

Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlussachenanweisung - VSA)

Vom 13. März 2023

Nach Artikel 86 Satz 1 des Grundgesetzes in Verbindung mit § 35 Absatz 1 des Sicherheitsüberprüfungsgesetzes vom 20. April 1994 (BGBl. I S. 867) in Verbindung mit § 1 Absatz 2 des Zuständigkeitsanpassungsgesetzes vom 16. August 2002 (BGBl. I S. 3165) und dem Organisationserlass des Bundeskanzlers vom 8. Dezember 2021 erlässt das Bundesministerium des Innern und für Heimat folgende Allgemeine Verwaltungsvorschrift:

Inhaltsübersicht

Abschnitt I: Allgemeine Bestimmungen

- § 1 Anwendungsbereich
- § 2 Begriff der Verschlussache und Geheimhaltungsgrade
- § 3 Allgemeine Grundsätze
- § 4 Verpflichtung, Ermächtigung und Zulassung
- § 5 Mitwirkende Behörden
- § 6 Mehrschichtige Sicherheit

Abschnitt II: Geheimschutzorganisation und Geheimschutzdokumentation

- § 7 Dienststellenleitung
- § 8 Geheimschutzbeauftragte
- § 8a Risikomanagement
- § 9 IT-Sicherheitsbeauftragte
- § 10 VS-Registrieren
- § 11 Qualifikation

Abschnitt III aufgelöst

- § 12 Erstellung der Geheimschutzdokumentation
- § 13 gestrichen
- § 14 gestrichen

Abschnitt IV: Einstufung und Befristung

- § 15 Einstufung
- § 16 Befristung
- § 17 Verlängerung der Einstufungsfrist
- § 18 Änderung der Einstufung
- § 19 Aufhebung der Einstufung

Abschnitt V: Handhabung von Verschlusssachen

- § 20 Herstellung und Kennzeichnung
- § 21 Verwaltung und Nachweis von Verschlusssachen
- § 22 Vervielfältigung von Verschlusssachen
- § 23 Aufbewahrung von Verschlusssachen
- § 24 Grundsätze zur Weitergabe von Verschlusssachen
- § 25 Weitergabe an nichtöffentliche Stellen
- § 26 Weitergabe an den Deutschen Bundestag, den Bundesrat, Landesparlamente und -behörden
- § 27 Empfang von Verschlusssachen
- § 28 Mitnahme von Verschlusssachen außerhalb des Dienstgebäudes
- § 29 Erörterung von Verschlusssachen
- § 30 Grundsätze der Aussonderung von Verschlusssachen
- § 31 Archivierung von Verschlusssachen
- § 32 Vernichtung von Verschlusssachen
- § 33 VS-Zwischenmaterial

Abschnitt VI: Zusammenarbeit mit nichtdeutschen Stellen und nichtöffentlichen Stellen mit Sitz im Ausland

- § 34 Weitergabe von deutschen Verschlusssachen an nichtdeutsche Stellen und nichtöffentliche Stellen mit Sitz im Ausland
- § 35 Empfang und Handhabung nichtdeutscher Verschlusssachen
- § 36 Sicherheitsakkreditierung
- § 37 Zentralregistraturen

Abschnitt VII: Materielle und technische Maßnahmen

- § 38 Planung und Durchführung
- § 39 Räumliche Sicherheitsmaßnahmen
- § 40 Technische Sicherung von Verschlusssachen
- § 41 Abhörschutzmaßnahmen
- § 42 Besondere Dienststellen
- § 43 VS-Registraturen
- § 44 VS-Verwahrgeleise
- § 45 VS-IT-Räume und -Bereiche
- § 46 Zutritts- und Zugangsmittel
- § 47 Abnahmen und Wiederholungsprüfungen
- § 48 Lauschabwehrprüfungen

Abschnitt VIII: Einsatz von Informationstechnik

- § 49 Allgemeine Grundsätze
- § 50 Freigabe des Betriebs von VS-IT
- § 51 Zulassung
- § 52 IT-Sicherheitsfunktionen
- § 53 Schutz von VS-Übertragungseinrichtungen, -leitungen und -verteiltern
- § 54 Handhabung von Datenträgern und IT-Produkten für unverschlüsselte Verschlusssachen

- § 55 Übertragung von Verschlusssachen über technische Kommunikationsverbindungen
- § 56 Vernichtung und Aussonderung von Datenträgern und registrierten IT-Produkten
- § 57 Abstrahlenschutzmaßnahmen
- § 58 Zusammenschaltung von VS-IT

Abschnitt IX: Kryptopersonal und Handhabung von Kryptomitteln

- § 59 Kryptomittel
- § 60 Nationale Verteilerstellen für Kryptomittel
- § 61 Kryptoverwaltung
- § 62 Kryptopersonal

Abschnitt X: Aufrechterhaltung des Geheimschutzes

- § 63 Kontrollen
- § 64 Behandlung von Geheimschutzvorkommnissen
- § 65 Verhalten in außergewöhnlichen Gefahrenlagen

Abschnitt XI: Abschließende Regelungen

- § 66 Schlussbestimmungen
- § 67 Inkrafttreten

Verzeichnis der Anlagen

Abschnitt I: Allgemeine Bestimmungen

§ 1 Anwendungsbereich

- (1) Die Verschlusssachenanweisung richtet sich an Bundesbehörden und bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit Verschlusssachen arbeiten, sowie an dort tätige Personen, die Zugang zu Verschlusssachen haben oder eine Tätigkeit ausüben, bei der sie sich Zugang zu Verschlusssachen verschaffen können. Dienststellen wenden in der Zusammenarbeit mit dem Deutschen Bundestag und dem Bundesrat ausschließlich diese Verschlusssachenanweisung an.
- (2) Die allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz bei den Nachrichtendiensten des Bundes erlässt die jeweils zuständige oberste Bundesbehörde im Einvernehmen mit dem Bundesministerium des Innern und für Heimat.
- (3) Die allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz im nichtöffentlichen Bereich erlässt das Bundesministerium für Wirtschaft und Klimaschutz im Einvernehmen mit dem Bundesministerium des Innern und für Heimat.
- (4) Die allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz im Geschäftsbereich des Bundesministeriums der Verteidigung erlässt das Bundesministerium der Verteidigung als militärische Sicherheitsbehörde im Einvernehmen mit dem Bundesministerium des Innern und für Heimat.

§ 2 Begriff der Verschlusssache und Geheimhaltungsgrade

- (1) Verschlusssachen sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform (zum Beispiel Schriftstücke, Zeichnungen, Karten, Fotokopien, Lichtbildmaterial, elektronische Dateien und Datenträger, elektrische Signale, Geräte, technische Einrichtungen oder das gesprochene Wort). Geheimhaltungsbedürftig im öffentlichen Interesse können auch Geschäfts-, Betriebs-, Erfindungs-, Steuer- oder sonstige private Geheimnisse oder Umstände des persönlichen Lebensbereichs sein.
- (2) Verschlusssachen werden entsprechend ihrer Schutzbedürftigkeit von einer Dienststelle oder auf deren Veranlassung nach § 4 Absatz 2 Sicherheitsüberprüfungsgesetz in folgende Geheimhaltungsgrade eingestuft:
 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.
- (3) Der Geheimhaltungsgrad einer Verschlussache bleibt auch bestehen, wenn sie unrechtmäßig bekannt geworden ist.

§ 3 Allgemeine Grundsätze

- (1) Von einer Verschlussache dürfen nur Personen Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen. Keine Person darf über eine Verschlussache umfassender oder eher unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist. Es gilt der Grundsatz „Kenntnis nur, wenn nötig“.
- (2) Eine Person, die Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlussachen erhalten soll oder ihn sich verschaffen kann, ist zuvor einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz zu unterziehen, es sei denn, sie hat Zugang zu Verschlussachen kraft Amtes nach § 2 Absatz 3 Satz 1 Nummer 1 oder 2 Sicherheitsüberprüfungsgesetz.
- (3) Jeder, dem eine Verschlussache anvertraut oder zugänglich gemacht worden ist, trägt ohne Rücksicht darauf, wie die Verschlussache zu seiner Kenntnis oder in seinen Besitz gelangt ist, die persönliche Verantwortung für ihre vorschriftsmäßige Behandlung.

§ 4 Verpflichtung, Ermächtigung und Zulassung

- (1) Bevor eine Person Zugang zu Verschlussachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH erhält, ist sie auf Anlage V zu verpflichten. Dabei ist ihr gegen Empfangsbestätigung ein Exemplar der Anlage V zugänglich zu machen.
- (2) Bevor eine Person Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlussachen erhält, ist sie durch den Geheimschutzbeauftragten zu ermächtigen. Dabei ist sie über die besonderen Bestimmungen des Geheimschutzes zu belehren, in erforderlichem Umfang auf den Geheimschutz zu verpflichten und über Anbahnungs- und Anwerbemethoden ausländischer Nachrichtendienste sowie die Möglichkeit straf- und disziplinarrechtlicher Ahndung oder arbeitsrechtlicher Maßnahmen bei Verstößen gegen die Geheimhaltungsvorschriften zu unterrichten. Die Belehrung und Unterrichtung soll spätestens nach fünf Jahren erneut erfolgen.
- (3) Bevor einer Person, die nicht nach Absatz 2 ermächtigt ist, eine Tätigkeit übertragen wird, bei der sie sich Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlussachen verschaffen kann, ist sie durch den Geheimschutzbeauftragten hierfür zuzulassen. Dabei ist sie über die besonderen Bestimmungen des Geheimschutzes zu belehren, in erforderlichem Umfang auf den Geheimschutz zu verpflichten und über Anbahnungs- und Anwerbemethoden ausländischer Nachrichtendienste sowie die Möglichkeit straf- und disziplinarrechtlicher Ahndung oder arbeitsrechtlicher Maßnahmen bei Verstößen gegen

die Geheimhaltungsvorschriften zu unterrichten. Die Belehrung und Unterrichtung soll spätestens nach fünf Jahren erneut erfolgen. Personen, die sich Zugang zu Verschlusssachen verschaffen können, können insbesondere Personen sein, die

1. als Boten oder Kuriere Verschlusssachen befördern (VS-Bote / VS-Kurier),
 2. VS-Verwahrgelasse oder Sicherheitsbereiche bewachen,
 3. Einbruch- oder Überfallmeldeanlagen zum Schutze von Verschlusssachen installieren, warten oder instandsetzen,
 4. Schlüssel oder Zahlenkombinationen zu VS-Verwahrgelassen, VS-Schlüssel-behältern, Einbruch- oder Überfallmeldeanlagen zum Schutze von Verschlusssachen verwalten,
 5. als IT-Wartungspersonal oder Administratoren von VS-IT eingesetzt sind.
- (4) Ermächtigten und zugelassenen Personen sind gegen Empfangsbestätigung die einschlägigen Strafvorschriften und die für ihre Tätigkeit erforderlichen Vorschriften zum Schutz von Verschlusssachen zugänglich zu machen und gegebenenfalls ein VS-Quittungsbuch auszuhändigen. Ermächtigungen, Zulassungen und ihre Befristung sind nach Muster der Anlage VIII zu dokumentieren.
- (5) Ermächtigten Personen ist bei Bedarf eine Konferenzbescheinigung nach Muster der Anlage VIII über ihre Ermächtigung auszustellen.
- (6) Entfällt die dienstliche Notwendigkeit für eine Ermächtigung oder Zulassung, ist diese aufzuheben oder auf den notwendigen Umfang einzuschränken. Ermächtigungen und Zulassungen sind aufzuheben, wenn ein Sicherheitsrisiko festgestellt wird. Ermächtigungen und Zulassungen erlöschen spätestens bei Ausscheiden der betroffenen Person aus der Dienststelle. Die VS-Registatur ist über Ermächtigungen und Zulassungen sowie deren Erweiterung, Einschränkung, Aufhebung oder Erlöschen zu unterrichten.
- (7) Personen, deren Ermächtigung oder Zulassung aufgehoben wird oder erlischt, sind verpflichtet, Verschlusssachen, die sich in ihrem Besitz befinden, und gegebenenfalls das VS-Quittungsbuch unaufgefordert abzugeben und darüber eine Erklärung nach Muster der Anlage VIII zu unterschreiben. Dies gilt im Falle der Einschränkung der Ermächtigung oder Zulassung entsprechend.
- (8) Bei Einschränkung, Aufhebung oder Erlöschen der Ermächtigung oder Zulassung ist die betroffene Person auf das Fortbestehen der Geheimschutzpflichten hinzuweisen.

