4. ***eine gesonderte Freischaltung und Beendigung jedes Fernwartungsvorganges durch die Dienststelle erfolgt.***

Die Fernwartung soll nur zu Zeiten erfolgen, zu denen keine Arbeit mit VS stattfindet und wenn alle im IT-System zugänglichen VS-Daten kryptiert oder gelöscht sind.

(3) Die Geheimschutzbeauftragten können abweichend von Absatz 2 zulassen, dass ein Unternehmen die Fernwartung durchführt, wenn

1. ***ihm ein Sicherheitsbescheid des Bundesministeriums für Wirtschaft und Technologie über das Unternehmen vorliegt oder eine andere Oberste Bundesbehörde für die erforderlichen Geheimschutzmaßnahmen bei dem Unternehmen gesorgt hat,***

2. ***eine gesonderte Freischaltung und Beendigung jedes Fernwartungsvorganges und Monitoring durch die Dienststelle erfolgt und***

3. ***nach Absatz 2 Satz 1 Nr. 2 bis 3 und Satz 2 verfahren wird,***

4. ***mit der Firma zuvor ein Vertrag oder eine Vertragsergänzung über die erforderlichen Sicherheitsmaßnahmen abgeschlossen wurde.***

(4) Sofern VS-Informationstechnik die Dienststelle verlässt (Defekt, Ende eines Leasing-Vertrages o.Ä.), sind auf internen Datenträgern gespeicherte VS mit vom BSI zugelassenen Geräten oder Programmen zu löschen. Ist dies nicht möglich, sind die Datenträger auszubauen und physikalisch so zu zerstören, dass eine Rekonstruktion der enthaltenen Information nicht möglich ist.

Zu Absatz 2:
Die in der Fernwartung auftretenden Risiken, z.B. Eindringen nicht autorisierter Personen in das IT-System, Einbringen von Sicherheitslücken in IT-Systeme, können nur durch eine sorgfältige Abstimmung technischer und organisatorischer Maßnahmen gering gehalten werden.
Da eine Fernwartung nur zu Zeiten zulässig ist, zu denen keine Arbeit mit VS stattfindet und wenn alle im IT-System zugänglichen VS-Daten kryptiert oder gelöscht sind, ist das Ausspähen von Daten nicht möglich.
Das Einbringen von Sicherheitslücken in das IT-System oder die Installation von fehlerhafter Software stellt ein Risiko dar, welches durch die Formulierungen gemäß Abs. 2 Satz 1 bzw. Satz 3 minimiert wird. Weiterhin wird für IT-Systeme, die für STRENG GEHEIM und nicht nur ausnahmsweise für GEHEIM eingestufte VS eingesetzt werden, eine technische Prüfung in regelmäßigen Abständen (§ 39 VSA) sowie eine Freigabe bei geheimschutz-relevanten Änderungen (§ 36 Abs. 3 VSA) gefordert. Zusammen mit der Dokumentationspflicht gemäß Anlage 5 Punkt 5.5.1 wird dem Risiko der Fernwartung angemessen begegnet.

VI. Abschließende Regelungen

§ 42 Kontrollen

(1) In jeder Dienststelle , die VS verwendet, sind stichprobenartig in angemessenen Zeitabständen unangekündigte Kontrollen durchzuführen, ob

1. ***in der Dienststelle hergestellte VS offensichtlich ungerechtfertigt oder unrichtig eingestuft sind; im Zweifelsfall kann eine schriftliche Begründung der herausgebenden Stelle eingeholt werden,***

2. ***die vorhandenen VS nach der VSA behandelt werden.***

Die Kontrollen sind durch die Geheimschutzbeauftragten oder durch besonders beauftragte Mitarbeiter, z. B. Geheimschutzbeamte, durchzuführen.

(2) Alle Bediensteten haben die Durchführung von Kontrollen zu unterstützen und hierfür auf Verlangen Zugang zu allen VS zu gewähren.

(3) Durch die Geheimschutzbeauftragten oder die besonders beauftragten Mitarbeiter sind insbesondere Art und Umfang der Maßnahmen zum Schutz von VS-VERTRAULICH oder höher eingestuften VS zu kontrollieren, ob

1. ***die Ermächtigungen zum Zugang zu VS und die Zulassungen für eine Tätigkeit nach § 10 Abs. 2 im vorliegenden Umfang erforderlich sind,***

2. ***die zum Zugang zu VS ermächtigten und die für eine Tätigkeit nach § 10 Abs. 2 zugelassenen Personen ausreichend überprüft und über die von ihnen zu beachtenden Geheimschutzbestimmungen unterrichtet sind,***

3. ***die VS vorschriftsgemäß hergestellt, vervielfältigt, gekennzeichnet, nachgewiesen, aufbewahrt und weitergegeben sowie nicht mehr benötigte VS vorschriftsgemäß vernichtet oder an das Geheimarchiv des Bundesarchivs abgegeben werden,***

4. ***der Grundsatz „Kenntnis nur, wenn nötig“ in der Praxis ausreichend beachtet wird.***

(4) Durch die für IT-Geheimschutzmaßnahmen Verantwortlichen ist insbesondere zu kontrollieren, ob

1. IT-Sicherheitskomponenten sicherheitsgerecht eingesetzt, gewartet und instand gesetzt werden,

2. Zugriffsrechte in der erteilten Form korrekt zugewiesen und erforderlich sind,

3. die Mittel zur Identifizierung/Authentisierung vorschriftsgemäß geschützt sind,

4. die freigegebene Hard- und Software unverändert ist.

(5) Die protokollierten Daten im Rahmen der Beweissicherung sind regelmäßig daraufhin zu überprüfen, ob

1. Zugangs-/Zugriffsversuche abgewiesen wurden und

2. Zugriffe auf VS-Daten offensichtlich ungerechtfertigt erfolgten.

(6) Über die Durchführung der Kontrollen sowie über sicherheitserhebliche Feststellungen ist ein Nachweis zu führen. Dieser ist 5 Jahre aufzubewahren.

Zu Absatz 1 Nr. 1:
In der Vergangenheit wurden zu häufige und zu hohe VS-Einstufungen vor allem auch vom Parlament wiederholt kritisiert.
Den nach der VSA vorgesehenen Schutz sollen nur VS erhalten, die zu Recht und angemessen eingestuft sind. In Zweifelsfällen ist zunächst die herausgebende Stelle zu hören.
Die Kontrollen sollten schwerpunktmäßig insbesondere dort erfolgen, wo der Schutzbedarf nach Anzahl und Höhe der Geheimhaltungsgrade besonders hoch ist oder den Möglichkeiten einer Preisgabe von VS besonders vorgebeugt werden muss.

Gesonderte Kontrollmaßnahmen nach Nr. 2 können für VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS i. d. R. entfallen.

Die Bestellung besonders beauftragter Geheimschutzmitarbeiter ist der jeweiligen Dienststelle – ausgenommen Dienststellen nach § 45 VSA – freigestellt.

Zu Absatz 2:
Der Grundsatz “Kenntnis nur, wenn nötig” gilt auch für das Kontrollpersonal. Es darf Zugang zu VS nur insoweit verlangen, als dies für die jeweilige Kontrolle erforderlich ist. Nicht bei jeder Kontrolle wird es nötig sein, dass der Kontrollierende Kenntnis vom Inhalt der VS nimmt.

§ 43 Benachrichtigung der Geheimschutzbeauftragten bei Verletzung von Geheimschutzvorschriften

Wird bekannt oder besteht der Verdacht, dass

1. ***Unbefugte von einer VS Kenntnis erhalten haben, zur Dekryptierung von VS benötigte Kryptoschlüssel oder andere Zugangsmittel zu VS Unbefugten zur Kenntnis gelangt oder verloren gegangen sind,***

2. ***eine VS, ein Schlüssel zu einem VS-Verwahrgelass, zu Schließfächern eines VS-Schlüsselbehälters oder zum Ein- und Ausschalten einer Alarmanlage verloren gegangen ist,***

3. ***Geheimschutzvorschriften verletzt sind oder***

4. ***sonst ein unter dem Gesichtspunkt des Geheimschutzes beachtlicher Sachverhalt (z. B. defekte Sicherungseinrichtungen oder außergewöhnliches Interesse bestimmter Personen an VS) vorliegt,***

so sind die Geheimschutzbeauftragten unverzüglich zu benachrichtigen.

Ziel dieser Bestimmung ist es, durch rechtzeitige Unterrichtung der oder des Geheimschutzbeauftragten (GB)(weiteren) Schaden zu verhüten. Die Erfahrungen aus Spionagefällen zeigen, dass der Schaden in vielen Fällen hätte begrenzt werden können, wären wichtige Informationen rechtzeitig dem GB mitgeteilt worden.

§ 44 Maßnahmen bei Verletzung von Geheimschutzvorschriften oder Bekanntwerden von Sicherheitsschwächen

(1) Die Geheimschutzbeauftragten stellen in Fällen der Verletzung von Geheimschutzvorschriften oder bei Bekanntwerden von Sicherheitsschwachstellen den Sachverhalt fest. Sie treffen die erforderlichen Maßnahmen, um Schaden zu verhüten oder zu verringern und um Wiederholungen zu vermeiden. Ist nach den ersten Ermittlungen ein nachrichtendienstlicher Hintergrund oder eine Verratstätigkeit anderer Art nicht auszuschließen, so ist das Bundesamt für Verfassungsschutz, im Geschäftsbereich des Bundesministeriums der Verteidigung das Amt für den Militärischen Abschirmdienst, zu beteiligen.

(2) Ist eine VS-VERTRAULICH oder höher eingestufte VS einem Unbefugten bekannt geworden oder muss mit dieser Möglichkeit gerechnet werden, so ist die herausgebende Stelle unter Hinweis auf diese Bestimmungen zu unterrichten. Die herausgebende Stelle trifft die ihrerseits notwendigen Maßnahmen, um Schaden zu verhindern oder zu verringern (z. B. durch Änderungen von Plänen oder Vorhaben und Benachrichtigung sonstiger Beteiligter). Soweit nationale VS von wesentlicher Bedeutung oder nichtdeutsche VS betroffen sind, ist unverzüglich das Bundesministerium des Innern als Nationale Sicherheitsbehörde zu unterrichten.

(3) Gehen Zugangsmittel (Kennwörter, Chipkarten u. Ä.) zu elektronischer Informationstechnik, die für VS verwendet wird, Schlüssel zu einem VS-Verwahrgelass, zu einem Schließfach eines VS-Schlüsselbehälters oder zum Ein- und Ausschalten einer Alarmanlage verloren oder ist aufgrund von Anhaltspunkten nicht auszuschließen, dass Unbefugte durch Manipulation von Sicherheitskomponenten Zugriff auf die VS erhalten haben oder ihn sich verschaffen können, sind die Zugangsmittel oder Schlösser durch neue auszutauschen oder die Verwendung von Informationstechnik ist einzuschränken bzw. zu sperren..

(4) War das Bundesamt für Verfassungsschutz bei einem Vorkommnis nach Absatz 1 beteiligt, so hat es die Leitung der betreffenden Dienststelle unverzüglich über seine Feststellungen zu unterrichten. Die Dienststellenleitung trifft die gegebenenfalls noch erforderlichen Maßnahmen.

(5) Verstöße gegen die VS-Anweisung können, auch wenn sie nicht nach den Bestimmungen des Strafgesetzbuches zu verfolgen sind, disziplinarrechtlich geahndet werden oder arbeitsrechtliche Maßnahmen (einschließlich Kündigung) nach sich ziehen.

Zu Absatz 1:
Die Feststellung des Sachverhaltens erstreckt sich auf alle relevanten Fakten (z. B. Angelegenheiten des personellen Geheimschutzes).

In Fällen, in denen nach den ersten Ermittlungen ein nachrichtendienstlicher Hintergrund oder eine Verratstätigkeit anderer Art nicht auszuschließen ist (Satz 3), ist grundsätzlich die zuständige Fachdienststelle (BfV bzw. MAD-Amt) einzuschalten. Sie verfügt i. d. R. über die notwendigen Hintergrundinformationen und das erforderliche Fachwissen, um den Sachverhalt richtig beurteilen zu können.

Bei Verdacht auf Manipulation (z.B. an Sicherungseinrichtungen) ist nach Möglichkeit sicherzustellen, dass keine Spuren beseitigt oder verändert werden können.

Zu Absatz 2:
Die herausgebende Stelle koordiniert die erforderlichen Maßnahmen. Die Unterrichtung des BMI hat grundsätzlich durch die herausgebende Stelle zu erfolgen.
Unter “nationale VS von wesentlicher Bedeutung” fallen i. d. R. nur STRENG GEHEIM, GEHEIM eingestufte VS oder mehre VS des Geheimhaltungsgrades VS-VERTRAULICH, die jedoch in ihrer Gesamtheit GEHEIM einzustufen sind.
Satz 3 findet auch dann Anwendung, wenn nichtdeutsche VS (VS-VERTRAULICH oder höher) mittelbar betroffen sind, z.B. bei Verlust einer nationalen VS, die inhaltlich im Wesentlichen auf einer nichtdeutschen VS beruht. Die zu ergreifenden Maßnahmen sind – soweit es für den Zuständigkeitsbereich in Frage kommt – auf der Grundlage multilateraler Geheimschutzregelungen (NATO, WEU, EAG, EUROCONTROL) zu treffen. Dem Bundesministerium des Innern als „Nationale Sicherheitsbehörde“ für den Geheimschutz obliegt die Unterrichtung des Sicherheitsbüros der in Frage kommenden supra-/internationalen Organisationen und/oder der Nationalen Sicherheitsbehörde des Partnerstaates.

Zu Absatz 4:
Soweit eine Unterrichtung der vorgesetzten Behörde angezeigt ist, ist dies Aufgabe des Dienststellenleiters.

Zu Absatz 5:
Verstöße gegen die Bestimmungen der Verschlusssachenanweisung können grundsätzlich ein Sicherheitsrisiko im Sinne des § 5 Sicherheitsüberprüfungsgesetz begründen.
Kommt es bei einer Person trotz mehrfacher Ermahnung wiederholt zu Verstößen, so sollen – ggf. nach Unterrichtung des Dienststellenleiters – entsprechende Maßnahmen eingeleitet werden. Hierauf kann z.B. in Hausordnungen und Dienstanweisungen in geeigneter Weise hingewiesen werden (Beispiel:
Der Geheimschutzbeauftragte ist angewiesen, jeden Verstoß gegen die Bestimmungen der VS-Anweisung dem Personalreferat zur Prüfung dienst- oder arbeitsrechtlicher Konsequenzen zur Kenntnis zu bringen und über jeden schwerwiegenden Verstoß auch den Dienststellenleiter und die bei dem Sicherheitsüberprüfungsverfahren mitwirkende Behörde zu unterrichten. Als Konsequenz droht der Entzug der Ermächtigung und damit die weitere Beschäftigung im sicherheitsempfindlichen Bereich). § 16 SÜG ist zu beachten.