§ 5 Mitwirkende Behörden

- (1) Das Bundesamt für Sicherheit in der Informationstechnik
 1. gibt zur Umsetzung dieser Verschlusssachenanweisung Technische Leitlinien heraus, die der Zustimmung des Bundesministeriums des Innern und für Heimat bedürfen, in ihrer jeweils gültigen Fassung zu beachten sind und von denen nur im Ausnahmefall

im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik abgewichen werden kann,

2. berät bei der Umsetzung dieser Verschlusssachenanweisung und der Technischen Leitlinien nach Nummer 1,
 3. führt technische Prüfungen sowie Fortbildungen durch,
 4. macht in Abstimmung mit dem Bundesministerium des Innern und für Heimat Vorgaben, welche technischen Mittel und Dienstleister vor dem Einsatz einer Eignungsprüfung zu unterziehen sind, und stellt Eignungsfeststellungen nach einem vom Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen mit dem Bundesministerium des Innern und für Heimat festgelegten Verfahren aus,
 5. erteilt Zulassungen für IT-Sicherheitsprodukte nach einem vom Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen mit dem Bundesministerium des Innern und für Heimat festgelegten Verfahren,
 6. berät bei der Auswahl von VS-IT und technischen Komponenten, sofern keine zugelassenen IT-Sicherheitsprodukte nach Nummer 5 verfügbar sind und
 7. unterrichtet unverzüglich alle Dienststellen über Erkenntnisse, die für den Schutz von dort befindlichen Verschlusssachen oder die Aufrechterhaltung des dortigen Geheimschutzes von Bedeutung sein können.
- (2) Das Bundesamt für Sicherheit in der Informationstechnik kann zu seiner Aufgabenerfüllung andere Stellen einbeziehen. Die Einbeziehung privater Stellen bedarf der vorherigen Billigung des Bundesministeriums des Innern. Bei Einbeziehung öffentlicher Stellen ist das Bundesministerium des Innern und für Heimat über die Einbeziehung unverzüglich zu informieren. Die Verantwortung des Bundesamtes für Sicherheit in der Informationstechnik für die ordnungsgemäße Aufgabenerfüllung bleibt von der Einbeziehung unberührt.
- (3) Das Bundesamt für Verfassungsschutz, das Bundesamt für den Militärischen Abschirmdienst und der Bundesnachrichtendienst teilen dem Bundesamt für Sicherheit in der Informationstechnik nichtpersonenbezogene Erkenntnisse, die für den Schutz von Verschlusssachen oder die Aufrechterhaltung des Geheimschutzes von Bedeutung sein können, unverzüglich mit. Das gilt nicht, soweit die Erkenntnisse einem Weitergabeverbot unterliegen. § 23 des Bundesverfassungsschutzgesetzes gilt entsprechend. Sofern sich die Erkenntnisse auf den Geheimschutz in der Wirtschaft beziehen, ist auch das Bundesministerium für Wirtschaft und Klimaschutz unverzüglich zu informieren.

§ 6 Mehrschichtige Sicherheit

Bei der Handhabung von Verschlusssachen werden technische und organisatorische Maßnahmen getroffen, die in ihrem Zusammenwirken die Risiken eines Angriffs reduzieren und im Falle eines erfolgreichen Angriffs die negativen Folgen begrenzen sollen. Die Sicherheitsmaßnahmen berücksichtigen die Aspekte Prävention, Detektion und Reaktion.

Abschnitt II: Geheimschutzorganisation und Geheimschutzdokumentation

§ 7 Dienststellenleitung

Die Dienststellenleitung ist innerhalb ihres Zuständigkeitsbereiches für die Umsetzung dieser Verschlussanweisung verantwortlich und hat die Voraussetzungen zur Gewährleistung des materiellen Geheimschutzes zu schaffen. Sie kann ihre Aufgaben ganz oder teilweise auf Mitarbeiter ihrer Dienststelle übertragen.

§ 8 Geheimschutzbeauftragte

- (1) Dienststellen, die VS-VERTRAULICH oder höher eingestufte Verschlussanweisungen handhaben, sollen Geheimschutzbeauftragte und zur Vertretung berechnigte Personen bestellen. Andernfalls nehmen die Dienststellenleitungen die Aufgaben der Geheimschutzbeauftragten wahr.
- (2) Dienststellen, die ausschließlich VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlussanweisungen handhaben, können Geheimschutzbeauftragte und zur Vertretung berechnigte Personen bestellen. Andernfalls nehmen die Dienststellenleitungen die Aufgaben der Geheimschutzbeauftragten wahr.
- (3) Geheimschutzbeauftragte sorgen für die Umsetzung dieser Verschlussanweisung und beraten die Dienststellenleitungen in allen Fragen des Geheimschutzes. Geheimschutzbeauftragte haben ein unmittelbares Vortragsrecht bei den Dienststellenleitungen. Geheimschutzbeauftragte sind bei allen geheimschutzrelevanten Maßnahmen zu beteiligen. Innerhalb der Dienststellen können besonders beauftragte Mitarbeiter (zum Beispiel Geheimschutzbeamte) zur Unterstützung der Geheimschutzbeauftragten bestellt werden.
- (4) Geheimschutzbeauftragte oder besonders beauftragte Mitarbeiter haben die mit der Handhabung von Verschlussanweisungen betrauten Personen durch geeignete Maßnahmen mit den Vorschriften dieser Verschlussanweisung sowie anderen einschlägigen Vorschriften zum Schutz von Verschlussanweisungen vertraut zu machen.

§ 8a Risikomanagement

Geheimschutzbeauftragte tragen durch angemessene Sicherheitsmaßnahmen dafür Sorge, Risiken für den Schutz von Verschlussanweisungen zu reduzieren und Restrisiken zu identifizieren, die mit den getroffenen Maßnahmen nicht abgewehrt werden können. Ein solches Risikomanagement wird als fortlaufender Prozess verstanden, in dem Planung, Umsetzung, Überwachung und Verbesserung von angemessenen Sicherheitsmaßnahmen kontinuierlich stattfinden. Eine Sicherheitsmaßnahme ist angemessen, wenn der Aufwand zur Umsetzung der Maßnahme und das verbleibende Restrisiko in einem ausgewogenen Verhältnis stehen. Die Bewertung der Angemessenheit erfolgt auf der Grundlage einer Risikoanalyse.

§ 9 IT-Sicherheitsbeauftragte

IT-Sicherheitsbeauftragte unterstützen und beraten die Geheimschutzbeauftragten in allen Fragen des Einsatzes von Informationstechnik zur Handhabung von Verschlusssachen einschließlich deren Übertragung (VS-IT).

§ 10 VS-Registatoren

Dienststellen, die VS-VERTRAULICH oder höher eingestufte Verschlusssachen handhaben, bestellen VS-Registatoren und zur Vertretung berechnigte Personen, die im Rahmen der Verschlusssachenanweisung für die ordnungsgemäße Verwaltung dieser Verschlusssachen Sorge tragen.

§ 11 Qualifikation

Die in §§ 8 bis 10 genannten Personen müssen über die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde verfügen.

§ 12 Erstellung der Geheimschutzdokumentation

- (1) Jede Dienststelle, die nicht nur gelegentlich mit Verschlusssachen arbeitet, führt eine Geheimschutzdokumentation, die
 1. Verweise auf alle in diesem Zusammenhang zu beachtenden Vorschriften,
 2. eine Auflistung der Dienstposten, auf denen eine sicherheitsempfindliche Tätigkeit im Sinne des Sicherheitsüberprüfungsgesetzes ausgeübt wird,
 3. eine Auflistung der ermächtigten und zugelassenen Personen,
 4. die VS-Sicherungsdokumentation mit den sich aus Anlage II ergebenden Inhalten,
 5. die VS-IT-Dokumentation, mit den sich aus Anlage II ergebenden Inhalten,
 6. Nachweise über durchgeführte Kontrollen und Überprüfungen und
 7. Berichte über Geheimschutzvorkommnisseumfasst.
- (2) Die Geheimschutzdokumentation ist bei allen geheimschutzrelevanten Änderungen zu aktualisieren, mindestens aber alle drei Jahre auf Aktualität, Vollständigkeit und Erforderlichkeit bestehender und noch zu treffender Geheimschutzmaßnahmen zu überprüfen.
- (3) Die Geheimschutzbeauftragten geben den Mitarbeitern ihrer Dienststelle die für die Dienststelle getroffenen, für die Handhabung von Verschlusssachen relevanten Regelungen in geeigneter Weise bekannt.

Weiteres zu diesem Abschnitt ist den Anlagen I und II zu entnehmen.

Abschnitt III (aufgelöst)

§§ 13, 14 (weggefallen)

Abschnitt IV: Einstufung und Befristung

§ 15 Einstufung

- (1) Die Dienststelle, die eine Verschlussache erstellt oder deren Erstellung veranlasst, oder der Rechtsnachfolger dieser Dienststelle ist der Herausgeber der Verschlussache. Der Herausgeber legt nach Maßgabe von § 4 Absatz 2 Sicherheitsüberprüfungsgesetz den Geheimhaltungsgrad der Verschlussache fest. Von einer Einstufung als Verschlussache ist nur Gebrauch zu machen, soweit dies notwendig ist.
- (2) Die Dienststelle kann Richtlinien zur Einstufung von Verschlussachen für häufiger vorkommende Fälle festlegen.
- (3) Weiteres ist der Anlage III zu entnehmen.

§ 16 Einstufungsfrist

- (1) Die Einstufung einer Verschlussache des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH ist auf 30 Jahre befristet. Der Herausgeber kann unter Berücksichtigung der Begründung für die Einstufung eine kürzere Einstufungsfrist bestimmen.
- (2) Der Herausgeber hat für VS-VERTRAULICH oder höher eingestufte Verschlussachen den Zeitpunkt des Ablaufs der Einstufung zu bestimmen. Die Einstufungsfrist hat sich hierbei an der aus der Begründung für die Einstufung resultierenden voraussichtlichen Dauer der Schutzbedürftigkeit der Verschlussache zu orientieren. Die Einstufungsfrist soll 30 Jahre nicht überschreiten. Soweit die Begründung für die Einstufung eine Einstufungsfrist einzelner Verschlussachen oder pauschal für die in einem bestimmten Bereich entstehenden Verschlussachen über einen Zeitraum von 30 Jahren hinaus gebietet, ist dies zu begründen und so zu vermerken, dass dies jederzeit erkennbar ist. Eine solche Abweichung bedarf der Zustimmung der zuständigen obersten Bundesbehörde.
- (3) Die Einstufung endet mit Ablauf des Jahres, in welches das Fristende fällt.
- (4) Die Dienststelle kann Richtlinien zur Bestimmung der Einstufungsfrist von Verschlussachen für häufiger vorkommende Fälle festlegen.