§ 45 Besondere Dienststellen

(1) Dienststellen, die nach Feststellung des Bundesministeriums des Innern in besonderem Maße Ziel von Angriffen auf Vertraulichkeit, Integrität und Verfügbarkeit von VS sind, treffen in Zusammenarbeit mit dem BSI weitere Sicherheitsvorkehrungen. Hierzu gehören insbesondere

1. intensive Unterrichtungen der Beschäftigten,

2. die Bestellung des oder der jeweiligen Geheimschutzbeauftragten und deren Schulung durch das BSI zur Verstärkung von Kontrollen,

3. häufigere schwerpunktmäßige Kontrollen; bei Bedarf wirkt das BSI beratend und fachlich unterstützend mit;

4 regelmäßige umfassende Beratungen (mindestens alle vier Jahre) durch das BSI,

5 die Bildung von Sicherheitsbereichen,

6. die Einrichtung von abhörsicheren oder zumindest abhörgeschützten Räumen,

7. Vorkehrungen gegen ein unbefugtes Vervielfältigen von VS-VERTRAULICH oder höher eingestuften VS.

(2) Das Bundesministerium der Verteidigung trifft für seinen Geschäftsbereich die Feststellung der Dienststellen entsprechend Absatz 1 selbst, dort tritt anstelle des BSI in diesem Falle das Amt für den Militärischen Abschirmdienst.

(3) In diesen Dienststellen sind mindestens alle vier Jahre technische Prüfungen nach § 39 durchzuführen und Abhörschutzmaßnahmen nach § 32 zu treffen. Die Raumprüfungen sollen sich auf abhörgeschützte und abhörsichere Räume sowie aus besonderem Anlass (z. B. internationale Konferenz) auch auf andere abhörgefährdete Räume beziehen. Die IT-Systeme und Telekommunikationsanlagen sind insbesondere daraufhin zu überprüfen, ob sie die erforderlichen Sicherheitsvorkehrungen aufweisen und in der jeweiligen Konfiguration keine unzulässigen Funktionen aktiviert sind.

Das Bundesministerium des Innern legt auf der Grundlage von Erkenntnissen der Sicherheitsbehörden Dienststellen gemäß § 45 VSA fest und unterrichtet die zuständige Oberste Bundesbehörde. Die zuständigen Geheimschutzbeauftragten haben die Notwendigkeit des Umfangs entsprechend der Gefährdung zu prüfen. Das Ergebnis kann sein, dass anstelle der gesamten Dienststelle nur Teilbereiche als Dienststelle gemäß § 45 VSA ausgewiesen werden.

§ 46 Schlussbestimmungen

(1) Sofern im Falle von Katastrophen sowie im Alarm- und Verteidigungsfall die Gefahr besteht, dass Unbefugte sich Zugang zu VS-VERTRAULICH oder höher eingestuften VS verschaffen können, sind die VS sicherzustellen oder zu vernichten.

(2) Das Bundesministerium des Innern kann im Benehmen mit den obersten Bundesbehörden die VS-Anweisung ändern und sie durch Hinweise und Richtlinien ergänzen.

(3) Jede Dienststelle kann über die Vorschriften der VS-Anweisung hinaus verschärfte Sicherheitsvorkehrungen treffen, soweit sie die notwendige einheitliche Behandlung der VS im gesamten VS-Verkehr nicht stören.

(4) Das Bundesministerium des Innern kann in besonderen Ausnahmefällen auch anderen Abweichungen unter der Voraussetzung zustimmen, dass der mit der VS-Anweisung beabsichtigte Schutz durch andere Sicherheitsvorkehrungen erreicht wird.

(5) Soweit Bestimmungen der VS-Anweisung bei Auslandsvertretungen der Bundesrepublik Deutschland nicht angewandt werden können, bestimmt das Auswärtige Amt im Einvernehmen mit dem Bundesministerium des Innern, wie zu verfahren ist.

(6) Der Bundesnachrichtendienst kann mit Zustimmung des Bundeskanzleramtes für seinen Bereich von der VS-Anweisung abweichende Regelungen treffen.

(7) Das Bundesministerium der Verteidigung regelt die Behandlung von VS für seinen Zuständigkeitsbereich durch eine Zentrale Dienstvorschrift in Übereinstimmung mit der VS-Anweisung.

(8) Der Deutsche Bundestag regelt Fragen des Geheimschutzes eigenständig.

Zu Absatz 1:
Die Maßnahmen sind in einem Notfallplan (Siehe Anlage 5 Nr. 5.1) entsprechend den örtlichen Bedingungen möglichst umfassend aufzuführen. Sie sind zu treffen, sobald die Gefahr sich abzeichnet. Für den Fall einer Brandkatastrophe reicht zunächst die Aufbewahrung der VS in VS-Verwahrgelassen nach § 17 VSA aus, um die VS vor Unbefugten zu schützen. Die weiteren Schutzmaßnahmen sind – abhängig vom Verlauf einer Katastrophe – z.B. mit der Feuerwehr oder Polizei abzusprechen.

Zu Absatz 2:
Durch die ergänzenden Hinweise und Richtlinien wird die VSA freigehalten von umfangreichen Spezialregelungen. Sie basieren, wie die VSA selbst, auf § 35 Abs. 1 SÜG und sind Verwaltungsvorschriften i. S. v. Art 86 Satz 1 GG.
Im Weiteren sind auch auf spezielle Organisationseinheiten bezogene, die VSA ergänzende Verwaltungsvorschriften (z. B. Polizeidienstvorschrift 870, Kryptobetriebsdienst) zu beachten.

Zu Absatz 4:

Mit dieser Bestimmung verfügt die VSA über die erforderliche Flexibilität, um auch im speziellen Einzelfall (z.B. bei besonderen örtlichen Gegebenheiten oder Verfahren) zu ausgewogenen und angemessenen Regelungen zu gelangen. Entscheidend ist allein, dass der beabsichtigte Zweck erreicht wird, wobei ein Ermessensspielraum bleibt. Um alle wichtigen Faktoren bei der Entscheidung berücksichtigen zu können, wird i. d. R. vorher eine Stellungnahme des BSI eingeholt, das ggf. die Gegebenheiten vor Ort prüft.

Zu Absatz 7:
Die Vorschriften für den militärischen Bereich dürfen in ihrem sachlichen Inhalt keinen geringeren VS-Schutz fordern als die VSA. Sie können lediglich entsprechend den militärischen Gegebenheiten anders gefasst sein, soweit dadurch die einheitliche Behandlung der VS im gesamten VS-Verkehr nicht gestört wird.

§ 47 Inkrafttreten oder Außerkrafttreten

Diese Allgemeine Verwaltungsvorschrift und ihre Anlagen treten am 1. Juni 2006 in Kraft. Gleichzeitig treten außer Kraft die Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung - VSA) vom 29. April 1994 (GMBl. 1994 S. 674), zuletzt geändert durch 1. VS-Anweisung ÄndVwV vom 1. Juli 2001 sowie folgende dazu erlassene Richtlinien:

- ***Richtlinien zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik (VS-IT-Richtlinien – VSITR) vom 1. September 1998***
- ***Richtlinien zur Beratung und Durchführung von Kontrollen zum Schutz von Verschlusssachen (VS-Kontrollrichtlinien – VSKR) vom 1. September 1998***
- ***Richtlinien für die Abgabe von Verschlusssachen an das Geheimarchiv des Bundesarchivs (VS-Archivrichtlinien – VSArchR) vom 20. März 1991***
- ***Richtlinien zur technischen Sicherung und Bewachung von Verschlusssachen (VS-Sicherungsrichtlinien – VSSR) vom 1. September 1998***

Es gelten folgende Anlagen zu dieser Vorschrift:

Anlage 1: Hinweise zur Einstufung

Anlage 2: Beispiele zur VS-Kennzeichnung

Anlage 3: Hinweise und Muster für VS-Nachweise

Anlage 4: Hinweise zur Kennzeichnung nichtdeutscher VS

Anlage 5: Hinweise zu Geheimschutzkonzept und -dokumentation

Anlage 6: Hinweise zu Weitergabe und Versand von VS

Anlage 7 Hinweise für VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS

Anlage 8 Richtlinie zur Archivierung von VS

Berlin, den 31. März 2006

Dr. Dürig

Begriffsbestimmungen

Verwendete Begriffe werden nur erläutert, wenn sie in einem speziell auf VS bezogenen Sinn verwendet werden oder in der Verwaltungspraxis wenig gebräuchlich sind.

1) Verfügbarkeit einer VS
   Der berechtigte Zugriff muss gesichert sein, z. B. durch hinterlegte Zweitschlüssel oder Sicherheitskopien bei elektronischer Darstellung.

2) Integrität einer VS, auch als Unversehrtheit bezeichnet
   Sicherheit, dass eine VS unverändert und vollständig ist, z. B. dass nicht eine Anlage der VS entnommen ist. Dies kann durch unzureichende Sicherung (einfaches Schloss) verursacht sein.

3) elektronische Signatur
   Bei elektronischen Dateien kann durch kryptographische Methoden eine Kontrolle der Unversehrtheit erfolgen. Weiteres ist im Signaturgesetz und zugehörigen Vorschriften zu finden.

4) Datenträger
   Speichermedium für Computerdaten und -programme, z. B. Disketten, Festplatten, CD

5) PDA
   Tragbarer Kleinstcomputer (Abkürzung von **P**ersonal **D**igital **A**ssistent)

6) nichtflüchtige Speicher
   Man unterscheidet Speichermedien, die beim Abschalten den gespeicherten Dateninhalt verlieren (zumeist innerhalb von Geräten verwendet) und nichtflüchtige Speicher, bei denen der Inhalt mindestens bis zum nächsten Einschalten erhalten bleibt (z. B. Disketten, CD, Festplatten).

7) Dongel, auch Dongle
   Vorrichtung für Computer, meist in Form eines Steckers, um Funktionen abzusichern, z. B. Kopierschutz oder Zugang

8) Common Criteria
   Verfahren zur Bestätigung (Zertifizierung) der Sicherheit von Computersystemen und von deren Komponenten. Das amtliche Zertifikat bestätigt anhand einer Prüfung durch eine unabhängige Stelle, dass das vorgegebene Schutzziel vom Produkt erreicht wurde.

9) Penetrationstest
   Verfahren zur Prüfung des Schutzes eines Computernetzes gegen unbefugtes Eindringen in die angeschlossenen Computer

10) DECT
    Standard für Telefone, die drahtlose Handapparate verwenden (Funk), aber nur an einem bestimmten Telefonanschluss im Festnetz arbeiten

11) Bluetooth
    Verfahren zur Kopplung elektronischer Geräte untereinander über Funk, z. B. Freisprechanlage mit Mobiltelefon

12) approved circuits
    Leitungen, die durch besondere Maßnahmen so geschützt sind, dass ein unberechtigter Zugriff („Anzapfen“) erkennbar ist

Anlage 1 zur VS-Anweisung

Hinweise zur VS-Einstufung

1. Allgemeines

Tragen Sie durch eine umsichtige und sachgerechte VS-Einstufung dazu bei, dass

- die tatsächlich geheimhaltungsbedürftigen Informationen effektiv geschützt und

- unnötige Sicherheitskosten vermieden werden.

Der Geheimhaltungsgrad einer VS richtet sich nach ihrem Inhalt und nicht nach dem Geheimhaltungsgrad des Vorgangs zu dem sie gehört oder auf den sie sich bezieht. Ein Schriftstück mit VS-Anlagen ist mindestens so hoch einzustufen wie die am höchsten eingestufte Anlage. Ist es wegen seiner Anlagen eingestuft oder höher eingestuft, so ist darauf zu vermerken, dass es ohne Anlagen nicht mehr als VS zu behandeln oder niedriger einzustufen ist.

Innerhalb der Gesamteinstufung einer VS können deutlich feststellbare Teile, z.B. Teilpläne, Abschnitte, Kapitel, Verzeichnisse oder Nummern, niedriger oder nicht eingestuft werden.

Prüfen Sie kritisch, ob eine VS-Einstufung tatsächlich notwendig ist.

Insbesondere ist zu prüfen, ob das Schutzbedürfnis zur VS-Einstufung nur zeitlich begrenzt besteht (siehe § 9 Abs. 2 der VS-Anweisung).

Im Falle einer VS-Einstufung muss schlüssig darzulegen sein, welche Gefährdungen, Schäden oder Nachteile für die Bundesrepublik Deutschland oder eines ihrer Länder konkret entstehen können, wenn Unbefugte von den Informationen Kenntnis erhalten.

Dabei kommt eine VS-Einstufung grundsätzlich nur bei Informationen in Betracht, die die

- äußere Sicherheit,
- auswärtigen Beziehungen
- innere Sicherheit oder
- durch die Bundesrepublik Deutschland zu schützende Belange Dritter

betreffen.

VS-Einstufungen, die durch die Bundesrepublik zu schützende Belange Dritter betreffen, bedürfen der Billigung durch die zuständige Oberste Bundesbehörde.

Für andere schutzbedürftige Informationen sind die hierfür bestehenden Regelungen (z.B. Pflicht zur Wahrung von Dienst- oder Steuergeheimnissen, Schutz personenbezogener Daten nach dem Bundesdatenschutzgesetz, Bundesarchivgesetz oder interne Geschäftsordnungen) anzuwenden.

Eine Einstufung in VS-VERTRAULICH oder höher hat zur Folge, dass alle mit der eingestuften Information befassten Personen einer aufwendigen, in Persönlichkeitsrechte eingreifenden Sicherheitsüberprüfung unterzogen und für die VS kostenintensive materielle Schutzmaßnahmen getroffen werden müssen.

2. Beispiele für VS-Einstufungen:

2.1 Eine Einstufung in STRENG GEHEIM kommt z.B. in Betracht für

- das Informationsaufkommen des Bundesnachrichtendienstes,

- andere Zusammenstellungen, deren Einzelheiten GEHEIM eingestuft sind, die jedoch in ihrer Gesamtheit STRENG GEHEIM einzustufen sind.

2.2 Eine Einstufung in GEHEIM kommt z.B. in Betracht für

- Informationen zur "Elektronischen Kampfführung" der Bundeswehr,

- Unterlagen, die kritische Infrastrukturen betreffen,

- Staats- und andere bedeutende Verträge der Bundesrepublik Deutschland,

- Kryptodaten, die für die Verschlüsselung von VS-VERTRAULICH und höher eingestuften VS eingesetzt werden,

- Zusammenstellungen, deren Einzelheiten VS-VERTRAULICH eingestuft sind, die jedoch in ihrer Gesamtheit GEHEIM einzustufen sind.

2.3 Eine Einstufung in VS-VERTRAULICH kommt z.B. in Betracht für

- Ermittlungsberichte in Spionageverdachtsfällen,

- Erkenntnisse über die Arbeitsweise extremistischer/terroristischer Organisationen, deren Preisgabe die weitere Beobachtung/Aufklärung gefährden würde,

- außenpolitische Verhandlungspositionen, deren frühzeitige Bekanntgabe deutschen Interessen schaden würde,

- Unterlagen, die kritische Infrastrukturen betreffen,

- Staats- und andere bedeutende Verträge der Bundesrepublik Deutschland,

- wichtige Erfindungen, Geschäfts- und Betriebsgeheimnisse oder andere Tatsachen, Gegenstände oder Erkenntnisse Dritter, deren Kenntnis durch Unbefugte der Bundesrepublik Deutschland Schaden zufügen kann,

- Pläne der Computernetze und Konfigurationsdaten der eingesetzten Systeme von Dienststellen nach § 5 Abs. 3 der VS-Anweisung,

- Zusammenstellungen, deren Einzelheiten VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind, die jedoch in ihrer Gesamtheit VS-VERTRAULICH einzustufen sind.

Dies können z. B. sein:

- Computernetze, in denen verschiedene Bearbeiter gelegentlich VS-NUR FÜR DEN DIENSTGEBRAUCH bearbeiten. Auf den einzelnen Arbeitsplätzen liegen dann zwar auch bei einer größeren Dienststelle nur wenige VS vor, auf den Servern kann die Zusammenstellung aber schon einen solchen Umfang an Informationen annehmen, dass beim Verlust der Vertraulichkeit ein Schaden für die Bundesrepublik oder eines ihrer Länder eintreten kann. Schnittstelle für die Einstufung ist dann das Netz oberhalb der Leitungen der einzelnen Arbeitsplatz-Computer.

- Zusammenstellungen polizeilicher Ermittlungen, die einzeln nicht oder als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind, in ihrer Gesamtheit aber polizeiliche Arbeitsweisen offenlegen.

2.4 Eine Einstufung in VS-NUR FÜR DEN DIENSTGEBRAUCH kommt z.B. in Betracht für

- Abschlussberichte über Sicherheitsüberprüfungen von Personen,

- Fahndungsunterlagen aus den Bereichen Terrorismus/Extremismus,

- Zusammenstellungen über Geheimschutzmaßnahmen (Geheimschutzdokumentation),

- besondere Dienstanweisungen und Dienstpläne,

- Protokolle von Computernetzen der Dienststellen nach § 5 Abs. 3 der VS-Anweisung,

- Zusammenstellungen polizeilicher Ermittlungen, die einzeln nicht eingestuft sind, in ihrer Gesamtheit aber polizeiliche Arbeitsweisen offenlegen.

Anlage 2 zur VS-Anweisung

mit Erläuterungen

Hinweise und Beispiele zur VS-Kennzeichnung

Anmerkung: Die nachfolgenden Hinweise gelten vorzugsweise für Schriftgut. Bei anderen Darstellungsformen der VS sind vergleichbare Schutzmaßnahmen zu ergreifen.

1. Allgemeines

1.1 Bei STRENG GEHEIM oder GEHEIM eingestuften VS wird der Geheimhaltungsgrad mit dem Zusatz „amtlich geheim gehalten“ in roter Farbe durch Stempel oder Druck am oberen und unteren Rand jeder beschriebenen Seite angebracht. Die beschriebenen Seiten sind zu nummerieren; ihre Gesamtzahl ist auf der ersten Seite anzugeben. Die VS sind mit Geschäftszeichen und Datum zu versehen. Das Geschäftszeichen ist am Schluss durch die Abkürzung str.geh. bzw. geh. zu ergänzen; bei STRENG GEHEIM eingestuften VS ist es auf jeder beschriebenen Seite anzubringen.

1.2 Bei VS-VERTRAULICH eingestuften VS wird der Geheimhaltungsgrad mit dem Zusatz „amtlich geheim gehalten“ in schwarzer oder blauer Farbe durch Stempel, Druck oder Maschinenschrift am oberen Rand jeder beschriebenen Seite angebracht. Die beschriebenen Seiten sind zu nummerieren. Die VS sind mit Geschäftszeichen und Datum zu versehen. Das Geschäftszeichen ist am Schluss durch die Abkürzung VS-Vertr. zu ergänzen.

1.3 Bei VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS wird der Geheimhaltungsgrad in schwarzer oder blauer Farbe durch Stempel, Druck oder Maschinenschrift am oberen Rand jeder beschriebenen Seite angebracht. Die VS sind mit Geschäftszeichen und Datum zu versehen. Das Geschäftszeichen ist am Schluss durch die Abkürzung VS-NfD zu ergänzen. Bei Büchern, Broschüren u.Ä. genügt die Kennzeichnung auf dem Einband und dem Titelblatt.

1.4 Die äußeren Vorder- und Rückseiten sowie ggf. die Rücken von Schriftgutbehältern (Lauf-, Klebe-, Sammelmappen, Ordner, Hefter), in denen STRENG GEHEIM, GEHEIM oder VS-VERTRAULICH eingestufte VS befördert oder verwahrt werden, sind wie folgt zu kennzeichnen:

1. bei STRENG GEHEIM mit einem gelben und einem roten Diagonalstreifen (überkreuzt),

2. bei GEHEIM mit einem roten Diagonalstreifen,

3. bei VS-VERTRAULICH mit einem blauen Diagonalstreifen.

Von dieser äußeren Kennzeichnung sind VS-Transportbehälter ausgenommen.

1.5 VS-Bestandsverzeichnisse sind in derselben Weise zu kennzeichnen.

1.6 Bei Kryptosystemen können als VS eingestufte zum Ver- und Entschlüsseln nötige Kryptodaten (Schlüsselmittel), Beschreibungen, Bauteile und sonstige Dokumentation unabhängig vom Geheimhaltungsgrad mit dem Warnvermerk KRYPTO gekennzeichnet werden, um die Umsetzung des Prinzips „Kenntnis nur wenn nötig“ zu erleichtern.

Als VS eingestufte Anlagen einer VS sind auf dem Anschreiben zu vermerken und entsprechend ihrer Einstufung gemäß Anlage 1, Abschn. 1, 3. Absatz zu kennzeichnen. Auf der ersten Seite jeder Anlage ist anzugeben, zu welcher VS (herausgebende Stelle, Geschäftszeichen, Datum und ggf. Ausfertigungsnummer) sie gehört.
Als VS eingestufte Anlagen sind auf der VS zu vermerken, sonstige Anlagen können vermerkt werden.

Die Ausfertigungsnummer des Anschreibens (vorgeschrieben nur bei GEHEIM und STRENG GEHEIM) auf den Anlagen (vgl. Beispiel 2 b) braucht nicht angegeben zu werden, wenn die Anlagen selbst eine Ausfertigungsnummer tragen.
Der Begriff "oberer Rand" lässt auch das Anbringen des Geheimhaltungsgrades unterhalb des Schriftkopfes zu.
Der Zusatz "amtlich geheimgehalten" ist aus strafrechtlichen Gründen gewählt worden, um jeden möglichen Zweifel auszuschließen, dass es sich um amtlich geheimgehaltene Unterlagen handelt.
Der Begriff "Seitenzahl" wurde gewählt, weil sich die Blattzahl im Falle beidseitiger Beschriftung bei Kopien ändern kann.
Unter u. Ä. im Sinne des letzten Satzes des Abschn. 1.3 fallen nur Schriftstücke, die in ihrer Beschaffenheit Büchern oder Broschüren vergleichbar, d.h. nicht ohne weiteres in ihre Bestandteile aufzulösen sind. Ein z.B. nur mit Heftklammern verbundenes Schriftstück erfüllt diese Anforderungen nicht. Heftklammern werden aus verschiedenen Gründen oft gelöst, z.B. zum Fotokopieren oder von der VS-Registratur beim Einheften in die Akten.
Die Verwendung der wie im Geschäftszeichen abgekürzten Geheimhaltungsgrade ist für die Kennzeichnung als VS nicht ausreichend.
Das Geschäftszeichen umfasst im Allgemeinen das Aktenzeichen und die Nummer aus dem VS-Bestandsverzeichnis (Tagebuchnummer).
Enthält eine VS unterschiedlich eingestufte Teile (vgl. Anlage 1, Abschn. 1, 3. Absatz und Beispiel 5 zur VSA), so sind unabhängig davon alle Seiten mit dem Geheimhaltungsgrad zu kennzeichnen, der der Gesamteinstufung entspricht. Anfang und Ende der unterschiedlich eingestuften Teile müssen klar erkennbar sein.
Sind einzelne Teile eines höher eingestuften Schriftstückes VS-NUR FÜR DEN DIENSTGEBRAUCH oder nicht eingestuft, so kann es zweckmäßig sein, diese gesondert als Anlage beizufügen.
Durch die Kennzeichnung der Schriftgutbehälter, die VS-VERTRAULICH eingestufte VS enthalten, mit einem blauen Diagonalstreifen soll auf die Schutzbedürftigkeit der Unterlagen hingewiesen und gleichzeitig eine Unterscheidung zu den höher eingestuften VS erreicht werden. Die Kennzeichnung gibt unmittelbare Hinweise über:

- Art des Transports,
- Art der Aufbewahrung.

Eine besondere Kennzeichnung der Schriftgutbehälter, die VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH enthalten, ist nicht vorgeschrieben. Dies würde in manchen Behörden zur Kennzeichnung aller Behälter führen.

Schriftgutbehälter, die VS unterschiedlicher Geheimhaltungsgrade enthalten, sind entsprechend dem jeweils höchsten Geheimhaltungsgrad zu kennzeichnen

2. Beispiele

Die nachfolgenden Beispiele dienen als Anregung, bei der Umsetzung der Vorschrift zur Anwendung in den Dienststellen sind die Textpassagen maßgebend.

Beispiel 1 **Entwurf** einer Verschlusssache STRENG GEHEIM

Beispiel 1a **Ausfertigung** einer Verschlusssache STRENG GEHEIM

Beispiel 1b **Vorlage** eines Serienbriefs STRENG GEHEIM

Beispiel 1c **1. Ausfertigung** eines Serienbriefs STRENG GEHEIM nach Beispiel 1b

Beispiel 2 **Entwurf** einer Verschlusssache GEHEIM

Beispiel_2a **Ausfertigung** einer Verschlusssache GEHEIM

Beispiel 2b **Anlage** zu einer Verschlusssache GEHEIM

Beispiel 3 **Entwurf** einer Verschlusssache VS-VERTRAULICH

Beispiel 3a **Ausfertigung** einer Verschlusssache VS-VERTRAULICH

Beispiel 4 **Entwurf** einer Verschlusssache VS-NUR FÜR DEN DIENSTGEBRAUCH

Beispiel 5 **Verschlusssache mit unterschiedlich eingestuften Teilen**

Beispiel 6 **Verfügen und Vermerken von Vervielfältigungen (z.B. Kopien)**

Beispiel 6a **Kopie** einer Verschlusssache GEHEIM

Beispiel 6b **Kopie einer Kopie** einer Verschlusssache GEHEIM

Beispiel 7 **Umschläge für VS-Sendungen** (hier: GEHEIM)

Beispiel 8 **Kennzeichnung für VS-Datenträger** (hier: CD-ROM)

Beispiel 9 **Kennzeichnung der Hülle für VS-Datenträger** (hier: CD-ROM)

Beispiel 10 **Kennzeichnung für VS-Datenträger** (hier: USB-Stick)

Anlage 3 zur VS-Anweisung

mit Erläuterungen

Hinweise und Muster für den Nachweis von VS

Hinweise zum Führen von VS-Bestandsverzeichnissen

Anmerkung: Die nachfolgenden Hinweise gelten vorzugsweise für Schriftgut. Bei anderen Darstellungsformen der VS sind vergleichbare Schutzmaßnahmen zu ergreifen.

Bei der Gestaltung der VS-Bestandsverzeichnisse kann die VS verwaltende Dienststelle von Muster 10 abweichen. Folgendes ist jedoch zu beachten:

1. Auf der ersten Seite ist zu vermerken, welche Geheimhaltungsgrade nachgewiesen werden und von wem das VS-Bestandsverzeichnis geführt wird.

2. Die Seiten gebundener VS-Bestandsverzeichnisse sind zu nummerieren. Bei VS-Bestandsverzeichnissen in Karteiform sind die Karteikarten fortlaufend zu nummerieren und mit Dienstsiegel zu kennzeichnen. Bei VS-Bestandsverzeichnissen in elektronischer und in Loseblattform ist das Bundesamt für Sicherheit in der Informationstechnik beratend hinzuzuziehen.

3. VS-Bestandsverzeichnisse erhalten den Geheimhaltungsgrad der in ihnen nachgewiesenen VS; Ausnahmen in Einzelfällen bedürfen der Zustimmung des Geheimschutzbeauftragten. Bei mobilen Datenträgern und gebundenem Schriftgut erfolgt die Kennzeichnung auf dem Objekt, dem Einband oder dem Titelblatt. Die Kennzeichnung hat bei Karten oder losen Blättern einzeln zu erfolgen.

4. In den VS-Bestandsverzeichnissen sind Eingang, Ausgang, Verbleib, Vervielfältigung, Herabstufung und Vernichtung von STRENG GEHEIM, GEHEIM oder VS-VERTRAULICH eingestuften VS nachzuweisen und besondere Fristen für die Aufhebung oder Reduzierung der VS-Einstufung zu vermerken.

5. STRENG GEHEIM eingestufte VS sind in einem getrennten VS-Bestandsverzeichnis zu führen.

6. Jede VS ist im VS-Bestandsverzeichnis unter einer eigenen fortlaufenden Nummer zu registrieren. Werden weitere Eingänge zu einer nachgewiesenen VS unter derselben Nummer registriert, so ist bei STRENG GEHEIM oder GEHEIM eingestuften VS als Unterscheidungsmerkmal eine weitere Zahl hinzuzusetzen (z.B. Hoch- oder Stückzahl).

7. Die Eintragungen sind mit Tinte oder Kugelschreiber (dokumentenecht nach DIN 16554) vorzunehmen. Änderungen müssen erkennbar sein, sie sind mit Datum und Unterschrift zu versehen. Bei Streichungen muss der ursprüngliche Text lesbar bleiben. Es ist unzulässig, in VS-Bestandsverzeichnissen zu radieren, Eintragungen unkenntlich zu machen oder Blätter zu entfernen oder einzufügen. Bei nicht dauerhaft benötigten Eintragungen (z. B. Wiedervorlagetermine) können die Geheimschutzbeauftragten nach Beratung durch das BSI Ausnahmen zulassen.

8. Die VS-Verwalter bestätigen den Empfang neuer VS-Bestandsverzeichnisse (VS-Tagebücher oder Karten). Die Empfangsbescheinigungen sowie etwaige VS-Übergabeverhandlungen nehmen die Geheimschutzbeauftragten oder von diesen Beauftragte in Verwahrung.