§ 17 Verlängerung der Einstufungsfrist

- (1) Die nach § 16 Absatz 1 festgelegte Einstufungsfrist von Verschlussachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH kann nicht verlängert werden.

- (2) Soweit die Schutzbedürftigkeit einer Verschlussache des Geheimhaltungsgrades VS-VERTRAULICH oder höher nach den Vorschriften des Sicherheitsüberprüfungsgesetzes über die nach § 16 Absatz 2 festgelegte Einstufungsfrist hinaus fortbesteht, hat der Herausgeber eine Verlängerung der Einstufungsfrist für einzelne Verschlussachen oder pauschal für die in einem bestimmten Bereich entstandenen Verschlussachen zu verfügen. Die Verlängerung ist zu begründen und so zu vermerken, dass diese und die verfügende Stelle jederzeit erkennbar sind. Die Verlängerung soll jeweils 30 Jahre nicht überschreiten. Soweit die Begründung für die Einstufung die Verlängerung der Einstufungsfrist einzelner Verschlussachen oder pauschal für die in einem bestimmten Bereich entstandenen Verschlussachen über einen Zeitraum von 30 Jahren hinaus gebietet, ist dies zu begründen und so zu vermerken, dass dies und die verfügende Stelle jederzeit erkennbar sind. Eine solche Abweichung bedarf der Zustimmung der zuständigen obersten Bundesbehörde.
- (3) Das Bundesarchiv betreibt eine Nachweisdatenbank für Verschlussachen, deren Einstufungsfristen verlängert wurden. Grundsätzlich ist jedem Empfänger von Verschlussachen des Bundes lesender Zugriff auf diese Datenbank zu gewähren. Die Verlängerung der Einstufungsfrist ist dem Bundesarchiv rechtzeitig vor Fristablauf zur Erfassung in der Nachweisdatenbank mitzuteilen. Die Empfänger von Verschlussachen, deren Einstufungsfrist abgelaufen ist, haben dort zu prüfen, ob die Einstufungsfrist verlängert wurde. Verschlussachen, die nicht in der Nachweisdatenbank erfasst sind, sind nach Ablauf der Einstufungsfrist offenes Schriftgut.
- (4) Nichtöffentliche Empfänger amtlich geheim gehaltener Verschlussachen sind von dem Verfahren nach Absatz 3 Satz 2 bis 5 ausgenommen. Sie sind als Empfänger von Verschlussachen schriftlich über die Verlängerungen von Einstufungsfristen zu benachrichtigen. Die Benachrichtigungen sind nachzuweisen.
- (5) Absatz 3 gilt nicht für die Verlängerung der Einstufungsfrist von auf amtliche Veranlassung geheim gehaltenen Verschlussachen, für die eine Einstufungsfrist bestimmt ist. Über die Verlängerungen der Einstufungsfristen dieser Verschlussachen hat der Herausgeber alle Empfänger schriftlich zu benachrichtigen. Die Benachrichtigungen sind nachzuweisen.

§ 18 Änderung der Einstufung

- (1) Ändert sich die Schutzbedürftigkeit einer Verschlussache, hat der Herausgeber den Geheimhaltungsgrad dieser Verschlussache entsprechend herauf- oder herabzusetzen. Über die Änderung hat der Herausgeber alle Empfänger der Verschlussache unverzüglich schriftlich zu benachrichtigen.
- (2) Eine nachträgliche Einstufung von nicht eingestuften Informationen sowie eine Heraufstufung von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlussachen ist grundsätzlich nicht zulässig. Ausnahmen sind nur im Benehmen mit den Geheimschutzbeauftragten zulässig.
- (3) Die Änderung des Geheimhaltungsgrades lässt die Einstufungsfrist nach § 16 unberührt.

- (4) Die Änderung des Geheimhaltungsgrades einer Verschlussache ist so zu vermerken, dass die Änderung bei der Handhabung der Verschlussache jederzeit erkennbar ist. Sind Verschlussachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher betroffen, ist die Änderung im VS-Bestandsverzeichnis des Herausgebers und der Empfänger nachzuweisen.

§ 19 Aufhebung der Einstufung

- (1) Entfällt die Geheimhaltungsbedürftigkeit einer Verschlussache vor Ablauf der Einstufungsfrist, hat der Herausgeber die Einstufung aufzuheben. Die Aufhebung der Einstufung ist so zu vermerken, dass diese und die verfügende Stelle jederzeit erkennbar sind. Im Falle von Verschlussachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher hat der Herausgeber alle Empfänger der Verschlussache oder deren Rechtsnachfolger schriftlich zu benachrichtigen. Die Aufhebung der Einstufung ist in diesem Falle zusätzlich im VS-Bestandsverzeichnis des Herausgebers und der Empfänger nachzuweisen.
- (2) Einstufungen sind aufgehoben, sofern auf der Verschlussache keine längere oder kürzere Frist bestimmt ist (vergleiche §§ 16 und 17)
1. für die Vorgänge der Jahre 1949 bis 1959 mit Ablauf des 31. Dezember 2012,
 2. für die Vorgänge der Jahre 1960 bis 1994 bis zum 1. Januar 2025 - dabei sind beginnend mit dem Ablauf des Jahres 2013 mindestens drei Jahrgänge je Kalenderjahr in chronologischer Reihenfolge auf Offenlegung zu prüfen,
 3. für die Vorgänge der Jahre ab 1995 nach 30 Jahren.

Für Empfänger von Verschlussachen, die nach § 17 Absatz 3 in der VS-Nachweisdatenbank zu prüfen haben, ob es sich bei diesen um offenes Schriftgut handelt, ersetzt diese Prüfung Benachrichtigungen nach Absatz 1 Satz 3.

Für nichtöffentliche Empfänger amtlich geheim gehaltener Verschlussachen, die nach § 17 Absatz 4 als Empfänger von Verschlussachen schriftlich über die Verlängerung der Fristen nach Satz 1 zu benachrichtigen sind, entfallen Benachrichtigungen nach Absatz 1 Satz 3.

- (3) Ausgenommen von der Fristenregelung nach Absatz 2 sind auf amtliche Veranlassung geheim gehaltene Verschlussachen.

Abschnitt V: Handhabung von Verschlussachen

§ 20 Herstellung und Kennzeichnung

- (1) Die Herstellung von VS-VERTRAULICH oder höher eingestuftem Verschlussachen ist nur an den hierfür bestimmten Stellen mit den dort vorgesehenen Mitteln zulässig.
- (2) Bei der Herstellung ist eine Verschlussache so zu kennzeichnen, dass bei ihrer Handhabung während der gesamten Dauer ihrer Einstufung jederzeit erkennbar sind:

1. der Geheimhaltungsgrad,
 2. der Herausgeber,
 3. das Datum der Verschlussache,
 4. bei VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlussachen das bei der Herstellung festgelegte Ende der Einstufungsfrist, sofern dieses die Regelfrist von 30 Jahren nach § 16 Absatz 1 unterschreitet,
 5. bei VS-VERTRAULICH oder höher eingestuften Verschlussachen das bei der Herstellung festgelegte Ende der Einstufungsfrist mit dem Zusatz „Die Einstufung endet mit Ablauf des Jahres...“,
 6. bei VS-VERTRAULICH oder höher eingestuften Verschlussachen ein geeignetes individuelles Merkmal (zum Beispiel Geschäftszeichen und Tagebuchnummer), ergänzt um das Kürzel des Geheimhaltungsgrades nach Absatz 4, anhand dessen sich in Verbindung mit dem VS-Bestandsverzeichnis die Handhabung der Verschlussache jederzeit lückenlos ermitteln lässt,
 7. bei jeder Ausfertigung einer als VS-VERTRAULICH oder höher eingestuften Verschlussache eine fortlaufende Nummer und der jeweilige Empfänger und
 8. die Seiten- und Gesamtseitenzahl.
- (3) Der Herausgeber kann weitere Vorgaben zum Schutz und zur Handhabung von Verschlussachen durch Warn- und Sperrvermerke nach Anlage IV festlegen.
- (4) Geheimhaltungsgrade sind auszuschreiben, soweit in dieser Vorschrift nichts anderes bestimmt ist oder die Beschaffenheit einer Verschlussache das nicht zulässt. In diesen Fällen sind folgende Abkürzungen zu verwenden:
- | | |
|-------------------------------|-----------|
| VS-NUR FÜR DEN DIENSTGEBRAUCH | VS-NfD |
| VS-VERTRAULICH | VS-Vertr. |
| GEHEIM | Geh. |
| STRENG GEHEIM | Str. Geh. |
- (5) Der Betreff einer Verschlussache soll so formuliert werden, dass er für sich genommen nicht geheimhaltungsbedürftig ist.
- (6) Besteht eine Verschlussache aus mehreren, unterschiedlich eingestuften Teilen (zum Beispiel Anlagen oder Komponenten), sind alle Teile mit ihrem jeweiligen Geheimhaltungsgrad und die Verschlussache in ihrer Gesamtheit nach dem höchsten Geheimhaltungsgrad zu kennzeichnen. Anfang und Ende der einzelnen Teile müssen erkennbar

sein.

- (7) Datenträger, auf denen Verschlusssachen unverschlüsselt gespeichert sind, sind mit dem Geheimhaltungsgrad der höchsten Einstufung der darauf gespeicherten Verschlusssachen zu kennzeichnen. Datenträger, auf denen Verschlusssachen ausschließlich vorschriftsgemäß verschlüsselt gespeichert sind, müssen nicht gekennzeichnet werden.
- (8) Die verbindliche Gestaltung der Kennzeichnung von Verschlusssachen, VS-Bestandsverzeichnissen sowie VS-Schriftgutbehältern und Behältern von VS-Datenträgern ist der Anlage IV sowie den Mustern der Anlage VIII zu entnehmen. Die Kennzeichnung gilt auch für elektronische Verschlusssachen. Von der Kennzeichnung sind VS-Transportbehälter ausgenommen. Lässt die Beschaffenheit einer Verschlusssache eine solche Kennzeichnung nicht zu, ist sinngemäß zu verfahren. Näheres zur zusätzlichen Kennzeichnung von elektronischen Verschlusssachen (zum Beispiel anhand von Metadaten) regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 21 Verwaltung und Nachweis von Verschlusssachen

- (1) VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen können, soweit sie nicht Bestandteil höher eingestufte Verschlusssachen sind, unter Beachtung des Grundsatzes „Kenntnis nur, wenn nötig“ in offenen Registraturen verwaltet werden.
- (2) VS-VERTRAULICH oder höher eingestufte Verschlusssachen sind in VS-Registraturen mittels geeigneter Verfahren so zu verwalten, dass ihre Existenz, ihre Einstufung einschließlich der Einstufungsfrist, ihr Verbleib, die Kenntnisnahmen, ihre Vervielfältigung und deren Verbleib sowie ihre Vernichtung nachvollziehbar sind (Nachweisführung). Für Verschlusssachen ausländischer Staaten und über- oder zwischenstaatlicher Organisationen können andere Regelungen nach Anlage VII dieser Verschlusssachenanweisung gelten.
- (3) Die Nachweisführung von VS-VERTRAULICH oder höher eingestufte Verschlusssachen kann in Papier- oder in elektronischer Form erfolgen. Sie muss Schutz vor unbemerkter Veränderung, Verlust und Verfälschung bieten. Die papiergestützte Nachweisführung von Verschlusssachen erfolgt anhand von VS-Bestandsverzeichnissen, VS-Quittungsbüchern, VS-Begleitzetteln, VS-Empfangsscheinen, VS-Übergabeprotokollen und VS-Vernichtungsprotokollen. Verbindliche Muster für diese Nachweise sind der Anlage VIII zu entnehmen. Die elektronische Nachweisführung von Verschlusssachen erfolgt anhand von VS-Registratursystemen. Diese unterliegen als VS-IT im Sinne des Abschnitts VIII den dortigen Bestimmungen.
- (4) VS-Datenträger, ihr Verbleib und ihre Vernichtung sind in einem gesonderten VS-Bestandsverzeichnis nachzuweisen. Für die eindeutige Identifizierbarkeit genügt die Angabe eines Ordnungskriteriums (zum Beispiel laufende Nummer).
- (5) VS-Bestandsverzeichnisse sind gemäß dem höchsten Geheimhaltungsgrad der in ihnen nachgewiesenen Verschlusssachen einzustufen. Der Zugriff auf das VS-Bestandsverzeichnis ist nur den Geheimschutzbeauftragten, den besonders beauftragten Mitarbeitern und den VS-Registratoren gestattet.