Unabhängig von der Darstellungsform (siehe § 2 VSA) sind VS-VERTRAULICH und höher eingestufte VS in einem Bestandverzeichnis nachzuweisen. Soweit es sich hierbei um Schriftstücke handelt, muss aus dem Bestandsverzeichnis jedes einzelne zur VS zugehörige Schriftstück (Schreiben, Anlagen, Kopien, Abschriften usw.) ersichtlichersichtlich sein. Die auf der VS aufgeführten Informationen (Geschäftszeichen, Tagebuchnummer, Datum, Seitenzahl bei GEHEIM und STRENG GEHEIM eingestuften Schriftstücken, etc.) haben sich im VS-Bestandsverzeichnis widerzuspiegeln. Die Gestaltung des VS-Bestandsverzeichnisses ist grundsätzlich den einzelnen Behörden überlassen, sollte aber die im Muster 10 aufgeführten Vorgaben beinhalten.

Muster für Nachweise

Die Muster werden auch elektronisch als Vorlage bereit gestellt.

Muster 1	Verpflichtung zur Geheimhaltung von Verschlusssachen
Muster 2	Ermächtigung und Zulassung
Muster 3	Wiederholung der Unterrichtung
Muster 4	Aufhebung der Ermächtigung oder Zulassung
Muster 5	VS-Begleitzettel
Muster 6	VS-Übergabeprotokoll
Muster 7	VS-Vernichtungsprotokoll
Muster 8	VS-Empfangschein
Muster 8a	Vereinbarung zum VS-Austausch
Muster 8d	VS-Austausch (deutsch)
Muster 8e	VS-Austausch (englisch)
Muster 9	Konferenzbescheinigung
Muster 10	VS-Bestandsverzeichnis
Muster 11	VS-Quittungsbuch

Anlage 4 zur VS-Anweisung

mit Erläuterungen

Hinweise zur Kennzeichnung nichtdeutscher VS

Nichtdeutsche Verschlusssachen (VS) sind wie folgt zu kennzeichnen:

1. Nichtdeutsche VS, zu deren Schutz sich die Bundesrepublik Deutschland vertraglich verpflichtet hat, sind mit dem deutschen Geheimhaltungsgrad, der dem zugeordneten nichtdeutschen Geheimhaltungsgrad entspricht, zu kennzeichnen. Der § 12 Abs. 1 der VS-Anweisung ist anzuwenden. Es genügt die Kennzeichnung mit dem deutschen Geheimhaltungsgrad auf der ersten Seite (Anlagen oder Teile gesondert).

2. Bei Übersetzungen, bei denen die nichtdeutsche Herkunft nicht erkennbar ist, ist diese auf der ersten Seite neben dem vergleichbaren deutschen Geheimhaltungsgraden kenntlich zu machen.

Beispiele:

SECRET DEFENSE

GEHEIM
amtlich geheimgehalten

COSMIC TOP SECRET

STRENG GEHEIM
amtlich geheimgehalten

3. Nachstehend sind die vergleichbaren Geheimhaltungsgrade der Organisationen und Staaten aufgeführt, denen gegenüber vertragliche Verpflichtungen gemäß Nummer 1 bestehen. Daneben bestehen mit weiteren Staaten Teilabkommen für bestimmte Gebiete der Zusammenarbeit, die den dafür zuständigen Stellen bekannt sind (Ressortabkommen, Projektabkommen). Im Zweifelsfall erteilt das Bundesministerium des Innern, das eine Übersicht über alle Geheimschutzabkommen führt, Auskunft.

Den deutschen Geheimhaltungsgraden entsprechen	VS-NUR FÜR DEN DIENSTGEBRAUCH	VS-VERTRAULICH	GEHEIM	STRENG GEHEIM

A. Bei internationalen Organisationen:

1. NATO *(1)*	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
2. WEU *(1)*	WEU RESTRICTED	WEU CONFIDENTIAL	WEU SECRET	FOCAL TOP SECRET
3. EURATOM *(1)*	EURA NUR FÜR DEN DIENSTGEBRAUCH	EURA VERTRAULICH	EURA GEHEIM	EURA STRENG GEHEIM
4. EUROCONTROL *(1)*	EUROCONTROL RESTRICTED	EUROCONTROL CONFIDENTIAL	EUROCONTROL SECRET	-
5. EUROPOL	EUROPOL RESTRICTED	EUROPOL CONFIDENTIAL	EUROPOL SECRET	EUROPOL TOP SECRET
6. EU	RESTREINT UE	CONFIDENTIEL UE	SECRET UE	TRES SECRET UE/ EU TOP SECRET

7. ESA	ESA RESTRICTED	ESA CONFIDENTIAL	ESA SECRET	ESA TOP SECRET
8. OCCAR	OCCAR RESTRICTED	OCCAR CONFIDENTIAL	OCCAR SECRET	OCCAR TOP SECRET

B. Bei ausländischen Staaten:

1. Belgien *(5)*	DIFFUSION RESTREINTE	CONFIDENTIEL	SECRET	TRÈS SECRET
2. Bulgarien (5)	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	СЕКРЕТНО	СТРОГО СЕКРЕТНО	-
3. Dänemark (5)	TIL TJENESTEBRUG	FORTROLIGT	HEMMELIGT	YDERST HEMMELIGT
4. Estland (5)	AMETKONDLIK	KONFIDENTSIAALNE	SALAJANE	-
5. Finnland *(5)*	KÄYTTÖ RAJOITETTUEI	LUOTTAMUKSELLINEN	SALAINEN	ERITTÄIN SALAINEN
6. Frankreich *(5)*	-	CONFIDENTIELDEFENSE	SECRETDEFENSE	TRES SECRET DEFENSE
7. Griechenland (5)	PERIORISMENIS CHRISSEOS	EMPISTEFTIKON	APPORITON	AKRROS APPORITON
8. Großbritanien (5)	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
9. Italien (5)	RISERVATO	RISERVATISSIMO	SEGRETO	SEGRETISSIMO
10. Kasachstan	Для служебного пользования	Секретно	Совершенно секретно	
11. Lettland (5)	KONFIDENTIALI	SLEPENI	SEVISKI SLEPENI	-
12. Litauen (5)	RIBOTO NAUDOJIMO	KONFIDENCIALIAI	SLAPTAI VISISKAI	SLAPTAI
13. Niederlande *(5)*	DEPARTEMENTAAL VERTROUWELIJK	CONFIDENTIEEL STG	GEHEIM STG	ZEER GEHEIM STG
14. Norwegen (5)	BEGRENSET	KONFIDENSIELT	HEMMELIG	STRENGT HEMMELIG
15. Polen (5)	ZASTREZONE	POUFNE	TAINE	SCISLE TAINE
16. Portugal (5)	RESERVADO	CONFIDENCIAL	SECRETO	MUITO SECRETO
17. Rumänien (5)	SECRET DE SERVICIU	SECRET	STRICT SECRET	-
18. Rußland	Для служебного пользования	Секретно	Совершенно секретно	
19. Schweden zivil *(3/5)*		-	HEMLIG	KVALIFICERAT HEMLIG
militärisch *(3/5)*	HEMLIG RESTRICTED	HEMLIG CONFIDENTIAL	HEMLIG SECRET	HEMLIG TOP SECRET
20. Schweiz *(4/5)*	-	VERTRAULICH	GEHEIM	-
21. Slowakische Republik (5)	-	TAJNE	PRISNE TAJNE	-

22. Spanien	(5)	DIFUSION LIMITADA	CONFIDENCIAL	RESERVADO	SECRETO
23. Tschechische Republik	(5)	VYHRAZENE	DUVIRNE	TAJNE	POISNI TAJNE
24. Ukraine			Таємно	Ціпком таємно	
25. Ungarn *(5)*		TITKOS	SZIGORUAN TITKOS	SZIGORUAN TITKOS	-
26. Vereinigte Staaten *(2/5)*		-	CONFIDENTIAL	SECRET	TOP SECRET

Erläuterung:
Die Bundesrepublik Deutschland hat sich als Mitglied inter- und supranationaler Organisationen sowie in Abkommen mit anderen Staaten verpflichtet, VS dieser Organisationen/Staaten entsprechend deutschem Recht zu schützen. Soweit geheimhaltungsbedürftige Informationen der Stationierungsstreitkräfte betroffen sind, sind auch die Strafvorschriften in Artikel 7 des 4. Strafrechtsänderungsgesetzes vom 11. Juni 1957 (BGBl. I S. 597) in der jeweils geltenden Fassung zu beachten.

Diese Anlage zur VSA regelt die Kennzeichnung und Behandlung der wichtigsten nichtdeutschen VS. In der Übersicht der inter- bzw. supranationalen Organisationen sind jedoch nur die Organisationen enthalten, deren Vorschriften aufgrund vertraglicher Vereinbarungen für die Bundesrepublik Deutschland unmittelbar verbindlich sind. Weitere detaillierte Regelungen bezüglich nichtdeutscher VS enthalten Rundschreiben des BMI. Im bilateralen Verkehr mit ausländischen Staaten, die in dieser Anlage nicht genannt sind, sind die vergleichbaren Geheimhaltungsgrade dem jeweiligen Geheimschutzabkommen zu entnehmen; Auskunft erteilt bei Bedarf das BMI.

Obwohl die Geheimhaltungsvorschriften der Organisationen NATO, WEU, EURATOM und EUROCONTROL unmittelbare Gültigkeit auch in den Mitgliedstaaten besitzen, genügt es, VS dieser Organisationen im nationalen Bereich nach der VS-Anweisung zu behandeln (vgl. Anmerkung 2), da die deutschen Vorschriften zumindest gleichwertig sind. Nur bei COSMIC TOP SECRET, FOCAL TOP SECRET und bei VS mit dem Zusatz ATOMAL bzw. anderen VS-Sonderkategorien sowie im direkten Verkehr mit den genannten Organisationen sind zusätzlich deren Vorschriften anzuwenden.
Werden deutsche VS in eine andere Sprache übersetzt, so ist der Geheimhaltungsgrad in dieser Sprache anzubringen; der deutsche Geheimhaltungsgrad kann außer bei Exemplaren, die im Inland verbleiben, entfallen.

Anmerkungen:

(1) Für VS dieser Organisationen gelten Vorschriften, die zum Teil über die Forderungen der VS-Anweisung hinausgehen (z.B. bei COSMIC TOP SECRET und ATOMAL Informationen der NATO). Die Vorschriften können bei Bedarf beim Bundesministerium des Innern angefordert werden.

(2) Die Vereinigten Staaten und Frankreich haben keinen VS-NUR FÜR DEN DIENSTGEBRAUCH entsprechenden Geheimhaltungsgrad. Sie verwalten und sichern solche VS anderer Staaten und internationaler Organisationen entsprechend gleichwertiger oder strengerer nationaler Vorschriften.

(3) Im zivilen Behördenbereich verwendet Schweden keine vergleichbaren Geheimhaltungsgrade für VS-NUR FÜR DEN DIENSTGEBRAUCH und VS-VERTRAULICH. Zivile deutsche VS der Geheimhaltungsgrade VS-NUR FÜR DEN DIENSTGEBRAUCH und VS-VERTRAULICH werden in Schweden entsprechend dem zivilen Geheimhaltungsgrad HEMLIG geschützt und behalten ihre deutsche Kennzeichnung. Mit der Beibehaltung der deutschen Kennzeichnung wird sichergestellt, dass eine z. B. VS-NfD eingestufte VS, die in Schweden wie GEHEIM geschützt wird und nach Deutschland zurückgegeben wird, ihre ursprüngliche Einstufung nicht verliert, es sei denn es gibt fachliche, von Schweden angezeigte Gründe dafür.

(4) Die Schweiz verwendet den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH nicht. Deutsche VS mit diesem Geheimhaltungsgrad werden in der Schweiz entsprechend den deutschen Geheimschutzvorschriften verwaltet und gesichert.

(5) Bei Staaten, die Mitglied in der EU, der NATO oder der ESA sind, können sich zwischenzeitlich Abweichungen bei den Geheimhaltungsgraden ergeben haben, die in den bilateralen Geheimschutzabkommen noch nicht berücksichtigt sind. Auskunft hierzu erteilt das Bundesministerium des Innern auf Anfrage.

Anlage 5 zur VS-Anweisung

Hinweise zur VS-Dokumentation

1. Die VS-Vorschriften einschließlich Rundschreiben, Erlasse und behördeneigene VS-Dienstanweisungen müssen den Mitarbeitern der Dienststelle jederzeit auf einfache Weise zugänglich sein.

2. In Dienststellen, die mit VS arbeiten, ist ein auf die Dienststelle bezogenes Geheimschutzkonzept zu erstellen, in dem die Informationen und vorgesehenen Maßnahmen entsprechend den nachfolgenden Absätzen dieser Anlage sowie insbesondere sonstige nach § 4 Abs. 3, § 18 Abs. 1 und § 25 der VS-Anweisung dokumentiert sind. In Dienststellen mit geringem Aufkommen an VS-VERTRAULICH oder höher eingestuften VS können das Geheimschutzkonzept oder dessen Teile in anderen Dienstvorschriften oder Konzepten enthalten sein oder auf diese verweisen (z.B. IT-Sicherheitskonzept).

3. Liste der nach § 10 der VS-Anweisung zum Zugang zu VS ermächtigten oder zugelassenen Personen

4. VS-Sicherungsdokumentation,

4.1 Auflistung der Standorte, der Anzahl und der Benutzer von VS-Aktensicherungsräumen, VS-Verwahrgelassen, VS-Transportbehältern, VS-Schlüsselbehältern und VS-Vernichtungsgeräten, der Aufbewahrungsorte der jeweils dazugehörigen Reserveschlüssel und Zahlenkombinationen, sowie die Namen der Verwalter und der Zugangsmöglichkeiten in Notfällen,

4.2 Dokumentation der Bewachung und technischen Überwachung; Einsatzbereiche von Alarmanlagen einschließlich der Regelungen, wer sie scharf und unscharf schalten sowie warten und instand setzen darf,

4.3 Lagepläne und Zutrittsregelungen von Sicherheitsbereichen sowie von abhörgeschützten und abhörsicheren Räumen,

4.4 Nachweise über durchgeführte Kontrollen, ob

4.4.1 die Ermächtigungen zum Zugang zu VS und die Zulassungen für Tätigkeiten, die dem Geheimschutz unterliegen, im vorliegenden Umfang erforderlich sind,

4.4.2 die zum Zugang zu VS ermächtigten und die für eine Tätigkeit, die dem Geheimschutz unterliegt, zugelassenen Personen ausreichend überprüft und über die von ihnen zu beachtenden Geheimschutzbestimmungen unterrichtet sind,

4.4.3 die VS gemäß der VS-Anweisung hergestellt, vervielfältigt, gekennzeichnet, nachgewiesen, aufbewahrt und weitergegeben sowie nicht mehr benötigte VS gemäß § 26 der VS-Anweisung aus dem Bestand der Dienststelle ausgesondert werden,

4.4.4 der Grundsatz "Kenntnis nur, wenn nötig" in der Praxis beachtet wird

5. IT-spezifische Dokumentation

5.1 Erstellung eines Geheimschutzkonzeptes unter Beachtung der in den BSI-Standards 100-2 und 100-3 beschriebenen Vorgehensweise

5.2 Übersicht über die für VS verwendete Hard- und Software, Datenträger sowie sonstige Informationstechnik und die genutzten IT-Sicherheitsfunktionen,

5.3 Dokumentation der Nutzungs- und Zugriffsrechte,

5.4 Dokumentation der Abnahme und Freigabe,

5.5 Nachweise über durchgeführte Kontrollen, ob

5.5.1 IT-Sicherheitskomponenten wie vorgesehen eingesetzt, gewartet und instand gesetzt werden,

5.5.2 Zugriffsrechte in der erteilten Form erforderlich sind, im IT-System korrekt zugewiesen sind und die Mittel zur Identifizierung und Authentisierung vorschriftsgemäß geschützt sind

5.5.3 unbefugte Zugangs- und Zugriffsversuche erfolgten und abgewiesen wurden und

5.5.4 Zugriffe auf VS-Daten offensichtlich ungerechtfertigt erfolgten.

6. Berichte über Sicherheitsvorkommnisse und Dokumentation von Sachverhalten, die den Geheimschutz beeinträchtigen sowie zu ergriffenen Maßnahmen und Ergebnissen.