- (6) Bei Wechsel eines VS-Registrators ist der Bestand zu überprüfen und ein Bestandsbericht (Übergabeprotokoll) zu fertigen.
- (7) VS-Nachweise sind mindestens fünf Jahre aufzubewahren. Für VS-Quittungsbücher beginnt die Frist mit der letzten Eintragung, für VS-Empfangsscheine, VS-Begleitzettel, VS-Übergabeprotokolle und VS-Vernichtungsprotokolle mit der Ausstellung. Für VS-Bestandsverzeichnisse beginnt die Frist, wenn alle in ihnen nachgewiesenen Verschlussachen
1. auf den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH herabgestuft,
 2. offengelegt (Aufhebung der Einstufung) oder
 3. vernichtet
- worden sind.

Wenn in einem VS-Bestandsverzeichnis nur noch wenige Verschlussachen nachgewiesen werden, können die Einträge unter Beibehaltung ihrer Tagebuchnummer in ein anderes VS-Bestandsverzeichnis übertragen werden und sind nur dort nachzuweisen. In diesem Fall beginnt die Aufbewahrungsfrist für das abgeschlossene VS-Bestandsverzeichnis mit der Übertragung der Einträge. Nach Ablauf der Frist sind VS-Nachweise zu vernichten.

- (8) Weiteres ist der Anlage IV zu entnehmen.

§ 22 Vervielfältigung von Verschlussachen

- (1) Vervielfältigung von Verschlussachen ist die absichtliche Herstellung von weiteren Exemplaren einer Ausfertigung einer Verschlussache, unabhängig von der Darstellungsform (insbesondere durch fotomechanische Kopie, Scan, Abdruck einer elektronisch dargestellten Verschlussache, elektronische Kopie von Dateien, elektronischer Versand, Auszug und Nachbau).
- (2) Jede Vervielfältigung von VS-VERTRAULICH oder höher eingestuften Verschlussachen ist mit einer fortlaufenden Nummer und dem jeweiligen Empfänger so zu kennzeichnen, dass sie als weiteres Exemplar einer Verschlussache (Kopie) eindeutig erkennbar ist und der Original-Verschlussache zugeordnet werden kann. Jede Vervielfältigung von VS-VERTRAULICH oder höher eingestuften Verschlussachen ist als weiteres Exemplar zudem nach § 21 unverzüglich zu registrieren.
- (3) In Dienststellen, in denen VS-VERTRAULICH oder höher eingestufte Verschlussachen hergestellt oder vervielfältigt werden, sollen hierfür bestimmte Stellen mit ermächtigtem Bedienungspersonal festgelegt werden. Soweit dies nicht geschieht, sind Vervielfältigungen dieser Verschlussachen durch die VS-Registatoren zu fertigen.

- (4) Die Vervielfältigung von STRENG GEHEIM eingestuften Verschlusssachen bedarf zusätzlich der schriftlichen Zustimmung des Herausgebers. Die Zustimmung ist im VS-Bestandsverzeichnis zu vermerken.
- (5) Werden in VS-IT Kopien von den dort registrierten Verschlusssachen als Backup-Daten zur Sicherung der Verfügbarkeit benötigt, sind diese in einem gesonderten Bestandsverzeichnis in der Art nachzuweisen, dass jederzeit feststellbar ist, welche Verschlusssachen als Kopie darin gespeichert sind.

§ 23 Aufbewahrung von Verschlusssachen

- (1) Die dauerhafte Aufbewahrung von VS-VERTRAULICH oder höher eingestuften Verschlusssachen hat in VS-Registaturen zu erfolgen. Die Aufbewahrung außerhalb der VS-Registatur ist nur für den Zeitraum zulässig, für den ein fortgesetzter Zugriff des Bearbeiters auf die Verschlusssache notwendig ist. Die VS-Registatoren erkundigen sich in angemessenen Zeitabständen, ob diese Voraussetzung weiterbesteht. VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen können, soweit sie nicht Bestandteil höher eingestufte Verschlusssachen sind, unter Beachtung des Grundsatzes „Kenntnis nur, wenn nötig“ in einer offenen Registatur dauerhaft aufbewahrt werden.
- (2) VS-VERTRAULICH oder höher eingestufte Verschlusssachen sind bei Nichtgebrauch in einem VS-Verwahrgelass einzuschließen. Dies gilt für STRENG GEHEIM eingestufte Verschlusssachen bereits bei kurzer Abwesenheit der die Verschlusssache bearbeitenden oder verwaltenden Personen. VS-VERTRAULICH oder GEHEIM eingestufte Verschlusssachen können bei einer kurzen Abwesenheit der die Verschlusssache bearbeitenden oder verwaltenden Personen während der Arbeitszeit im VS-Arbeitsbereich verbleiben, sofern die Zimmertür mit einem Sicherheitsschloss verschlossen ist. VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen sind bei Nichtgebrauch in verschlossenen Behältern oder abgeschlossenen Räumen aufzubewahren.
- (3) Außerhalb der Arbeitszeit sind VS-Verwahrgelasse zu bewachen oder durch eine Alarmanlage technisch zu überwachen. In beiden Fällen ist sicherzustellen, dass Unbefugte am Zugriff auf die darin gelagerten Verschlusssachen gehindert werden und dass ein Zugriff Unbefugter erkannt und hilfeleistenden Stellen gemeldet wird. Bei GEHEIM oder VS-VERTRAULICH eingestuften Verschlusssachen kann eine Bewachung beziehungsweise technische Überwachung des VS-Verwahrgelasses unterbleiben, wenn das Gebäude oder der Gebäudeteil, in dem sich das Verwahrgelass befindet, bewacht oder technisch überwacht ist. Näheres über Art und Umfang der Bewachung und technischen Überwachung legen die Geheimschutzbeauftragten unter Berücksichtigung des Schutzziels für die jeweiligen VS-Verwahrgelasse und Gebäude fest.

§ 24 Grundsätze zur Weitergabe von Verschlusssachen

- (1) Weitergabe ist
 1. die Weitergabe von Hand zu Hand,
 2. die Beförderung durch Boten,

3. der Versand durch Kuriere,
 4. der Versand durch private Zustelldienste,
 5. die mündliche Mitteilung,
 6. die Übertragung über technische Kommunikationsverbindungen oder
 7. die Bereitstellung in einem Kommunikationsnetzwerk.
- (2) Jeder hat sich vor der Weitergabe von Verschlussachen zu vergewissern, dass der vorgesehene Empfänger zur Annahme oder Kenntnisnahme berechtigt ist.
- (3) Die Weitergabe von VS-VERTRAULICH oder höher eingestuften Verschlussachen soll über die VS-Registaturen erfolgen und ist nachzuweisen. Die Weitergabe von STRENG GEHEIM eingestuften Verschlussachen bedarf der schriftlichen Zustimmung des Herausgebers.
- (4) Zwischen zwei getrennt liegenden Gebäuden, die nicht zu einer geschlossenen Gebäudegruppe gehören, sollen Verschlussachen grundsätzlich mittels technischer Kommunikationsverbindungen nach § 55 übertragen werden. Ist dies nicht möglich, sollen sie durch Kuriere versandt werden. Ist auch dies nicht möglich können Verschlussachen bis zum Geheimhaltungsgrad GEHEIM durch private Zustelldienste versandt werden.
- (5) Die Geheimschutzbeauftragten können besondere Regelungen zur Weitergabe von Verschlussachen innerhalb einer Gemeinschaft von Geheimnisträgern festlegen.
- (6) Weiteres ist der Anlage IV zu entnehmen.

§ 25 Weitergabe an nichtöffentliche Stellen

Die Weitergabe von Verschlussachen an nichtöffentliche Stellen ist nur zulässig, wenn sie im staatlichen Interesse erforderlich ist (zum Beispiel zur Durchführung eines staatlichen Auftrages oder zur Analyse oder Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Kritischen Infrastrukturen, von sonstigen Unternehmen im staatlichen Interesse oder einer Stelle des Bundes). Für die Weitergabe von Verschlussachen an nichtöffentliche Stellen gilt unter Beachtung von § 1 Absatz 3 Folgendes:

1. Vor Weitergabe von VS-VERTRAULICH oder höher eingestuften Verschlussachen sind beim Bundesministerium für Wirtschaft und Klimaschutz Sicherheitsbescheide (Facility Security Clearance, FSC) über die beteiligten nichtöffentlichen Stellen anzufordern. Haben Beschäftigte dieser nichtöffentlichen Stellen ausschließlich in Dienststellen Zugang zu solchen Verschlussachen gilt dies nur, wenn die Zustimmung des Bundesministeriums für Wirtschaft und Klimaschutz nach § 24 Absatz 2 Sicherheitsüberprüfungsgesetz vorliegt.
2. Bei der Weitergabe von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlussachen ist Anlage V (VS-NfD-Merkblatt) zu beachten.

§ 26 Weitergabe an den Deutschen Bundestag, den Bundesrat, Landesparlamente und -behörden

- (1) Die Weitergabe von VS-VERTRAULICH oder höher eingestuften Verschlusssachen an den Deutschen Bundestag, den Bundesrat oder Landesparlamente erfolgt über die zuständige oberste Bundesbehörde grundsätzlich an die VS-Registatur des Empfängers.
- (2) Die Weitergabe von Verschlusssachen an ein Land sowie der Zugriff eines Landes auf VS-IT des Bundes und die Teilnahme eines Landes an einem VS-IT-System des Bundes sind nur zulässig, sofern in diesem Land Regelungen zum Schutz von Verschlusssachen entsprechend dieser Verschlusssachenanweisung gelten oder sich das Land zum Schutz von Verschlusssachen entsprechend dieser Verschlusssachenanweisung verpflichtet. Bei VS-IT-Systemen des Bundes ist vor der ersten Nutzung zudem eine Zusicherung des Landes an die für den Betrieb verantwortlichen Dienststelle des Bundes erforderlich, dass deren Anforderungen des Geheimschutzes erfüllt werden.

§ 27 Empfang von Verschlusssachen

- (1) Bei Empfang von Verschlusssachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher sind
 1. die Sendungen umgehend der VS-Registatur zuzuleiten und nach § 21 zu registrieren,
 2. die Integrität, Authentizität und Vollständigkeit der Sendungen zu prüfen und
 3. der Empfang mit dem Ergebnis der Prüfung gegenüber der VS-Verwaltung des Absenders unverzüglich zu bestätigen.
- (2) Zeigen sich Hinweise auf unbefugte Kenntnisnahme, Unvollständigkeit oder Veränderung, so sind die Geheimschutzbeauftragten und die Absender unverzüglich zu benachrichtigen.

§ 28 Mitnahme von Verschlusssachen außerhalb des Dienstgebäudes

- (1) Innerhalb des Bundesgebiets sollen VS-VERTRAULICH oder höher eingestufte Verschlusssachen grundsätzlich im Voraus an eine Dienststelle am Zielort, die selbst Verschlusssachen verwaltet und aufbewahrt, mittels technischer Kommunikationsverbindungen nach § 55 übertragen werden. Ist dies nicht möglich sind die folgenden Absätze bei der persönlichen Mitnahme zu beachten.
- (2) Verschlusssachen können außerhalb des Dienstgebäudes oder einer Liegenschaft nur auf Dienstreisen und zu Dienstbesprechungen mitgenommen werden, soweit dies dienstlich notwendig ist und sie angemessen gegen unbefugte Kenntnisnahme und unbefugten Zugriff gesichert werden. Die Mitnahme von VS-VERTRAULICH oder höher eingestuften Verschlusssachen aus anderem Anlass (zum Beispiel zur Bearbeitung in der Privatwohnung) ist unzulässig. In besonderen Fällen können die Geheimschutzbeauftragten Ausnahmen zulassen. Die Mitnahme von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen richtet sich nach Ziffer 7 der Anlage V.

- (3) Die Mitnahme von STRENG GEHEIM eingestuften Verschlussachen bedarf der vorherigen Zustimmung durch die Geheimschutzbeauftragten. Dies gilt ebenso bei der Mitnahme von VS-VERTRAULICH und GEHEIM eingestuften Verschlussachen in das Ausland.
- (4) VS-VERTRAULICH oder höher eingestufte Verschlussachen sind in einem äußerlich neutralen und verschlossenen VS-Transportbehälter mitzunehmen. An verdeckter Stelle ist die Anschrift der Dienststelle anzubringen. Werden STRENG GEHEIM oder GEHEIM eingestufte Verschlussachen mitgenommen, soll ein Dienstwagen genutzt werden. Ist dies nicht möglich, sind STRENG GEHEIM eingestufte Verschlussachen mit mindestens zwei ausreichend ermächtigten oder zugelassenen Personen zu befördern. Verschlussachen in elektronischer Form sind auf hierfür zugelassener VS-IT oder mit einem zugelassenen Verfahren verschlüsselten Datenträgern mitzunehmen.
- (5) Nach außerhalb des Bundesgebiets sind VS-VERTRAULICH oder höher eingestufte Verschlussachen nach Möglichkeit durch den Kurierdienst des Auswärtigen Amtes an die zuständige Auslandsvertretung voraus zu senden oder mittels technischer Kommunikationsverbindungen nach § 55 zu übertragen und nach Erledigung des Dienstgeschäftes auf demselben Weg zurückzusenden. Ist dies nicht möglich, so versiegelt das Auswärtige Amt beziehungsweise die zuständige Auslandsvertretung die verpackten Verschlussachen und stellt eine Bescheinigung aus, nach der ihr Inhaber zur Mitnahme des versiegelten Stückes als „Kuriergepäck“ berechtigt ist. Die persönliche Mitnahme von VS-VERTRAULICH oder GEHEIM eingestuften Verschlussachen ist ohne Mitwirkung des Auswärtigen Amtes gestattet, wenn sich diese in elektronischer Form auf hierfür zugelassener VS-IT oder mit einem zugelassenen Verfahren verschlüsselt auf einem Datenträger befinden. Die persönliche Mitnahme von STRENG GEHEIM eingestuften Verschlussachen im grenzüberschreitenden Verkehr ist unzulässig.
- (6) Bei Mitnahme von Verschlussachen sind diese ständig in persönlichem Gewahrsam zu halten oder nach § 23 aufzubewahren. Die Aufbewahrung in Hotelzimmern bei persönlicher Abwesenheit, Hotelsafes, Gepäckschließfächern oder in unbesetzten Fahrzeugen ist grundsätzlich unzulässig.

§ 29 Erörterung von Verschlussachen

- (1) Bei der Erörterung von geheimhaltungsbedürftigen Sachverhalten ist der Grundsatz „Kenntnis nur, wenn nötig“ zu beachten. Die Erörterung in der Öffentlichkeit ist zu unterlassen.
- (2) Sollen Verschlussachen in Dienstbesprechungen erörtert werden, so ist darauf bei der Einladung unter Angabe des Geheimhaltungsgrades hinzuweisen.
- (3) Die entsendenden Dienststellen gewährleisten, dass nur ausreichend ermächtigte Teilnehmer entsandt werden und stellen bei VS-VERTRAULICH oder höher eingestuften Verschlussachen über die Ermächtigung eine Konferenzbescheinigung nach Muster der Anlage VIII aus, soweit die einladende Stelle dies aus besonderen Gründen für erforderlich hält.

- (4) Vor Beginn der Dienstbesprechung hat der Leiter der Veranstaltung auf die Geheimhaltungsbedürftigkeit der Erörterungen hinzuweisen und sich zu vergewissern, dass alle teilnehmenden Personen ausreichend ermächtigt sind.
- (5) Aufzeichnungen bedürfen der Zustimmung und sind als Verschlussachen zu behandeln. Über das Mitführen von Bild- und Tonaufzeichnungsgeräten, mobilen Telekommunikationsgeräten und sonstiger Informationstechnik soll der Leiter der Veranstaltung vor deren Beginn entscheiden.
- (6) Bei Erörterung von STRENG GEHEIM oder GEHEIM eingestuften Verschlussachen, sollen abhörsichere oder abhörgeschützte Räume benutzt werden. Vor Konferenzen auf hoher Ebene oder von besonderer Bedeutung ist bezüglich der notwendigen Abhörschutzmaßnahmen das Bundesamt für Sicherheit in der Informationstechnik rechtzeitig beratend hinzuzuziehen.

§ 30 Grundsätze der Aussonderung von Verschlussachen

- (1) Als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlussachen werden wie nicht eingestuftes Material entsprechend dem Bundesarchivgesetz ausgesondert. Die Vernichtung erfolgt nach § 32.
- (2) Nicht mehr benötigte VS-VERTRAULICH oder höher eingestufte Verschlussachen sind aus dem Bestand der Dienststelle zur Archivierung oder Vernichtung nach den §§ 31 und 32 auszusondern.

§ 31 Archivierung von Verschlussachen

- (1) Dienststellen bieten, soweit gesetzlich nichts anderes bestimmt, ihre nicht mehr benötigten Verschlussachen der Geheimhaltungsgrade VS-VERTRAULICH oder höher dem Bundesarchiv (Geheimarchiv) nach der VS-Archivrichtlinie (Anlage VI) zur Archivierung an.
- (2) Dienststellen, die das Zwischenarchiv des Bundesarchivs nach § 20 der Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien nutzen, sollen ihre nicht mehr laufend benötigten Verschlussachen dem Bundesarchiv (Geheimarchiv) zur weiteren Aufbewahrung nach der VS-Archivrichtlinie übergeben.
- (3) Nachgeordnete Dienststellen mit regionaler Zuständigkeit, für deren Unterlagen nach § 7 des Bundesarchivgesetzes ein Landesarchiv zuständig ist, bieten ihre nicht mehr benötigten Verschlussachen dem Landesarchiv (Geheimarchiv) zur Archivierung an. Die VS-Archivrichtlinie ist sinngemäß anzuwenden. Soweit kein Geheimarchiv besteht, sind die Verschlussachen bis zur Aufhebung der Einstufung bei der jeweiligen Dienststelle zu verwahren.
- (4) Elektronisch vorliegende Verschlussachen sind dem zuständigen Archiv in entsprechender Anwendung der VS-Archivrichtlinie zur Übernahme anzubieten. Das technische Verfahren der Übergabe ist zuvor mit dem Archiv abzusprechen. Das Bundesarchiv stellt für die Aussonderung digitaler Unterlagen und deren Archivierung einen Leitfaden zur Verfügung.

§ 32 Vernichtung von Verschlussachen

- (1) Verschlussachen, die das zuständige Archiv nicht übernimmt, sind zu vernichten. Verschlussachen sind so zu vernichten, dass der Inhalt weder erkennbar ist, noch erkennbar gemacht werden kann.
- (2) Für die Vernichtung dürfen nur Produkte oder Verfahren eingesetzt oder Dienstleister beauftragt werden, die die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik erfüllen.
- (3) VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlussachen können vom Bearbeiter an den dafür vorgesehenen Orten selbst vernichtet werden.
- (4) VS-VERTRAULICH oder höher eingestufte Verschlussachen dürfen nur auf Weisung eines zeichnungsbefugten VS-Bearbeiters durch die VS-Registatoren vernichtet werden. Die VS-Registatoren prüfen die Verschlussachen vor der Vernichtung auf ihre Vollständigkeit. Die Vernichtung wird mittels Vernichtungsprotokoll und Vermerk der Vernichtungsprotokollnummer im VS-Bestandsverzeichnis nachgewiesen. Dabei ist zu vermerken, an welchem Tag welche Verschlussachen oder welche Teile davon vernichtet wurden (mit Angabe der Ausfertigungsnummer und Seitenzahl) und wer die Weisung zur Vernichtung erteilt hat. Das Vernichtungsprotokoll ist vom ausführenden VS-Registrator und von einem Zeugen zu unterschreiben.
- (5) Ist die Vernichtung von Verschlussachen technisch nur für eine Zusammenstellung von Verschlussachen möglich (zum Beispiel im Falle von Verschlussachen, die auf einem Datenträger gespeichert sind), ist die Vernichtung grundsätzlich so lange auszusetzen, bis alle Verschlussachen der Zusammenstellung vernichtet werden können. Ist die vorherige Vernichtung einzelner Dokumente unabdingbar, können die noch benötigten Dateien vor Vernichtung der Zusammenstellung nach den Bestimmungen dieser Verschlussachenanweisung vervielfältigt werden.

§ 33 VS-Zwischenmaterial

- (1) VS-Zwischenmaterial, das im Zusammenhang mit einer Verschlussache anfällt (zum Beispiel Dateien, Vorentwürfe, Stenogramme, Tonträger, Folien oder Fehldrucke), gilt als Verschlussache. Für die Behandlung von VS-Zwischenmaterial sind Abweichungen bei der Kennzeichnung und beim Nachweis sowie bei der Vernichtung zugelassen.
- (2) VS-Zwischenmaterial, das nicht an Dritte weitergegeben und das unverzüglich vernichtet wird, braucht nicht als Verschlussache gekennzeichnet und nicht nachgewiesen zu werden.
- (3) VS-Zwischenmaterial, das nicht unverzüglich vernichtet wird, ist mit dem entsprechenden Geheimhaltungsgrad und dem Zusatz "VS-Zwischenmaterial" zu kennzeichnen. Bei Weitergabe von VS-Zwischenmaterial von VS-VERTRAULICH oder höher eingestuften Verschlussachen an Dritte ist ein Nachweis erforderlich; dies gilt nicht bei Weitergabe an die VS-Registatur.

- (4) Die Vernichtung von VS-Zwischenmaterial richtet sich nach § 32 mit Ausnahme des Absatzes 4 Satz 2 bis 5, der keine Anwendung findet.