Anlage 6 zur VS-Anweisung

mit Erläuterung

Hinweise zu Weitergabe und Versand von VS

Anmerkung: Die nachfolgenden Hinweise gelten vorzugsweise für Schriftgut. Bei anderen Darstellungsformen der VS sind vergleichbare Schutzmaßnahmen zu ergreifen.

1. Weitergabe von VS innerhalb desselben Gebäudes oder einer geschlossenen Gebäudegruppe

1.1 Innerhalb desselben Gebäudes oder einer geschlossenen Gebäudegruppe sind VS-VERTRAULICH oder höher eingestufte VS von Hand zu Hand weiterzugeben oder durch Boten zu befördern; sie sind in einem VS-Quittungsbuch nachzuweisen. Von einer Quittungspflicht ausgenommen sind VS-VERTRAULICH eingestufte VS, die innerhalb von Referaten oder vergleichbaren Organisationseinheiten weitergegeben oder die täglich an die VS-Registratur zurückgegeben werden.

1.2 Bei GEHEIM eingestuften VS können die Geheimschutzbeauftragten ausnahmsweise zulassen, dass innerhalb bestimmter Referate oder vergleichbarer Organisationseinheiten eine Quittung entfällt, wenn besondere Umstände (außergewöhnlich große Anzahl dieser VS und unvertretbare Zeitverzögerungen) vorliegen und der aktuelle Verbleib der VS jederzeit feststellbar ist. VS-VERTRAULICH eingestufte VS können bei besonders großer Anzahl dieser VS mit Zustimmung der Dienststellenleitung auch an andere Organisationseinheiten ohne Quittung weitergegeben werden; bei Weitergabe soll die VS-Registratur beteiligt werden. Der Verbleib solcher VS ist verstärkt zu kontrollieren.

1.3 Innerhalb desselben Ortes können zwischen Gebäuden einer Dienststelle GEHEIM oder VS-VERTRAULICH eingestufte VS von Hand zu Hand weitergegeben oder durch Boten befördert werden.

1.4 VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS werden ohne Quittung weitergegeben und wie nicht eingestuftes Schriftgut befördert.

2. Weitergabe von VS durch Boten

2.1 STRENG GEHEIM oder GEHEIM eingestufte VS sind bei Beförderung durch VS-Boten in Klebemappen oder Umschlägen zu verschließen. Der Klebestreifen oder Umschlag muss neben der Unterschrift des Absenders die Aufschrift tragen:

„STRENG GEHEIM/GEHEIM – diese Mappe (dieser Umschlag)
darf nur von .....oder
dem STRENG GEHEIM/GEHEIM ermächtigten Vertreter geöffnet werden!“

Die Klebemappen oder Umschläge sollen in verschlossenen VS-Transportbehältern mit Zählwerk befördert werden; die Mappen/Umschläge dürfen jeweils nur VS für einen Empfänger enthalten. Stehen VS-Transportbehälter mit Zählwerk nicht zur Verfügung, so ist als Hülle ein zweiter Umschlag zu verwenden, auf dem die Anschrift des Empfängers und das Geschäftszeichen ohne den Geheimhaltungsgrad angegeben werden.

2.2 Der Absender hat die erforderlichen Eintragungen im VS-Quittungsbuch vorzunehmen. Das VS-Quittungsbuch ist dem VS-Boten mitzugeben. Der Absender hat auf baldige Rückgabe des Quittungsbuches zu achten und die Eintragungen hinsichtlich der Vollständigkeit, der für die Beförderung benötigten Zeit und ggf. der Übereinstimmung der Zählwerknummern zu überprüfen.

2.3 Der Bote hat die VS unverzüglich zu befördern und bis zu ihrer Ablieferung im persönlichen Gewahrsam zu halten. Kann eine STRENG GEHEIM eingestufte VS nicht sofort zugestellt werden, so ist sie dem Absender oder der zuständigen VS-Registratur zur einstweiligen Verwahrung zurückzugeben.

2.4 Der Empfänger hat die Unversehrtheit und den Verschluss des VS-Transportbehälters bzw. Umschlages zu prüfen und ihn persönlich zu öffnen. Er überprüft anhand der Eintragungen im VS-Quittungsbuch die für die

Beförderung benötigte Zeit sowie bei VS-Transportbehältern den Zählwerkstand. Er trägt das Datum, die Uhrzeit und bei VS-Transportbehältern den Zählwerkstand in das VS-Quittungsbuch ein und quittiert die VS.

2.5 VS-VERTRAULICH eingestufte VS sind bei Beförderung durch Boten in Klebemappen, Umschlägen oder anderer angemessener Verpackung zu verschließen. Der Klebestreifen oder Umschlag muss neben der Unterschrift des Absenders die Aufschrift tragen:

> „VS-VERTRAULICH – Mappe (dieser Umschlag)
> darf nur von .....oder
> dem VS-VERTRAULICH ermächtigten Vertreter
> geöffnet werden!“

Der Verwendung von VS-Transportbehältern bedarf es nicht.
Unterbleibt eine Quittung bei der Weitergabe, so ist der Klebestreifen durch das Datum und die Uhrzeit beim Absenden zu ergänzen. Im Übrigen gilt § 21 Abs. 2 bis 4 der VS-Anweisung entsprechend.

2.6 Sendungen mit VS-VERTRAULICH oder höher eingestuften VS, die auf dem inneren Umschlag den Vermerk „Persönlich“ oder „Nicht durch die Registratur zu öffnen“ tragen, sind dem Empfänger oder ggf. dem Vertreter im Amt ungeöffnet mit einem VS-Begleitzettel zuzuleiten. Der Empfänger kann eine solche VS von der Weitergabe in den Geschäftsgang ausschließen, wenn es der Grundsatz „Kenntnis nur, wenn nötig“ erfordert. In diesem Falle werden der zuständigen VS-Registratur nur der ausgefüllte VS-Begleitzettel und der unterschriebene VS-Empfangsschein zugeleitet.

3. Versand von VS

Bei Weitergabe von VS-VERTRAULICH oder höher eingestuften VS zwischen getrennt liegenden Gebäuden, die nicht zu einer geschlossenen Gebäudegruppe gehören (Versand), sind die nachfolgenden Vorschriften anzuwenden.

3.1 STRENG GEHEIM eingestufte VS sind durch VS-Kurier zu versenden.

3.2 VS-Kuriere, die STRENG GEHEIM oder GEHEIM eingestufte VS befördern, haben einen Dienstwagen mit Fahrer zu benutzen. Ist dies nicht möglich, so ist bei STRENG GEHEIM eingestuften VS ein zweiter VS-Kurier einzusetzen. Die Benutzung öffentlicher Nahverkehrsmittel außer Taxi ist möglichst, bei STRENG GEHEIM eingestuften VS ausnahmslos, zu vermeiden.

3.3 Für die Versendung durch VS-Kurier ist ein neutraler, verschlossener VS-Transportbehälter mit Zählwerkschloss, an dem ein verdecktes Schild mit Anschrift der Dienststelle angebracht ist, zu benutzen.

3.4 VS-Kuriere haben die VS ständig in persönlichem Gewahrsam zu halten. Können mitgeführte VS nicht ständig in persönlichem Gewahrsam gehalten werden, sind sie nach § 17 der VS-Anweisung aufzubewahren. Ist dies nicht möglich, sind sie verschlossen einer Polizeidienststelle zur sicheren Aufbewahrung zu übergeben.

3.5 GEHEIM oder VS-VERTRAULICH eingestufte VS können durch VS-Kurier oder private Zustelldienste befördert werden. Bei Nutzung eines privaten Zustelldienstes müssen folgende Voraussetzungen erfüllt sein:

1. Beim Absender:
   a) eindeutige Adressierung und zuverlässige Verpackung,
   b) Absendung zum letztmöglichen Zeitpunkt für eine Zustellung bis zum Mittag des folgenden Arbeitstages.

2. Beim privaten Zustelldienst:
   a) Abholung beim Absender mit Zustellungsgarantie bis zum Mittag des folgenden Arbeitstages,
   b) Nachweis der Annahme und Auslieferung der Sendung,
   c) lückenlose DV-gestützte Verfolgung der Sendungen von der Annahme bis zur Auslieferung.

Bei Bedarf erteilt das BSI Auskunft, welche privaten Zustelldienste die Voraussetzungen nach Nummer 2 erfüllen.

3.6 VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS können als gewöhnliche Sendung befördert werden.

4. Versand oder Weitergabe von VS an Parlamente, Privatpersonen oder Unternehmen

4.1 VS, die dem Deutschen Bundestag oder dem Parlament eines Bundeslandes zugänglich gemacht werden sollen, sind von den obersten Bundesbehörden grundsätzlich der VS-Registratur der Verwaltung des Deutschen Bundestages bzw. des Landesparlamentes zur Registrierung zu übersenden.

4.2 Bevor VS an Privatpersonen oder Unternehmen weitergegeben werden, ist erneut zu prüfen, ob die VS-Einstufung in allen Teilen erforderlich ist. Soweit möglich und zweckmäßig, ist eine differenzierte VS-Einstufung vorzunehmen.

4.3 Bei VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS genügt es, das VS-NfD-Merkblatt (Anlage 7) zum Vertragsbestandteil zu machen oder die Privatperson auf diese Bestimmungen hinzuweisen. Vor Weitergabe von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS an ein Unternehmen ist zu prüfen, ob die VS-Einstufung zwingend beibehalten werden muss.

4.4 Für die Weitergabe von VS VERTRAULICH und höher eingestuften VS an Unternehmen gilt § 21 Abs. 4 der VS-Anweisung.

4.5 Privatpersonen dürfen Kenntnis von VS nur erhalten, wenn dies im staatlichen Interesse (z.B. zur Durchführung eines staatlichen Auftrags) erforderlich ist. Sie sind, wenn es sich um VS-VERTRAULICH oder höher eingestufte VS handelt, zuvor gemäß dem Sicherheitsüberprüfungsgesetz und den allgemeinen Verwaltungsvorschriften zur Durchführung von Sicherheitsüberprüfungen (s. § 35 SÜG) zu überprüfen, über die in Betracht kommenden Vorschriften der VS-Anweisung zu unterrichten sowie unter Hinweis auf die Strafbarkeit der Geheimnisverletzung förmlich zur Geheimhaltung zu verpflichten (Muster 1) und zu ermächtigen. Bei Bedarf können an die Stelle vorstehender Bestimmungen besondere Sicherheitsvorschriften treten. VS dürfen Privatpersonen erst dann übergeben werden, wenn Maßnahmen für den Schutz der VS unter sinngemäßer Beachtung der VSA getroffen worden sind (Beispiel: Vorübergehende Überlassung eines VS-Verwahrgelasses).

5. Versand von VS an Empfänger im Ausland

5.1 VS-VERTRAULICH oder höher eingestufte VS an berechtigte Empfänger im Ausland sind durch den Kurierdienst des Auswärtigen Amtes zur zuständigen Auslandsvertretung der Bundesrepublik Deutschland zu versenden; ist diese nicht selbst Empfänger, so ist sie um sichere Weiterleitung an den Empfänger zu ersuchen. Hierbei ist die Geschäftsordnung des Auswärtigen Amtes für den Einsatz von Kurieren zu beachten (RES 21-23 Tz. 1.16.3). Soweit termingebundene VS-Transporte nicht direkt für die Auslandsvertretung bestimmt sind, sondern im Interesse anderer Behörden erfolgen, muss die veranlassende Stelle die damit verbundenen Kosten übernehmen.

VS des Geheimhaltungsgrades STRENG GEHEIM sind zusätzlich zu verschlüsseln oder mit Doppelkurier zu befördern. Die Verschlüsselung für den zivilen Bereich übernimmt das Auswärtige Amt. Das versendende Ressort setzt sich deswegen mit dem Auswärtigen Amt in Verbindung.

5.2 VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS von und zu deutschen Auslandsvertretungen sind ebenfalls durch den Kurierdienst des Auswärtigen Amtes zu versenden. Sendungen an andere Empfänger im Ausland können mit einem privaten Zustelldienst versandt werden.

6. Verpackung für den Versand

6.1 VS-VERTRAULICH oder höher eingestuftes Schriftgut ist in doppeltem Umschlag zu versenden. Der Umschlag darf außer bei VS-VERTRAULICH nicht mehr als einen Vorgang enthalten.

6.2 Die inneren Umschläge müssen so beschaffen sein, dass sie nach Feststellung des Bundesamtes für Sicherheit in der Informationstechnik einen Zugriff auf den Inhalt erkennen lassen.

6.3 Der innere Umschlag ist mit folgenden Angaben zu versenden:

1. Empfänger und Absender,
2. Bezeichnung des Empfangsberechtigten mit dem Zusatz „oder Vertreter im Amt (o.V.i.A.)“,
3. Geheimhaltungsgrad und
4. Geschäftszeichen.

6.4 Sendungen, deren Inhalt aus besonderem Grund nur für den auf dem Umschlag bezeichneten Empfänger bestimmt ist, sind auf dem inneren Umschlag mit dem Zusatz „Persönlich“ zu versehen.

6.5 Der äußere Umschlag darf nur die für die Zustellung erforderlichen Angaben enthalten. Er darf keine Zusätze aufweisen, die Rückschluss auf den Inhalt zulassen oder auf eine Sonderbehandlung der Sendung hindeuten.

6.6 Kuriersendungen sind abweichend von Absatz 1 im einfachen Umschlag zu verpacken und mit dem Geschäftszeichen einschließlich des abgekürzten Geheimhaltungsgrades oder einer Ausgangsnummer zu versehen. Die Übergabe ist vom Kurier und vom Empfänger zu quittieren.

6.7 Beim Versand von VS-VERTRAULICH oder höher eingestuften VS über privaten Zustelldienst ist im inneren Umschlag ein ausgefüllter VS-Empfangsschein beizufügen, der vom Empfänger zurückzusenden ist. Geht der VS-Empfangsschein innerhalb einer angemessenen Frist (in der Regel nach einer Woche) nicht ein, so hat der Absender den Schein anzumahnen.

6.8 Für den Versand von Paketen gelten die vorstehenden Bestimmungen entsprechend.

7. Aufbewahrung von VS-Transportbehältern

VS-Transportbehälter sind so aufzubewahren, dass sie Unbefugten nicht zugänglich sind. Der VS-Verwalter hat darauf zu achten, dass die VS-Transportbehälter nach Gebrauch unverzüglich an die VS-Registratur zurückgegeben werden.

Zu 1.1:
Die Quittung von VS erlangt in folgenden Fällen Bedeutung:

1. Auffinden benötigter VS (Wer ist in ihrem Besitz?).
2. Verlust einer VS (wo und wie?).
3. Verratsfall (Welche VS konnten verraten werden?).

Grundsätzlich ist die Weiterleitung von VS über die VS-Registratur, u. a. zur Erleichterung von Verbleibskontrollen, anzustreben. Davon sollte nur bei Behörden abgewichen werden, bei denen dies aufgrund der Vielzahl der zu bearbeitenden VS-VERTRAULICH und höher eingestuften VS nur mit unverhältnismäßigem Aufwand oder Zeitverlust realisierbar ist.

Das VS-Quittungsbuch nach Muster 1 enthält eine Spalte 11, “Rücklaufkontrolle”. Mit deren Nutzung soll bei Bedarf eine Kontrolle erleichtert werden, ob ausgegebene VS wieder zurückgelangt sind (z. B. in die VS-Registratur).

Bei der Formulierung „Referat oder vergleichbare Organisationseinheit“ wurde von einer überschaubaren Organisationsgröße, innerhalb derer der Verbleib einer VS aufgrund der begrenzten Zahl von VS-Ermächtigten jederzeit feststellbar ist, ausgegangen.

Bei (regelmäßiger) täglicher Rückgabe an die VS-Registratur (vgl. auch § 20 Abs. 2 Satz 1 VSA) entfällt bei VS-VERTTRAULICH eingestuften VS eine Quittungspflicht, soweit keine anders lautende Anweisung vorliegt (vgl. § 46 Abs. 3 VSA).

Zu 1.2:
Mit der Formulierung „soll die VS-Registratur beteiligt werden“ in Satz 2 wird den Besonderheiten in Behörden mit umfangreichem VS-Bestand Rechnung getragen.

Zu 1.3:
Die Formulierung „innerhalb desselben Ortes“ schließt den näheren Einzugsbereich des Ortes mit ein.

Zu Abschn. 2:
Klebemappen/Umschläge und VS-Transportbehälter für sich alleine bieten nur einen sehr begrenzten Schutz vor unbefugtem Zugriff auf VS. Der Kontrolle der für den Transport benötigten Zeit sowie des Zählwerkstandes bei VS-Transportbehältern kommt deshalb besondere Bedeutung zu. Nur im Verbund damit ist eine angemessene Sicherheit zu erzielen.

Im Übrigen müssen insbesondere die VS-Verwalter darauf achten, dass die Klebemappen/Umschläge ordnungsgemäß verschlossen sind (z.B. kein Überkleben alter, loser Klebestreifen, Trocknung des Klebers abwarten).
In einem Spionagefall wurden Klebemappen mit VS, die allerdings vorschriftswidrig über längere Zeit (z.B. die Nacht über) ungesichert aufbewahrt wurden, heimlich geöffnet und wieder verschlossen.

Die Herstellung bzw. der Einsatz von Klebemappen/-streifen, die ein heimliches Öffnen ausschließen, ist nach Feststellung des BSI nicht möglich bzw. wäre mit unangemessenen Kosten verbunden. Totalfälschungen (neue Mappe, neuer Klebestreifen) sind ohnehin nicht auszuschließen.
Soweit aus arbeitstechnischen Gründen auf dem Klebestreifen auch das Geschäftszeichen benötigt wird, steht einer entsprechenden Ergänzung der Aufschrift nichts entgegen.
VS-Transportbehälter können auch von Boten geöffnet werden, nachdem sich der Empfangsberechtigte vom ordnungsgemäßen Verschluss überzeugt hat (Vergleich Stand des Zählwerkstandes im Quittungsbuch und des Behälters).

Zu 2.6:
Der Präsident des Bundesamtes für Verfassungsschutz bzw. sein Vertreter kann den Versand von VS-VERTRAULICH eingestuften VS auch mit gewöhnlichem Brief zulassen, wenn eine Versendung mit Kurier oder einem privaten Zustelldienst aus taktischen Gründen nicht sinnvoll ist.

Zu 3:
Zur Annahme von VS-VERTRAULICH und höher eingestuften VS ist die Poststelle der Behörde oder Dienststellen über die weitere Verfahrensweise in Kenntnis zu setzen (Dienstanweisung).
Grundsätzlich ist der innere, ungeöffnete Umschlag (siehe Abs. 2.1, 2. Absatz) unverzüglich der VS-Registratur zuzustellen. Diese hat dann, nach Durchführung der geschäftsmäßigen Behandlung der VS, die Zustellung an den berechtigten Empfänger sicherzustellen. Abweichende Sonderregelungen, (z. B. entsprechend Abschn. 2.6) sind zu berücksichtigen.
Bei Behörden/Dienststelle die über keine gesonderte VS-Registratur verfügen, ist der innere, ungeöffnete Umschlag der Behörden-/Dienststellenleitung unverzüglich vorzulegen.

Zu 3.5 letzter Satz:
Diese Angabe wurde aus der VSA, Stand: 1994 übernommen. Zwischenzeitlich führt das Bundesamt für Sicherheit in der Informationstechnik keine diesbezüglichen Marktbeobachtungen mehr durch.
Es ist ausreichend, wenn der private Zustelldienst die Einhaltung der unter Abschn. 3.5 Ziffer 2 aufgeführten Anforderungen bestätigt (Firmenerklärung).

Zu 7:
Diese Bestimmung soll verhindern, dass Transportbehälter über längere Zeit unbemerkt entfernt und manipuliert werden können.

Anlage 7 zur VS-Anweisung

Merkblatt zur Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)

Das Merkblatt ist für die Unterrichtung der Mitarbeiter von Dienststellen für den allgemeinen Umgang mit VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufter VS gedacht, insbesondere aber für Verträge mit privaten Firmen und Organisationen über die Erbringung von als Verschlusssache VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Leistungen. Die Bestimmungen dieses Merkblattes sollen in die Vertragsgestaltung einfließen.

I. Allgemeines

1. Zugangsberechtigung und Weitergabe

1.1. VS des Geheimhaltungsgrades VS-NfD dürfen nur Personen zugänglich gemacht werden, die im Zusammenhang mit der Auftragsdurchführung oder bei der Auftragsanbahnung Kenntnis erhalten müssen (Grundsatz „Kenntnis nur, wenn nötig“). Den zugangsberechtigten Personen ist dieses Merkblatt vor dem Zugang zu solchen VS nachweislich bekannt zu geben; sie werden auf ihre besondere Verantwortung für den Schutz der VS gemäß diesem Merkblatt sowie eventuelle strafrechtliche oder vertragsrechtliche Konsequenzen bei Zuwiderhandlung hingewiesen.

Weitergehende Maßnahmen wie ein Geheimschutzverfahren des Bundesministeriums für Wirtschaft und Technologie (BMWi), Sicherheitsüberprüfungen oder formale Besuchsanmeldungen sind bei diesem Geheimhaltungsgrad nicht erforderlich.

1.2. Über den Inhalt der VS ist Verschwiegenheit gegenüber Nichtbeteiligten zu wahren. Mitarbeiter, die sich zum Umgang mit solchen VS als ungeeignet erwiesen oder gegen die Verpflichtung zur Geheimhaltung verstoßen haben, sind von der Bearbeitung solcher VS auszuschließen.

1.3. Die Weitergabe von als VS-NfD eingestuften VS darf nur an Regierungsstellen, zwischenstaatliche Organisationen oder Auftragnehmer erfolgen, die an einem Programm/Projekt/Auftrag beteiligt sind und die Zugang zu den Informationen im Zusammenhang mit der Bearbeitung des Programms/Projekts/Auftrags haben müssen. Vor der Weitergabe von VS-NfD eingestuften VS an nicht beteiligte zwischenstaatliche Organisationen oder Auftragnehmer aus nicht beteiligten Ländern ist die schriftliche Einwilligung des amtlichen VS-Auftraggebers der VS einzuholen. Grundsätzlich bedarf es hierbei einer Geheimschutzvereinbarung (Siehe auch § 23 VSA).

1.4. In Deutschland kann sich das BMWi beim VS-Auftragnehmer über die Einhaltung der Bestimmungen dieses Merkblattes vergewissern. Ist Auftraggeber eine Behörde, kann auch diese die Kontrollrechte nach Satz 1 wahrnehmen.

1.5. Die VS-Einstufung ist dreißig Jahre nach dem 1. Januar des auf die Einstufung folgenden Jahres aufgehoben, sofern keine andere Frist bestimmt ist. Bei internationalen Aufträgen ist das BMWi zu konsultieren, sofern keine Programm- oder Projektvereinbarungen bestehen (Siehe auch § 26 VSA).

2. Bearbeitungsmaßnahmen

2.1. Kennzeichnung und Handhabung bzw. Verwahrung

Dokumente und Material des Geheimhaltungsgrades VS-NfD sind wie folgt zu kennzeichnen, zu behandeln und zu verwahren:

2.1.1. Dokumente sind durch schwarzen oder blauen Stempelaufdruck, Druck „VS – NUR FÜR DEN DIENSTGEBRAUCH“ am oberen Rand jeder beschriebenen Seite sowie aller entsprechend eingestuften Anlagen zu kennzeichnen bzw. im Falle internationaler oder ausländischer VS mit der entsprechenden deutschen Kennzeichnung umzustempeln. Bei Büchern, Broschüren u.Ä. genügt die Kennzeichnung auf dem Einband und dem Titelblatt. Trägt jede beschriebene Seite eines ausländischen Buches oder einer ausländischen Broschüre den ausländischen Geheimhaltungsgrad, genügt die Kennzeichnung mit dem deutschen Geheimhaltungsgrad auf dem Einband oder dem Titelblatt.

2.1.2. VS-NfD eingestuftes Material (z.B. Gerät, Ausrüstung) oder Datenträger (z.B. Disketten, CDs, Mikrochips, Mikrofiche) sind ebenfalls entweder deutlich sichtbar am Material selbst oder – falls dies nicht möglich ist – an den Aufbewahrungsbehältnissen des Materials zu kennzeichnen bzw. grundsätzlich umzustempeln.

2.1.3. Die VS sind in verschlossenen Räumen oder Behältern (Schränken, Schreibtischen usw.) zu verwahren. Außerhalb von solchen Räumen oder Behältnissen sind sie stets so aufzubewahren bzw. zu behandeln, dass Unbefugte keinen Zugang zu oder Einblick in die VS haben.

2.1.4. VS-Zwischenmaterial (z.B. Vorentwürfe, Stenogramme, Tonträger, Folien) ist gegen Einsichtnahme Unbefugter in derselben Weise zu schützen wie das Bezugsdokument. VS-Zwischenmaterial, das nicht an Dritte weitergegeben und unverzüglich vernichtet wird, muss nicht als VS gekennzeichnet werden.

2.2. Weitergabe

2.2.1. Die Weitergabe in Deutschland erfolgt durch Boten oder Versand durch Zustelldienste in einfachem verschlossenen Umschlag bzw. Behältnis. Der Umschlag bzw. das Behältnis erhalten keine VS-Kennzeichnung.

2.2.2. VS können durch private Zustelldienste als gewöhnlicher Brief bzw. Paket oder auch als Luft- oder Seefracht in das Ausland versendet werden, es sei denn, der VS-Auftraggeber hat dieser Versendungsart ausdrücklich widersprochen oder andere Modalitäten für den Auslandsversand festgelegt. Dabei sind vom VS-Auftraggeber zwischenstaatliche Vereinbarungen bzw. besondere Programm- oder Projektvereinbarungen zu berücksichtigen.

2.3. Vernichtung/Rückgabe

2.3.1. Um größere Bestände von VS zu vermeiden, sind nicht mehr benötigte VS zu vernichten oder an den VS-Auftraggeber zurückzugeben.

2.3.2. VS, auch VS-Zwischenmaterial, sind so zu vernichten, dass der Inhalt nicht mehr erkennbar ist und nicht mehr erkennbar gemacht werden kann.

2.4 Verlust, unbefugte Weitergabe, Auffinden von VS oder Nichtbeachtung des Merkblatts

Der Verlust, die unbefugte Weitergabe sowie das Auffinden von VS oder die Nichtbeachtung dieses Merkblattes ist unverzüglich dem deutschen VS-Auftraggeber und ggf. dem BMWi mitzuteilen, um einen eventuell entstandenen Schaden zu begrenzen und den Vorfall aufzuklären.

2.5. Besuche

Besuche in das oder aus dem Ausland mit Zugang zu VS-NfD oder vergleichbarem Geheimhaltungsgrad werden in der Regel unmittelbar zwischen der entsendenden und der zu besuchenden Einrichtung vereinbart. Es gibt keine besonderen Formvorschriften.

2.6. Aufträge

2.6.1. Alle VS-Auftragnehmer/-Unterauftragnehmer sind vom VS-Auftraggeber vertraglich zu verpflichten, die Regelungen dieses Merkblattes zu beachten. Dabei ist darauf hinzuweisen, dass eine Nichtbeachtung die Auflösung des Vertrages bzw. von Teilen des Vertrages zur Folge haben kann.

2.6.2. Bei Angeboten bzw. der Aufforderung zur Abgabe von Angeboten und nach Auftragsdurchführung sind VS bis zur Aufhebung der Einstufung vorschriftsmäßig zu verwahren, baldmöglichst zu vernichten oder zurück zu geben.

2.6.3. VS-Auftragnehmer/-Unterauftragnehmer im Ausland sind vertraglich zu verpflichten, die Vorschriften ihrer zuständigen Sicherheitsbehörde für die Behandlung von VS vergleichbaren Geheimhaltungsgrades zu beachten. Gibt es keinen vergleichbaren Geheimhaltungsgrad in dem Land eines VS-Auftragnehmers/-Unterauftragnehmers, ist das BMWi einzuschalten, das Regelungen für den Schutz mit der zuständigen ausländischen Sicherheitsbehörde vereinbart. Die Weitergabe darf dann erst nach Zustimmung des BMWi erfolgen.