Abschnitt VI: Zusammenarbeit mit nichtdeutschen Stellen und nichtöffentlichen Stellen mit Sitz im Ausland

§ 34 Weitergabe von deutschen Verschlusssachen an nichtdeutsche Stellen und nichtöffentliche Stellen mit Sitz im Ausland

- (1) Die Weitergabe von deutschen Verschlusssachen an Dienststellen ausländischer Staaten sowie über- oder zwischenstaatlicher Organisationen (nichtdeutsche Stellen) setzt ein Regierungs- oder Ressortgeheimchutzabkommen oder ein entsprechendes internationales Abkommen voraus, welches die Bedingungen für die Weitergabe und weitere Handhabung regelt. Die Weitergabe von Verschlusssachen an nichtöffentliche Stellen mit Sitz im Ausland setzt entsprechende Regelungen in einem solchen Abkommen voraus.
- (2) Ein Regierungsgeheimchutzabkommen ermöglicht allen öffentlichen Stellen des Bundes den Verschlusssachenaustausch, ein Ressortgeheimchutzabkommen lediglich dem jeweiligen Ressort mit der weiteren Vertragspartei.
- (3) Wird die Notwendigkeit eines regelmäßigen VS-Austausches mit einem ausländischen Staat oder einer über- oder zwischenstaatlichen Organisation erkennbar, mit dem oder der kein Geheimchutzabkommen oder ein entsprechendes internationales Abkommen besteht, ist dem Bundesministerium des Innern und für Heimat in seiner Eigenschaft als Nationale Sicherheitsbehörde für den Geheimchutz die Notwendigkeit eines Regierungsgeheimchutzabkommens anzuzeigen. Nur für den Fall, dass der Abschluss eines solchen aus politischen, rechtlichen oder anderen Gründen nicht möglich sein sollte, ist der Abschluss eines Ressortgeheimchutzabkommens anzustreben. Die Erteilung einer Verhandlungsgenehmigung des Auswärtigen Amtes für ein Ressortgeheimchutzabkommen bedarf der Zustimmung des Bundesministeriums des Innern, für Bau und Heimat.
- (4) Liegt kein Regierungs- oder Ressortgeheimchutzabkommen oder ein entsprechendes internationales Abkommen vor, können deutsche Verschlusssachen nur dann an nichtdeutsche Stellen oder nichtöffentliche Stellen nach Absatz 1 weitergegeben werden, wenn
1. dies zur Erfüllung der Aufgaben der deutschen Stelle erforderlich ist,
 2. der Empfänger über die Geheimhaltungspflicht informiert wurde,
 3. die nichtdeutsche Stelle der deutschen Stelle nach dem Muster der Anlage VIII schriftlich zusichert, die Verschlusssachen entsprechend der eigenen Geheimchutzvorschriften zu schützen,

4. im Falle von VS-VERTRAULICH oder höher eingestuften Verschlusssachen der Empfänger schriftlich erklärt, dass nur sicherheitsüberprüftes Personal Zugang zu den Verschlusssachen erhält und
 5. die deutsche Stelle die Weitergabe dokumentiert.
- (5) Soweit die Weitergabe zur Wahrung wesentlicher Sicherheitsinteressen dringend erforderlich ist, können die Voraussetzungen des Absatzes 4 Nummer 1 bis 5 nachgeholt werden.
 - (6) Soweit deutsche Stellen deutsche Verschlusssachen an nichtdeutsche Stellen nach Absatz 1 oder Absatz 4 weitergeben, teilt der Geheimschutzbeauftragte dies unter Nennung der Anzahl, des Geheimhaltungsgrades und des Empfängers dem Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz jährlich mit.
 - (7) Deutsche Verschlusssachen sind vor der Weitergabe nach § 20 Absatz 2 hinsichtlich des Empfängers zu kennzeichnen.
 - (8) Vor der Weitergabe von Verschlusssachen an nichtdeutsche Stellen oder nichtöffentliche Stellen mit Sitz im Ausland ist die Zustimmung des Herausgebers einzuholen.

§ 35 Empfang und Handhabung nichtdeutscher Verschlusssachen

- (1) Nichtdeutsche Verschlusssachen, zu deren Schutz deutsche Dienststellen verpflichtet sind, sind nach dem deutschen Geheimhaltungsgrad, der dem Geheimhaltungsgrad der empfangenen Verschlusssache entspricht, und den getroffenen Vereinbarungen oder der Zusicherung nach Absatz 2 zu behandeln. Über- oder zwischenstaatliche Regelungen bleiben unberührt.
- (2) Soweit kein Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen vorliegt, dürfen deutsche Stellen zum Empfang nichtdeutscher Verschlusssachen Zusicherungen entsprechend § 34 Absatz 4 gegenüber nichtdeutschen Stellen abgeben. Das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz kann im Ausnahmefall abweichende Regelungen treffen.
- (3) Alle Rechte des nichtdeutschen Herausgebers bleiben unberührt.

§ 36 Sicherheitsakkreditierung

- (1) IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen (beispielsweise der EU oder der NATO) müssen einem Sicherheitsakkreditierungsverfahren unterzogen werden. Dieses Verfahren dient dem Zweck, Gewissheit darüber zu erlangen, dass alle angemessenen Sicherheitsmaßnahmen durchgeführt worden sind und dass ein ausreichender Schutz der Verschlusssachen und des IT-Systems nach den anzuwendenden Regelungen der über- oder zwischenstaatlichen Organisationen erreicht wird.

- (2) Das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz ist im Sinne der nationalen Zuständigkeit Sicherheitsakkreditierungsstelle (SAA) für IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen. Es kann diese Rolle oder die damit verbundenen Aufgaben ganz oder teilweise an andere Stellen delegieren.
- (3) Die Erarbeitung und fortlaufende Aktualisierung der anzuwendenden Akkreditierungsstrategie obliegt dem Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen mit dem Bundesministerium des Innern und für Heimat. Letzteres kann in Einzelfällen von der Akkreditierungsstrategie abweichen oder Abweichungen genehmigen.

§ 37 Zentralregistraturen

- (1) Für nichtdeutsche Verschlusssachen der NATO des Geheimhaltungsgrades COSMIC TOP SECRET oder mit dem Warnvermerk ATOMAL oder höher richtet die Nationale Sicherheitsbehörde für den Geheimschutz beim Bundesministerium der Verteidigung eine Zentralregistratur als zentrale Ein- und Ausgangsstelle für den Empfang und die Weitergabe der Verschlusssachen ein.
- (2) Für nichtdeutsche Verschlusssachen der EU des Geheimhaltungsgrades TRES SECRET UE/EU TOP SECRET richtet das Auswärtige Amt eine Zentralregistratur als zentrale Ein- und Ausgangsstelle für den Empfang und die Weitergabe der Verschlusssachen ein.

Weiteres zu diesem Abschnitt ist der Anlage VII zu entnehmen.

Abschnitt VII: Materielle und technische Maßnahmen

§ 38 Planung und Durchführung

- (1) Bei der Planung und Durchführung von Baumaßnahmen sind rechtzeitig die notwendigen Geheimschutzvorkehrungen zu treffen. Näheres bestimmen die Richtlinien für Sicherheitsmaßnahmen bei der Durchführung von Bauaufgaben.
- (2) Bei der Planung von VS-Aktensicherungsräumen, VS-Arbeitsbereichen, VS-IT-Räumen und -Bereichen, Sicherheitsbereichen, Alarmanlagen zum Schutz von Verschlusssachen, Telekommunikationsanlagen und abhörsicheren oder abhörgeschützten Räumen ist das Bundesamt für Sicherheit in der Informationstechnik beratend hinzuzuziehen.

§ 39 Räumliche Sicherheitsmaßnahmen

- (1) VS-IT-Räume und alle anderen Räume, in denen VS-VERTRAULICH oder höher eingestufte Verschlusssachen gehandhabt werden (VS-Arbeitsbereiche) sind so zu schützen, dass Unbefugte am Zutritt gehindert werden. Unberechtigte Zutrittsversuche sollen automatisiert aufgezeichnet werden.
- (2) Mit der Handhabung von Verschlusssachen befasste Organisationseinheiten und Personen sind nach Möglichkeit räumlich zusammenzufassen.

- (3) Sofern Umfang und Bedeutung der dort anfallenden Verschlussachen es erfordern, sind in einer Behörde oder sonstigen öffentlichen Stelle des Bundes oder in einem Teil von ihr von der jeweils zuständigen obersten Bundesbehörde im Einvernehmen mit dem Bundesministerium des Innern und für Heimat 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) Die in einem Sicherheitsbereich tätigen Personen sind beim Betreten des Sicherheitsbereiches anhand des Dienstausweises oder auf andere geeignete Weise zu identifizieren. Besucher und Fremdpersonal sind nach Identitätsfeststellung während des Aufenthalts im Sicherheitsbereich zu beaufsichtigen. Bei Besuchern und Fremdpersonal, die/das nachweislich (zum Beispiel durch eine Konferenzbescheinigung nach Muster der Anlage VIII) nach dem Sicherheitsüberprüfungsgesetz und der Allgemeinen Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz überprüft sind/ist, kann die Beaufsichtigung entfallen.
- (5) Das Kontrollpersonal ist über alle Arten von Ausweisen, die zum Betreten des Sicherheitsbereichs berechtigen, zu unterrichten. Die Aufgaben des Kontrollpersonals sind in einer Dienstanweisung festzulegen.
- (6) Personen, die zum Zugang zu Verschlussachen ermächtigt sind oder die eine Tätigkeit ausüben, bei der sie sich Zugang zu Verschlussachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher verschaffen können, ist der Betrieb von privaten Bild- und Tonaufzeichnungsgeräten, privater Informationstechnik und mobilen Telekommunikations-Endgeräten (dies sind zum Beispiel Mobiltelefone, Datenträger, PDA 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.

§ 40 Technische Sicherung von Verschlussachen

- (1) Technische Mittel zur Sicherung von Verschlussachen müssen die vom Bundesamt für Sicherheit in der Informationstechnik festgelegten Anforderungen erfüllen. Dies gilt insbesondere für:
 1. VS-Verwahrgelasse,
 2. VS-Schlüsselbehälter,
 3. Einbruch- und Überfallmeldeanlagen,
 4. Zutrittskontrollanlagen,
 5. VS-Transportbehälter,
 6. VS-Verpackungen,

7. VS-Sicherheitstüren und -schlösser und

8. technische Mittel zur Vernichtung von Verschlusssachen.

- (2) Das Bundesamt für Sicherheit in der Informationstechnik führt Prüfungen technischer Mittel und Eignungsfeststellungen entweder auf der Grundlage eines festgestellten Bedarfs in der Bundesverwaltung oder auf Antrag einer Dienststelle durch. Die abschließende Produktabnahme beinhaltet die Prüfung und Bewertung der technischen Mittel zur Sicherung von Verschlusssachen nach Maßgabe der besonderen Belange des Geheimschutzes. Die entsprechend einzuhaltenden Normen und ergänzenden Anforderungen legt das Bundesamt für Sicherheit in der Informationstechnik in Technischen Leitlinien fest.
- (3) Das Bundesamt für Sicherheit in der Informationstechnik gibt eine auf der Eignungsfeststellung basierende aktuelle Liste der geeigneten technischen Mittel als Technische Leitlinie heraus.
- (4) Stehen keine technischen Mittel mit Eignungsfeststellung zur Verfügung, kann das Bundesamt für Sicherheit in der Informationstechnik im Einzelfall auch dem Einsatz anderer technischer Mittel zustimmen, soweit diese einen vergleichbaren Schutz bieten.