II. Nutzung von Informationstechnik (IT)

1. Bearbeitung

1.1. Wird IT für die Bearbeitung von VS-NfD eingestuften VS genutzt, sind zum Schutz der VS (entsprechend Teil I 1.1 und 1.2) geeignete informationstechnische Maßnahmen und / oder materielle und organisatorische Maßnahmen zu treffen .

1.2. Vor der Bearbeitung oder Speicherung von VS-NfD eingestuften VS ist sicherzustellen, dass das Gerät oder das interne Netzwerk nicht unmittelbar (z.B. ohne Schutz durch eine Firewall) mit dem Internet verbunden ist, sofern nicht weitergehende Maßnahmen entsprechend 3.3 aufgeführt, ergriffen worden sind.

1.3. Bei der Bearbeitung von VS-NfD eingestuften VS kommen insbesondere folgende Maßnahmen in Betracht:

- Übersicht über die Zugriffsberechtigungen,
- Nutzung von Identifizierungs- und Authentisierungsmechanismen (z.B. Login, Passwort),
- geeignete IT-Sicherheitsanweisung (einzelplatz- oder unternehmensbezogen).

Funktastaturen und Funk-Netzwerke dürfen nur eingesetzt werden, wenn sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind.

1.4 Werden für die Bearbeitung oder Speicherung von VS-NfD eingestuften Daten tragbare IT-Systeme (z.B. Notebooks oder Handhelds) eingesetzt, sind die verwendeten Speichermedien durch vom BSI zugelassene Produkte zu verschlüsseln. Sofern Programme und Geräte mit BSI-Zulassung nicht verfügbar sind, können durch das BSI nach Common Criteria, Prüftiefe mindestens EAL 3, zertifizierte Produkte verwendet werden.

1.5 Transportable Datenträger (z.B. Disketten, CDs, Wechselplatten), die VS-NfD eingestufte Daten unkryptiert enthalten, sind gemäß Teil I 2.1.2 zu kennzeichnen und gemäß Teil I 2.1.3 aufzubewahren.

1.6 Das Löschen von Datenträgern hat mit Hilfe von Softwareprodukten zu erfolgen, die mindestens ein zweifaches Überschreiben vorsehen. Hierbei soll auf vom BSI empfohlene Produkte zurückgegriffen werden.

1.7 Informationstechnik und Datenträger sind auf Virenbefall (insbesondere Trojanische Pferde oder Würmer) zu überprüfen bevor VS-NfD damit bearbeitet werden. Diese Prüfung ist in regelmäßigen Zeitabständen zu wiederholen.

1.8 Private Informationstechnik (z.B. Laptops), Software oder Datenträger dürfen nicht für die Bearbeitung eingesetzt werden. In für VS-NfD genutzten Informationssystemen dürfen keine private Software oder private Datenträger verwendet werden.

1.9 Auf fest installierten Datenträgern, die VS-NfD eingestufte Daten unkryptiert enthalten, sind die Verschlusssachen gemäß 1.6 zu löschen, bevor die Datenträger im Rahmen von Wartungs- oder Reparaturarbeiten an IT-Systemkomponenten den Bereich der zugriffsberechtigten Personen verlassen. Ist eine Löschung nicht möglich, sind die Datenträger auszubauen und zurückzubehalten bzw. ist die Wartungs-/Reparaturfirma vertraglich auf die Einhaltung der Regeln dieses Merkblattes zu verpflichten.

2. Übertragung

2.1. Bei der elektronischen Übermittlung auf Telekommunikations- oder anderen technischen Kommunikationsverbindungen (einschließlich Onlinedienste wie WWW, FTP, TELNET, E-Mail etc.) in Deutschland sind die VS mit einem vom BSI zugelassenen, zertifizierten (§ 40 VSA) oder vom BMWi freigegebenen Kryptosystem zu kryptieren. Abweichend davon ist ausnahmsweise eine unkryptierte Übertragung zulässig:
a) innerhalb von Festnetzen bei Telefongesprächen, bei Videokonferenzen und bei Fernkopien und Fernschreiben, wenn zwischen Absender und Empfänger für die erforderliche Übertragungsart keine Kryptiermöglichkeit besteht und der VS-Auftraggeber bei der Auftragsvergabe nicht ausdrücklich eine Kryptierung verlangt. Die absendende Stelle hat sich vor der Übertragung möglichst zu vergewissern, dass sie mit dem richtigen Empfänger verbunden ist,
b) innerhalb eines geschlossenen Netzes (LAN), wenn es ausschließlich auf einem örtlich zusammenhängenden firmeneigenen Gelände betrieben wird und die Übertragungseinrichtungen gegen unmittelbaren Zugriff Unbefugter geschützt sind.

2.2. Bei grenzüberschreitenden elektronischen Übermittlungen müssen die Verschlüsselungsverfahren zwischen den nationalen Sicherheitsbehörden der beteiligten Staaten abgestimmt werden. Sofern in einem Programm/Projekt besondere Sicherheitsanweisungen für die Übermittlung vereinbart wurden, sind diese zu beachten. Bei Bedarf erteilt das BMWi weitere Auskünfte.

3. Maßnahmen zum Schutz der Vertraulichkeit

Die im Folgenden empfohlenen Maßnahmen sollen die Vertraulichkeit der elektronisch gespeicherten VS sicherstellen. Sie dienen nicht in erster Linie dazu, die Integrität und die Verfügbarkeit der Daten zu gewährleisten.

Drei unterschiedliche Ausgangsituationen sind zu unterscheiden:

3.1. Einzelplatz-PC oder Netzwerke mit geschlossenen Nutzergruppen, die nicht mit anderen Netzen verbunden sind

- Das Betriebssystem muss ein differenziertes Benutzerprofil und Zugriffschutz bis auf Dateiebene gewährleisten, damit der Grundsatz „Kenntnis nur, wenn nötig“ sichergestellt wird (z. B. Unix/Linux; Win NT; Win 2000, Win XP).

- Es muss ein Login und ein Passwort vorhanden sein. Das Passwort muss mindestens 6 alphanumerische Stellen, Sonderzeichen; Groß- und Kleinbuchstaben enthalten.

- Das BIOS muss ebenfalls durch ein Passwort geschützt sein.

- Ein Booten des IT-Systems darf grundsätzlich nur von der Festplatte aus möglich sein.

- Es sollte – falls möglich – eine RAM-Disk für die Temp-Dateien enthalten (Nutzungshilfe).

- Ein aktuelles Virenschutzprogramm muss eingesetzt sein.

- Bei Netzwerken sollte eine eigene Partition zum Speichern der VS-Daten auf dem Server installiert werden.

3.2. Geschlossene Netze mit E-Mail-Anschluss nach außen

Zusätzlich zu den unter Nummer. 3.1 festgelegten Punkten muss

- ein serverbasiertes Netz vorhanden sein, bei dem der Server im zugangsgeschützten Bereich steht,

- eine Firewall vorhanden sein, entweder auf dem Server oder als eigenes IT-System (und ggf. zusätzlich E-Mailserver) auch im zugangsgeschützten Bereich, - ein Paketfilter eingesetzt werden; ein Application-Gateway ist möglich,

- jede weitere IP-Adresse, außer der Server-IP, nach außen verborgen werden (DNS-Server),

- die Übertragung von VS-NfD verschlüsselt erfolgen, wobei für die Verschlüsselung nur vom BMWi freigegebene Produkte eingesetzt werden dürfen; Schlüssel sind grundsätzlich nicht auf der Festplatte abzulegen. Es müssen verbindliche Anwenderregelungen innerhalb des Unternehmens festgelegt und geschult werden. Die neuesten Sicherheits-Updates der genutzten Software sind nach Verfügbarkeit insbesondere auch an der Firewall einzubinden.

3.3. Standalone-PC oder Geschlossene Netze mit E-Mail- und Internetanschluss

Zusätzlich zu den unter Nummer. 3.1 und Nummer. 3.2 festgelegten Punkten müssen

- eine Firewall und ein Application-Gateway vorhanden sein,

- die Regelungen des BSI-Grundschutzhandbuchs für Passwörter angewendet werden,

- VS-NfD-Daten auf dem Server in einer eigenen Partition bzw. in einem speziell geschützten Datenbereich gehalten werden; die dadurch gegebenen Schutzmechanismen sind entsprechend anzuwenden.

Je nach Umfang ist die Einrichtung eines eigenen VPN z.B. für eine Nutzergruppe oder ein Projekt erforderlich.

Anlage 8 zur VS-Anweisung

Richtlinie für die Abgabe von Verschlusssachen an das Geheimarchiv des Bundesarchivs (VS-Archivrichtlinie – VS-ArchR)

§ 1 Allgemeines / Grundlagen

(1) Nach dem „Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz – BArchG)[1]“ ist das Archivgut des Bundes durch das Bundesarchiv auf Dauer zu sichern und nutzbar zu machen. Ohne Zustimmung des zuständigen Archivs dürfen VS daher nicht vernichtet werden.

(2) Eine übermäßig lange Verwahrung von VS-eingestuften Unterlagen in den Geheimregistraturen kann zu teilweise irreparablen konservatorischen Schäden oder sogar zu Verlusten führen. Eine rechtzeitige Abgabe der nicht mehr oder nicht mehr laufend zur Aufgabenerfüllung benötigten VS an das Geheimarchiv des Bundesarchivs ist daher geboten.

§ 2 Geheimarchiv[2]

(1) Das Geheimarchiv des Bundesarchivs hat die Aufgabe, STRENG GEHEIM, GEHEIM und VS-VERTRAULICH eingestufte VS, die für die Verwaltungsarbeit nicht mehr oder nicht mehr laufend benötigt werden, zu verwahren.

(2) An das Geheimarchiv sind vollständige Aufbewahrungseinheiten (z.B. Hefter, Stehordner, Filme oder Bänder) abzugeben. Der Ordnungszustand ist nicht zu verändern (z.B. keine Entnahme von Schriftstücken).

(3) Anschriften und nähere Hinweise enthält das Merkblatt „Aussonderung von VS und deren Abgabe an das Geheimarchiv des Bundesarchivs“. Das Merkblatt und die Vorlagen für das Abgabeverzeichnis sowie die Aufhebung der VS-Einstufung werden auf der Website des Bundesarchivs – www.bundesarchiv.de – vorgehalten.

§ 3 Festsetzung der Aufbewahrungsfrist und der Dauer der VS-Einstufung

(1) Vor einer Abgabe von VS hat die abgebende Stelle das Endjahr der Aufbewahrungsfrist und der VS-Einstufung je Aufbewahrungseinheit festzulegen.

(2) Die Aufbewahrungsfrist ist so kurz wie möglich und unabhängig vom Zeitraum der VS-Einstufung zu bemessen. § 19 der Registraturrichtlinie (RegR) ist entsprechend anzuwenden.

(3) Für deutsche VS bestimmt sich die Frist für die Aufhebung der VS-Einstufung nach § 9 Abs. 1 bis 4 VSA.

(4) Das Bundesarchiv hat das Recht, sich bei nicht gerechtfertigt erscheinenden, insbesondere überlangen Einstufungsfristen an die zuständige oberste Bundesbehörde mit der Bitte um Überprüfung der Einstufungsbegründung zu wenden.

§ 4 Behandlung der VS im Archiv

(1) Das Geheimarchiv weist die übernommenen Aufbewahrungseinheiten anhand der Abgabeverzeichnisse nach.

(2) Auf Anforderung der abgebenden Stelle stellt das Geheimarchiv dieser die VS wieder zur Verfügung.

(3) Das Geheimarchiv kann die ihm übergebenen VS, soweit sie nicht versiegelt oder auf andere Weise besonders gesichert sind, für Archivzwecke bearbeiten.

(4) Nach Aufhebung der VS-Einstufung werden die archivwürdigen Unterlagen in die Archivbestände des Bundesarchivs übernommen. Nicht-archivwürdige VS werden nach Ablauf der Aufbewahrungsfrist vernichtet.

---

[1] Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz – BArchG) vom 6. Januar 1988 (BGBl. I S. 62), zuletzt geändert durch Gesetz zur Änderung des Bundesarchivgesetzes vom 5. Juni 2002 (BGBl. I S. 1782)

[2] Bundesarchiv-Zwischenarchiv, Bundesgrenzschutzstr. 100, 53757 St. Augustin und Bundesarchiv-Militärarchiv, 79024 Freiburg

(5) Die Vernichtung wird abweichend von § 28 Abs. 3 VSA im Abgabeverzeichnis nachgewiesen. Die Aufhebung der VS-Einstufung wird abweichend von § 16 Abs. 3 VSA nur auf der Aufbewahrungseinheit kenntlich gemacht.

§ 5 Nutzung der VS durch Dritte

(1) Die Nutzung von im Geheimarchiv des Bundesarchivs verwahrten VS durch Dritte bedarf der vorherigen Zustimmung der abgebenden Stelle. Die Zustimmung ist nur zu erteilen, soweit die Nutzung amtlich veranlasst ist oder im amtlichen Interesse liegt und mit der Geheimhaltungsbedürftigkeit der VS vereinbar ist. Soweit Geheimschutzinteressen anderer Stellen berührt sind, hat die abgebende Stelle sich zuvor mit diesen abzustimmen.

(2) Vor einer Genehmigung der Nutzung von VS durch Dritte (z.B. Wissenschaftler) ist die Möglichkeit der Offenlegung dieser VS zu prüfen. VS, die Dritten zur Nutzung zur Verfügung gestellt worden sind, sollen im Interesse der Wissenschaftlichkeit, der Gleichbehandlung und der Nachprüfbarkeit der Ergebnisse einer Benutzung offen gelegt werden.

(3) Die Vorschriften von § 5 Abs. 5 BArchG und § 39 GGO gelten entsprechend.

§ 6 Schlussbestimmungen

(1) Dem Geheimarchiv ist der Wechsel der Zuständigkeit für im Geheimarchiv verwahrte VS infolge Aufgabenverlagerungen schriftlich mitzuteilen. Vor der Weitergabe von VS-Unterlagen an die nunmehr zuständige Stelle gemäß § 23 RegR prüft die bislang zuständige Stelle, welche VS an das Geheimarchiv abgegeben werden können.

(2) Das Auswärtige Amt und das Bundesministerium der Verteidigung können für ihre Bereiche in Übereinstimmung mit den Grundsätzen dieser Richtlinie eigene Bestimmungen erlassen.