§ 41 Abhörschutzmaßnahmen

- (1) Dienststellen haben Vorkehrungen zu treffen, damit ihre Telekommunikations- und Informationstechnik nicht dazu missbraucht werden kann, um Raum- und Telefongespräche abzuhören.
- (2) Dienststellen richten Räume, in denen häufig oder regelmäßig Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt geführt werden, abhörgeschützt oder abhörsicher wie folgt ein:
 1. VS-VERTRAULICH Abhörgeschützter Raum,
 2. GEHEIM Abhörgeschützter Raum und
 3. STRENG GEHEIM Abhörsicherer Raum.
- (3) Für Räume nach Absatz 2 gelten die folgenden grundsätzlichen Anforderungen:
 1. Verfügt die Dienststelle über einen Sicherheitsbereich, sollen sie grundsätzlich innerhalb dieses Sicherheitsbereichs eingerichtet werden.
 2. Sie sind gegen den unbemerkten Zutritt Unbefugter zu schützen. Art und Umfang des Schutzes legen die Geheimschutzbeauftragten unter Berücksichtigung der Lage und des bestehenden Umgebungsschutzes fest.
 3. Sie müssen mindestens eine akustische Dämpfung aufweisen, die ein Mithören von außen hinreichend ausschließt.

4. Sie sind so ausgeführt und ausgestattet, dass Versteckmöglichkeiten für Abhöreinrichtungen nach Möglichkeit beschränkt sind und Manipulationsprüfungen wirksam und in angemessener Zeit durchgeführt werden können.
5. Abhörsichere Besprechungsräume sind so zu gestalten, dass auch eine unbefugte Übertragung von Gesprächen mittels technischer Hilfsmittel (Abhörgeräten) nach außen verhindert wird.

Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

- (4) Geräte, die geeignet sind Bild- und/oder Tonaufnahmen zu erstellen, zu speichern oder zu übertragen (zum Beispiel Mobiltelefone, Smartphones, Notebooks, Kameras, Diktiergeräte), dürfen in abhörgeschützten oder abhörsicheren Räumen nicht mitgeführt werden, wenn diese für Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt genutzt werden. Ausnahmen bedürfen im Einzelfall der Zustimmung der Geheimschutzbeauftragten.

§ 42 Besondere Dienststellen

- (1) Sofern Dienststellen in besonderem Maße Ziel von Angriffen auf Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Verschlusssachen sind, legt das Bundesministerium des Innern und für Heimat diese als Dienststellen mit besonderem Geheimschutzbedarf fest.
- (2) Dienststellen nach Absatz 1 treffen in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik weitere Sicherheitsvorkehrungen. Insbesondere sind mindestens alle vier Jahre umfassende Beratungen und Prüfungen durch das Bundesamt für Sicherheit in der Informationstechnik in Anspruch zu nehmen.

§ 43 VS-Registraturen

- (1) VS-Registraturen werden, sofern vorhanden, in Sicherheitsbereichen eingerichtet.
- (2) Außerhalb der Arbeitszeit sind sie zu bewachen oder durch eine Alarmanlage technisch zu überwachen. In beiden Fällen ist sicherzustellen, dass Unbefugte am Zutritt gehindert werden und dass ein Eindringen Unbefugter erkannt und hilfeleistenden Stellen gemeldet wird.
- (3) Der Zutritt zu VS-Registraturen wird grundsätzlich nur den von den Geheimschutzbeauftragten festgelegten Mitarbeitern gewährt. Alle anderen Personen sind, soweit ihnen ebenfalls Zutritt gewährt werden muss, von Mitarbeitern der VS-Verwaltung zu begleiten.

§ 44 VS-Verwahrgele

- (1) VS-Verwahrgele sind besonders gesicherte Räume, Schränke oder sonstige Behälter zur Aufbewahrung von Verschlusssachen.

- (2) Jede VS-Registratur verfügt über mindestens ein VS-Verwahrgelass.
- (3) Ein VS-Verwahrgelass kann von mehreren Personen genutzt werden, soweit dem Grundsatz „Kenntnis nur, wenn nötig“ durch geeignete technische Maßnahmen Rechnung getragen wird, die die Geheimschutzbeauftragten in Abhängigkeit von den dort aufbewahrten Verschlusssachen und den zum Zugang berechtigten Personen festlegen und in der Geheimschutzdokumentation beschreiben.
- (4) Unberechtigte Zugangsversuche zu VS-Verwahrgelassen sind, soweit technisch möglich, zu protokollieren.

§ 45 VS-IT-Räume und -Bereiche

- (1) VS-IT-Räume und -Bereiche sind Räume und Bereiche, in denen VS-VERTRAULICH oder höher eingestufte Verschlusssachen mit IT be- oder verarbeitet werden.
- (2) Sie sollen, sofern vorhanden, in Sicherheitsbereichen eingerichtet oder zu Sicherheitsbereichen im Sinne von § 39 Absatz 3 erklärt und entsprechend gegen unbefugten Zutritt geschützt werden.
- (3) Die Sicherungsmaßnahmen für Räume und Bereiche, in denen VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen mit IT be- und verarbeitet werden, sind von den Geheimschutzbeauftragten festzulegen.

§ 46 Zutritts- und Zugangsmittel

- (1) Zutritts- und Zugangsmittel zu VS-Arbeitsbereichen, Sicherheitsbereichen, VS-Verwahrgelassen, abhörgeschützten und abhörsicheren Räumen, VS-IT, mit der VS-VERTRAULICH oder höher eingestufte Verschlusssachen gehandhabt werden oder Systemen zur technischen Überwachung von Verschlusssachen sind so zu schützen, dass Unbefugte keinen Zugriff auf Verschlusssachen erhalten.
- (2) Gegenständliche Zutritts- und Zugangsmittel sind grundsätzlich während der Dienstzeit in persönlichem Gewahrsam zu halten. Vor Verlassen des Dienstgebäudes sind sie grundsätzlich in einem VS-Verwahrgelass oder VS-Schlüsselbehälter zu verschließen. VS-Schlüsselbehälter sind möglichst zu beaufsichtigen. Der Verschluss von Zutritts- und Zugangsmitteln unterschiedlicher Nutzer erfolgt grundsätzlich getrennt. Die Schlüssel zu den VS-Schlüsselbehältern verbleiben im persönlichen Gewahrsam des Nutzers des VS-Schlüsselbehälters.
- (3) Wissensbasierte Zutritts- und Zugangsmittel dürfen nur den Berechtigten bekannt sein. Sie sind zu ändern:
 1. vor der erstmaligen Nutzung,
 2. bei einem Wechsel der Berechtigten,
 3. nach deren Nutzung in Abwesenheit des Berechtigten,

4. bei einem Verdacht, dass sie bekannt geworden sind und
 5. mindestens alle zwölf Monate.
- (4) Zutritts- und Zugangsmittel nach Absatz 1 sind zentral zu verwalten und deren Ausgabe zu dokumentieren.
 - (5) Für Notfälle sollen gegenständliche und wissensbasierte Reservezutritts- und -zugangsmittel in beschrifteten und versiegelten Umschlägen voneinander und von den Originalzutritts- und -zugangsmitteln getrennt in VS-Verwahr gelassen aufbewahrt werden.

§ 47 Abnahmen und Wiederholungsprüfungen

- (1) Dienststellen weisen die ordnungsgemäße Funktion und Ausführung von technischen Mitteln zur Sicherung von Verschlusssachen, von abhörgeschützten und abhörsicheren Räumen sowie die Einhaltung der Anforderungen der jeweiligen Technischen Leitlinien durch Abnahmeprüfungen des Bundesamtes für Sicherheit in der Informationstechnik und entsprechende Prüfprotokolle nach.
- (2) Das Bundesamt für Sicherheit in der Informationstechnik ist über anstehende Prüfungen nach Absatz 1 rechtzeitig zu unterrichten.
- (3) Nach wesentlichen Änderungen oder wenn eine Beeinträchtigung der Wirksamkeit (zum Beispiel durch Abnutzung oder Verschleiß) zu erwarten ist, sind die Überprüfungen zu wiederholen.
- (4) Bei Auslandsvertretungen der Bundesrepublik Deutschland tritt der Bundesnachrichtendienst an die Stelle des Bundesamtes für Sicherheit in der Informationstechnik.

§ 48 Lauschabwehrprüfungen

- (1) Lauschabwehrprüfungen werden vom Bundesamt für Sicherheit in der Informationstechnik durchgeführt.
- (2) Abhörgeschützte und abhörsichere Räume sind auf Veranlassung der Geheimschutzbeauftragten vor der erstmaligen Nutzung für Verschlusssachen und danach stichprobenweise sowie anlassbezogen auf Manipulationen zu untersuchen, die die Sicherheit der Verschlusssachen gefährden können.
- (3) Die Geheimschutzbeauftragten legen die Häufigkeit der Stichproben in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik fest. In Dienststellen nach § 42 soll die Prüfung ausgewählter Räume mindestens alle vier Jahre durchgeführt werden.
- (4) Andere Räume sind bei Vorliegen eines Manipulationsverdachts oder aus Anlass von Konferenzen von besonderer Bedeutung zu prüfen.

- (5) Die Dienststellen unterstützen das Bundesamt für Sicherheit in der Informationstechnik bei der Durchführung der Überprüfungen.
- (6) Bei Auslandsvertretungen der Bundesrepublik Deutschland tritt der Bundesnachrichtendienst an die Stelle des Bundesamtes für Sicherheit in der Informationstechnik.

Abschnitt VIII: Einsatz von Informationstechnik

§ 49 Allgemeine Grundsätze

- (1) Die Sicherheit von VS-IT ist während des gesamten Lebenszyklus ab dem Zeitpunkt, zu dem feststeht, dass sie zur VS-Verarbeitung eingesetzt werden soll, bis zur Aussonderung kontinuierlich zu gewährleisten.
- (2) Werden mit VS-IT VS-VERTRAULICH oder höher eingestufte Verschlusssachen verarbeitet, ist eine Risikoanalyse nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils gültigen Fassung durchzuführen.

§ 50 Freigabe des Betriebs von VS-IT

- (1) Die Verarbeitung von Verschlusssachen ist nur mit VS-IT zulässig, die hierfür freigegeben ist. Die Freigabe kann mit Auflagen erteilt werden.
- (2) Voraussetzung für die Freigabe ist die Einhaltung der Standards zur Informationssicherheit des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung. Dies ist dem Bundesamt nach dessen Vorgaben nachzuweisen; es überprüft die Umsetzung turnusmäßig nach den Vorgaben des Bundesministeriums des Innern und für Heimat risikobasiert gemäß § 4a BSIG.
- (3) Für eine Freigabe ist zudem erforderlich, dass die Anforderungen des Geheimschutzes erfüllt sind; das sind regelmäßig:
 1. Die Erfüllung des Grundsatzes „Kenntnis nur, wenn nötig“ (§§ 3 Absatz 1, 24 Absatz 2 und 58 Absatz 1 Nummer 2)
 2. die Beachtung der Grundsätze zu Einstufung und Kennzeichnung von Verschlusssachen (§§ 15 Absatz 1, 17 Absatz 1, 18 Absatz 2, 19 und 20 Absatz 2)
 3. die Verwaltung und der Nachweis der Verschlusssachen (§ 21)
 4. die Einhaltung der Regeln zur (zeitweiligen) Aufbewahrung von Verschlusssachen (§ 23)
 5. die Gewährleistung der Sicherheit von VS-IT über deren gesamten Lebenszyklus (§ 49 Absatz 1)
 6. die Aussonderung und Vernichtung von Verschlusssachen (§§ 30 fortfolgende, 56)
 7. die Beachtung der Vorgaben zur Übertragung von Verschlusssachen über technische Kommunikationsverbindungen (§ 55)
 8. die Beachtung der einschlägigen Bestimmungen über- oder zwischenstaatlicher Organisationen sowie bilateraler Geheimschutzabkommen (§§ 34 und 35)

9. die Sicherheitsakkreditierung (§ 36).