(zu § 2 (3) VS-ArchR)

Bundesarchiv Stand: 16.9 2005

B 1 – 2051/1

Merkblatt für die Aussonderung von VS und deren Abgabe an das Geheimarchiv des Bundesarchivs

I. Allgemeines

1. Die Aussonderung von VS richtet sich nach § 26 in Verbindung mit Anlage 8 (VS-Archivrichtlinie, VS-ArchR) der VS-Anweisung (VSA).
2. Bei der Abgabe von VS an das Geheimarchiv ist § 20 Registraturrichtlinie (RegR) entsprechend anzuwenden. Das Vorblatt zum Verzeichnis für die Abgabe von VS an das Geheimarchiv sowie das Verzeichnis für die Abgabe von VS an das Geheimarchiv (Abgabeverzeichnis) sind als Anlage 2 und Anlage 3 zum Herunterladen beigefügt.
3. Für VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS und für Unterlagen, deren VS-Einstufung aufgehoben wurde, gelten die für nicht eingestufte Unterlagen festgelegten Regelungen.
4. VS, deren Aufbewahrungsfrist abgelaufen ist und denen offensichtlich kein bleibender Wert zukommt, können mit schriftlicher Zustimmung des Bundesarchivs bereits in der Behörde vernichtet werden (vgl. § 22 RegR).
5. Bei Aussonderungsproblemen und -fragen stehen die Leiter der Geheimarchive in St. Augustin und in Freiburg sowie die zuständigen Archivare in Koblenz, Berlin oder Freiburg zur Verfügung.

II. Technische Hinweise für das Aussondern

1. Empfohlen wird, jede voraussichtlich auszusondernde Akte (Aufbewahrungseinheit) dem zuständigen Bearbeiter mit einem entsprechenden Formblatt vorzulegen. Auf diesem Formblatt hat dieser anzugeben:
   - ob und ggf. wann diese Aufbewahrungseinheit auszusondern ist,
   - ob und ggf. bis zu welchem Jahr sie für einen Rückgriff bereitzuhalten ist (Aufbewahrungsfrist),
   - zu welchem Jahr die Aufhebung der VS-Einstufung erfolgt.
2. Im Falle der Aufhebung der VS-Einstufung bereits zum Zeitpunkt der Abgabe der Unterlagen ist diese auf der Aufbewahrungseinheit (Muster: Anlage 1) zu vermerken. Die Abgabe erfolgt nach dem Verfahren für offene Unterlagen.
3. VS-Schriftgut ist in der Ordnung anzubieten und ggf. zu übergeben, die in der VS-Registratur bestand. Ein Neu- oder Umordnen ist deshalb zu vermeiden. Zu unterlassen ist auch die nachträgliche Entfernung einzelner Schriftstücke aus einer Akte oder deren Abheftung in einem anderen Schriftgutbehälter.
4. In dem Abgabeverzeichnis (Anlage 3) sind die Akten vollständig und zutreffend aufzulisten. Dies gilt vor allem für Aktenzeichen und Inhaltsangaben, wobei die Inhaltsangaben so formuliert werden sollten, dass das Abgabeverzeichnis nicht höher als VS-NfD einzustufen ist. Ein sorgfältiges Ausfüllen des Vorblatts (Anlage 2) erleichtert den späteren Rückgriff.
5. Das Abgabeverzeichnis mit Vorblatt ist dem Bundesarchiv in Papierform oder in elektronischer Form zuzuleiten. Das Geheimarchiv übersendet der abgebenden Stelle eine Kopie des Abgabeverzeichnisses mit den eingetragenen Archivnummern.
6. Für die spätere archivische Bearbeitung der an das Geheimarchiv abgegebenen VS sollten dem Bundesarchiv auch der entsprechende VS-Aktenplan, soweit ein solcher vorhanden ist, sowie das VS-Aktenverzeichnis, nicht jedoch schriftstückbezogene VS-Bestandsverzeichnisse (z.B. Tagebuch), zur Verfügung gestellt werden.

III. Weiterführende Hinweise

7. Grundsätzlich ist – wie beim offenen Schriftgut – sachlich Gleiches bearbeitungsgerecht zu Sachakten (Einzel-, Sammel- und Sondersachakten) zusammenzufassen; auf die entsprechenden Regelungen der Registraturrichtlinie und die Erläuterungen der „Empfehlungen für die Schriftgutverwaltung“ wird hingewiesen. Unter dem Gesichtspunkt des späteren leichteren Aussonderns können umfangreiche Unterlagen anderer Stellen getrennt geordnet werden, soweit sich nicht aus der Bearbeitung heraus eine Zusammenfassung empfiehlt.
8. Zwischen aktenführender Behörde und dem Bundesarchiv kann vereinbart werden, dass zusätzlich zu dem VS-Zwischenmaterial und den technischen Einrichtungen (z.B. technische Modelle) bestimmte VS-Komplexe unmittelbar in der Behörde in eigener Verantwortung vernichtet werden können. Diese Komplexe sollten in einem Aussonderungs- und Bewertungskatalog zusammengefasst werden. In Zweifelsfällen (z.B. bei anstehenden Aussonderungen umfangreicher Unterlagen) kann der zuständige Archivar des Bundesarchivs auf dem Wege der Vorbewertung die an das Geheimarchiv abzugebenden Unterlagen in der VS-Registratur bestimmen.
9. Bei gleichartigen, in größerer Zahl anfallenden Unterlagen (insbesondere so genannte Fallakten) ist das Bundesarchiv für entsprechende Hinweise der Bearbeiter, die den Inhalt der Akten kennen und aus fachlicher Sicht beurteilen können, dankbar. In Betracht für eine dauernde Aufbewahrung kommen Akten vornehmlich wegen der Bedeutung des Falls oder Sachverhalts oder wegen Besonderheiten (z.B. neuartiges technisches Verfahren). Hier sollte der Bearbeiter diejenigen Aufbewahrungseinheiten auf geeignete Weise (z.B. auf dem Aktenvorblatt) kennzeichnen, die nach seiner Auffassung für eine dauernde Aufbewahrung infrage kommen. Diese Kennzeichnung kann bereits bei der ZdA-Verfügung oder erst bei der Festlegung von Fristen geschehen.
10. Die Bestimmungen der ZDv 64/3 VS-NfD "Behandlung und Sicherung von Unterlagen der Bundeswehr im Frieden und bei Alarmierung" sind bei der Abgabe von VS aus dem Geschäftsbereich des BMVg zu beachten.

III. Behandlung der VS im Geheimarchiv des Bundesarchivs

1. Bei der Kontrolle der abgegebenen Unterlagen beschränkt sich die Überprüfung durch das Geheimarchiv auf Aufbewahrungseinheiten (Akten), nicht jedoch auf einzelne Schriftstücke.
2. Das Bundesarchiv kann die übernommenen Unterlagen – nach Ablauf evtl. bestehender Aufbewahrungsfristen – im Zuge der archivischen Bearbeitung noch im Einzelfall vernichten.
3. Die Aufhebung der VS-Einstufung vermerkt das Geheimarchiv auf der Aufbewahrungseinheit (Muster: Anlage 1).
4. Nach der Aufhebung der VS-Einstufung und archivischen Erschließung werden die archivwürdigen Unterlagen in den entsprechenden offenen Archivbestand im Endarchiv in Koblenz überführt. Auf Anfrage erhält die jeweilige Behörde den Nachweis über den endgültigen Verbleib einer VS-Aufbewahrungseinheit.

V. *Weiterführende Angaben*

Vorschriften zur Schriftgutverwaltung

Die Gemeinsame Geschäftsordnung der Bundesministerien (GGO) von 2000 und die Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien (RegR) von 2001 sind einzusehen über www.staat-modern.de, Papierausgaben können über bestellservice@bva.bund.de bestellt werden.

Die RegR von 2001 kann als Mustervorschrift auch für nichtministerielle Dienststellen dienen. Detaillierte Ausführungen enthält das Merkblatt „Die nichtministerielle Bundesverwaltung und das Bundesarchiv“ (www.bundesarchiv.de).

Empfehlenswerte Literatur zur Schriftgutverwaltung

- Empfehlungen zur Schriftgutverwaltung. Hrsg. vom Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung und vom Bundesministerium des Innern, 2. Aufl. 1989. 103 S.
- Schriftgutverwaltung in Bundesbehörden – eine Einführung in die Praxis. Hrsg. vom Bundesverwaltungsamt - Bundesstelle für Büroorganisation und Bürotechnik. 2. überarbeitete Auflage Köln 2005. Zu beziehen als .pdf-Download über http://www.bva.bund.de unter „Veröffentlichungen A-Z“ .
- Heinz Hoffmann: Behördliche Schriftgutverwaltung. Ein Handbuch für das Ordnen, Registrieren, Aussondern und Archivieren von Akten der Behörden. 2. Aufl. München 2000. XVIII, 647 S. (Schriften des Bundesarchivs 43). Über den Buchhandel zu beziehen.
- DOMEA-Konzept. Erweiterungsmodul zum Organisationskonzept 2.0: Aussonderung und Archivierung elektronischer Akten. Schriftenreihe der KBSt. Bd. 66, Bonn 2004 (www.kbst.bund.de)

Angaben über das Bundesarchiv

- Informationen unter der Internet-Adresse www.bundesarchiv.de
- Das Bundesarchiv. Dienstleister für Forschung, Öffentlichkeit und Verwaltung. Koblenz 2002. 137 S.

Anschriften des Bundesarchivs

Abteilung Bundesrepublik Deutschland

56064 Koblenz

Potsdamer Str. 1, 56075 Koblenz

Telefon: 0261/505-0

Telefax: 0261/505-226

E-Mail: koblenz@barch.bund.de

und

12175 Berlin, Postfach: 450 569

Finckensteinallee 63 , 12205 Berlin

Telefon: 01888/7770-0

Telefax: 01888/7770-111

E-Mail: berlin@barch.bund.de

Geheimarchiv

Bundesgrenzschutzstr. 100, 53757 St. Augustin-Hangelar

Telefon: 01888/74000-0

Telefax: 01888/74000-33

E-Mail: zwarchst.aug@barch.bund.de

Abteilung Militärarchiv und Militärisches Geheimarchiv

79024 Freiburg

Wiesentalstr. 10, 79115 Freiburg

Telefon: 0761/47817-0

Telefax: 0761/47817-900

E-Mail: militaerarchiv@barch.bund.de

Anlage 1

Dienststelle	
Ort	Datum

Aufhebung der VS-Einstufung

Für die anliegende Aufbewahrungseinheit

Betreff
Geschäftszeichen[1]

ist die VS-Einstufung mit Wirkung vom ..... aufgehoben.

.....

(Name, Unterschrift) Dienstsiegel

[1] Bei Benutzung dieses Formblatts durch das Bundesarchiv (Abschnitt IV, Ziff. 3) ist hier nur die Archivsignatur einzutragen.

Vorblatt zum Verzeichnis für die Abgabe von **Anlage 2**

VS an das Geheimarchiv

Ausfüllhinweise:

- Möglichst vollständig ausfüllen
- Bei Bedarf Rückseite ausfüllen (mit Angabe der Zeilennummer)
- Zeilen 5 - 7 nur für Akten ausfüllen
- Bitte Fußnoten beachten

vom Geheimarchiv auszufüllen

1	Archivsignatur

2	Abgebende Behörde (Kurzbezeichnung)			Anzahl der Aufbewahrungseinheiten
3	Zustimmende Organisationseinheit	Datum	Hausruf	Unterschrift
4	Abgabe aus VS-Reg.	Abgabe am [1)]	Hausruf	Name

5	Stichwortartige Inhaltsangabe in Anlehnung an Angaben des Organisations- oder Geschäftsverteilungsplans, möglichst für das Endjahr der Laufzeit der Akten [2)]	
6		Laufzeit (Jahreszahl des ältesten und jüngsten Schriftstücks)
7	Benennung der Aktenplanteile mit Kennzeichen und Begriffsbezeichnung [3)]	
8	Letzte aktenführende Organisationseinheit(en) [4)]	

---

1) Gilt auch als Ausstellungsdatum des Abgabeverzeichnisses.

2) Bei (unter-)abteilungsbezogenen Abgaben reicht die Sachbezeichnung der (Unter-)Abteilung aus. Falls nicht möglich, nur das Feld 7 ausfüllen.

3) Bei umfangreichen Abgaben ist oft nur eine grobe Beschreibung möglich (z.B. nur Angabe der Aktenplan-Hauptgruppen).

4) Bei der Reihung des Schriftguts mehrerer Organisationseinheiten nach dem Aktenzeichen ist die Erläuterung Nr. 4 zu Anlage 3 zu beachten.

9	Weitere aktenführende Organisationseinheiten im Zeitablauf [5)]	
	a)	d) .....
	b)	e) .....
	c)	f)
10	Bemerkungen (z.B. Angabe und Begründung von Fristen nach § 5 Abs. 2 und § 7 Abs. 2 VS-ArchR)	

5) Anzugeben sind nach Möglichkeit alle wesentlichen aktenführenden Organisationseinheiten für den in Feld 6 genannten Zeitraum (ggf. auch von Vorgängerbehörden) sowie die Zeitpunkte des Wechsels der Zuständigkeit oder der Benennung. Falls der Zeitraum der Zuständigkeit nicht ermittelt werden kann, ist ein in diesen Zeitraum fallendes Datum anzugeben.

Verzeichnis für die Abgabe von VS an das Geheimarchiv (Abgabeverzeichnis)[1] **Anlage 3**

Lfd. Nr.[2]	Archiv-Nummer[3]	Akten-zeichen[4]	Inhaltsangabe	Band-Nr.[5]	Zeitraum von	Zeitraum bis	Eingestuft bis 31.12. (Jahr)	VS-Grad[6]	Aufzubewahren bis 31.12. (Jahr)	Vernichtungs-vermerk[7]

[1] Die Angaben im Abgabeverzeichnis sind so zu wählen, dass keine höhere Einstufung als VS-NUR FÜR DEN DIENSTGEBRAUCH erforderlich wird.
[2] Jede Aufbewahrungseinheit nach § 3 Abs. 3 (bei Akten: Je nach Art der Ablage Ordner oder Hefter) erhält eine lfd. Nr.; die Nummern sind jeweils einzeln aufzuführen und für jede aufgeführte Akte derselben Aufbewahrungseinheit zu wiederholen.
[3] Diese Spalte wird vom Geheimarchiv ausgefüllt. Bei einer späteren Anforderung sind nur die Archivnummern anzugeben.
[4] Nur für Akten: Sachliche Ordnung gemäß Aktenplan. Zusätzlich kann in einer eigenen Spalte die aktenführende Organisationseinheit angegeben werden, wenn Schriftgut mehrerer Organisationseinheiten nach der Ordnung des Aktenplans aufgeführt wird.
[5] Anzugeben ist bei Akten die lfd. Bandnummer, nicht die Zahl der Bände.
[6] Anzugeben sind nur folgende Großbuchstaben: S (=Streng Geheim), G (= Geheim), V (=VS-Vertraulich), N (=VS-Nur für den Dienstgebrauch).
[7] Anzugeben sind Datum und Unterschrift des Ausführenden und Zeugen.

Stichwortverzeichnis (VSA)

A

B

D

E

P

R

S

T

U

V

W

Z