Die Anforderungen werden in dem vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Geheimschutzbaustein des IT-Grundschutzes konkretisiert. Im Einzelfall und insbesondere infolge weiterer Geheimschutzanforderungen aufgrund nationaler und internationaler Bestimmungen mit Bezug auf die Handhabung und Verarbeitung von Verschlussachen der Geheimhaltungsgrade VS-VERTRAULICH oder höher können die Geheimschutzbeauftragten weitere Anforderungen vorsehen.

Vor der Freigabe veranlassen die Geheimschutzbeauftragten eine Überprüfung der wirksamen Umsetzung der Geheimschutzanforderungen, beispielsweise durch einrichtungs-externe Prüfer. Das Ergebnis der Überprüfung ist in der Geheimschutzdokumentation festzuhalten.

- (4) Die Dienststellenleitung erteilt die Freigabe, sofern die in den Absätzen 2 und 3 genannten Voraussetzungen vorliegen. Bei Freigaben von VS-IT-Systemen für den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH ist dies insbesondere der Fall, soweit hierfür eine ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes inklusive der im Geheimschutzbaustein aufgeführten Anforderungen vorliegt. Sollen Verschlussachen der Geheimhaltungsgrade VS-VERTRAULICH oder höher verarbeitet werden, tritt als weitere Voraussetzung ein Freigabevotum des Bundesamtes für Sicherheit in der Informationstechnik hinzu. Das Freigabevotum und die Freigabe sind in der Geheimschutzdokumentation festzuhalten.
- (5) Sind an einem VS-IT-System mehrere Dienststellen des Bundes beteiligt, handelt es sich um einen VS-IT-Verbund. In diesem Fall obliegt die Gesamtfreigabe der für den Betrieb verantwortlichen Dienststelle (Betreiber). Die Gesamtfreigabe erfolgt auf Grundlage der in Absatz 4 genannten Voraussetzungen. Im Zweifel bestimmt bei ressortinternen VS-IT-Verbänden die zuständige oberste Bundesbehörde und bei ressortübergreifenden VS-IT-Verbänden das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz den Betreiber des VS-IT-Verbundes. Der Betreiber ist für die Koordinierung der Erfüllung der in Absatz 4 genannten Voraussetzungen zuständig. Das Freigabevotum und die Freigabe sind in der Geheimschutzdokumentation des Betreibers festzuhalten.
- (6) Wird ein VS-IT-System im Auftrag des Bundes privatrechtlich betrieben, so bestimmt die jeweils zuständige oberste Bundesbehörde, welche Stelle als Betreiber für die Umsetzung der sich aus der VSA ergebenden Aufgaben Sorge trägt. Bei ressortübergreifenden VS-IT-Systemen bestimmt im Zweifel das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz die hierfür zuständige Dienststelle.
- (7) Das Bundesamt für Sicherheit in der Informationstechnik unterstützt die Dienststellen im Prozess der VS-IT-Freigabe einschließlich der Erfüllung seiner Vorgaben. Dies erfolgt etwa auch anhand von Handreichungen und Praxisbeispielen.
- (8) Die Geheimschutzbeauftragten veranlassen eine Wiederholung der Überprüfung nach Absatz 3 in regelmäßigen Abständen sowie anlassbezogen. Ergibt die Überprüfung, dass eine Freigabe nicht erneut erteilt werden könnte, haben die Geheimschutzbeauftragten

auf die unverzügliche Herstellung eines vorschriftenkonformen Zustandes hinzuwirken. Die Freigabe ist zu widerrufen, wenn auch mit Maßnahmen des Risikomanagements ein vorschriftenkonformer Zustand nicht hergestellt werden kann. Die Ergebnisse der Folgeüberprüfungen sowie ein Widerruf der Freigabe sind in der Geheimschutzdokumentation festzuhalten.

- (9) Geheimschutzrelevante Änderungen bei freigegebener VS-IT bedürfen der vorherigen Zustimmung der Geheimschutzbeauftragten.
- (10) Dem Bundesamt für Sicherheit in der Informationstechnik ist die erfolgte Freigabe sowie ihr Widerruf mitzuteilen. Das Bundesamt für Sicherheit in der Informationstechnik führt eine Liste über die in den Dienststellen freigegebene VS-IT sowie der freigegebenen VS-IT-Verbünde und erteilt allen Dienststellen auf berechtigtes Verlangen darüber Auskunft.
- (11) Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 51 Zulassung

- (1) Das Bundesamt für Sicherheit in der Informationstechnik legt fest, welche IT-Sicherheitsprodukte oder -komponenten über eine Zulassung verfügen müssen. Diese IT-Sicherheitsprodukte und -komponenten übernehmen innerhalb von VS-IT IT-Sicherheitsfunktionen zum Schutz elektronischer Verschlusssachen.
- (2) Grundlage für die Zulassung ist das Zulassungskonzept des Bundesamtes für Sicherheit in der Informationstechnik. Dieses wird im Einvernehmen zwischen dem Bundesministerium des Innern und für Heimat und dem Bundesamt für Sicherheit in der Informationstechnik festgelegt.
- (3) Die Zulassung wird durch einen Zulassungsnachweis des Bundesamtes für Sicherheit in der Informationstechnik bestätigt. Dieser enthält auch Bestimmungen für den Einsatz und den Betrieb.
- (4) Das Bundesamt für Sicherheit in der Informationstechnik führt Zulassungsverfahren entweder auf der Grundlage eines festgestellten Bedarfs in der Bundesverwaltung oder auf Antrag einer Dienststelle durch.
- (5) Sofern für bestimmte VS-IT keine zugelassenen IT-Sicherheitsprodukte oder -komponenten zur Verfügung stehen oder eine Bereitstellung nicht oder nicht zeitgerecht veranlasst werden kann, ist beim Bundesamt für Sicherheit in der Informationstechnik eine Einsatzerlaubnis für andere IT-Sicherheitsprodukte oder -komponenten zu beantragen. Das Bundesamt kann diese Einsatzerlaubnis zeitlich befristen sowie besondere Auflagen und Einschränkungen hinsichtlich der Einsatz- und Betriebsbedingungen erteilen. Nähere Einzelheiten regelt das Zulassungskonzept des Bundesamtes für Sicherheit in der Informationstechnik.

§ 52 IT-Sicherheitsfunktionen

- (1) IT-Sicherheitsfunktionen innerhalb von VS-IT, die Gegenstand einer Zulassungsaussage nach § 51 sein können, sind Funktionen, die sich den folgenden Kategorien zuordnen lassen:
1. zur Zugangs- und Zugriffskontrolle,
 2. zur Identifikation und Authentisierung,
 3. zur kryptographischen Unterstützung,
 4. für das Sicherheitsmanagement,
 5. zur Informationsflusskontrolle,
 6. zum internen Schutz der Benutzerdaten,
 7. zum Selbstschutz der Sicherheitsfunktionen und ihrer Daten,
 8. zur Netzwerktrennung,
 9. zum Schutz der Unversehrtheit,
 10. zur Verfügbarkeitsüberwachung oder
 11. zur Sicherheitsprotokollierung und Nachweisführung.

Einzelheiten dazu und zum Zulassungskonzept werden in den Technischen Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik geregelt. Diese regeln auch die Mitwirkungspflichten der an einem Zulassungsverfahren beteiligten Parteien.

- (2) Das Bundesamt für Sicherheit in der Informationstechnik gibt einen auf diesen IT-Sicherheitsfunktionen und den sich hieraus ableitenden Produktklassen und -typen basierenden Katalog sowie eine aktuelle Liste zugelassener IT-Sicherheitsprodukte und -komponenten heraus. Der Katalog der Produktklassen und -typen definiert insbesondere,
1. ob eine Zulassungsaussage für einen Produkttyp erforderlich ist und
 2. welche Sicherheitsfunktionen in einem Zulassungsverfahren für einzelne Produkttypen gelten.

§ 53 Schutz von VS-Übertragungseinrichtungen, -leitungen und -verteilern

- (1) VS-Übertragungseinrichtungen, -leitungen und -verteiler, die Verschlusssachen unverschlüsselt führen, sind gegen unbefugten Zugriff zu schützen.

- (2) Für VS-IT, die für VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen eingesetzt wird, gilt dieser Schutz innerhalb von Räumen und Bereichen, die gegen unkontrollierten Zutritt geschützt sind, grundsätzlich als gegeben.
- (3) Für VS-IT, die für VS-VERTRAULICH oder höher eingestufte Verschlusssachen eingesetzt wird, gilt dieser Schutz innerhalb von VS-IT-Räumen und -Bereichen grundsätzlich als gegeben.
- (4) Außerhalb von Räumen und Bereichen nach den Absätzen 2 und 3 sind durch die Geheimschutzbeauftragten festzulegende zusätzliche Maßnahmen zu treffen. Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 54 Handhabung von Datenträgern und IT-Produkten für unverschlüsselte Verschlusssachen

IT-Produkte, die keiner Zulassung bedürfen, Datenträger und mobile IT, auf denen jeweils elektronische Verschlusssachen unverschlüsselt gespeichert sind, sind so zu schützen wie es die Einstufung der darauf gespeicherten Information erfordert.

§ 55 Übertragung von Verschlusssachen über technische Kommunikationsverbindungen

- (1) Verschlusssachen müssen bei der Weitergabe über technische Kommunikationsverbindungen (elektronische Übertragung) grundsätzlich durch IT-Sicherheitsprodukte nach Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik verschlüsselt werden. § 57 bleibt unberührt.
- (2) Abweichend von Absatz 1 ist die unverschlüsselte Weitergabe von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH grundsätzlich erlaubt, wenn sie unter Einsatz von VS-IT erfolgt, die gemäß den Vorschriften des § 50 dazu freigegeben worden ist. Vor der Weitergabe hat sich jede Nutzerin und jeder Nutzer zu vergewissern, dass nicht nur die Bedingungen des § 24 Absatz 2 und 3 erfüllt sind, sondern die Empfängerinnen und Empfänger die Verschlusssachen ausschließlich über das dafür freigegebene Netz erhalten. Sind diese Bedingungen erfüllt, ist auch die Weitergabe von Verschlusssachen über- und zwischenstaatlicher Organisationen sowie anderer Staaten erlaubt, es sei denn, höherrangige Rechtsvorschriften stehen dem ausdrücklich entgegen.
- (3) Abweichend von Absatz 1 dürfen Verschlusssachen ausnahmsweise über andere technische Kommunikationsverbindungen übermittelt werden, wenn die Übermittlung über eine Kommunikationsverbindung nach Absatz 1 einen unvermeidbaren Zeitverlust bedeuten würde. In diesem Fall darf
 1. für die Kommunikation von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen eine nicht nach Absatz 1 geschützte Verbindung genutzt werden. Es sind Verbindungen auszuwählen, bei denen das Risiko des Mithörens durch Unbefugte weitestgehend reduziert wird.
 2. für die Kommunikation von VS-VERTRAULICH eingestuften Informationen eine für VS-NUR FÜR DEN DIENSTGEBRAUCH freigegebene Verbindung genutzt werden.

- (4) Abweichend von Absatz 1 dürfen Verschlusssachen über andere technische Kommunikationsverbindungen übermittelt werden, wenn eine Verzögerung zu einem Schaden führen würde, der den mit einer Preisgabe der Verschlusssache verbundenen Schaden deutlich überwiegen würde. In jedem Einzelfall ist die Einwilligung der Dienststellenleitung einzuholen und zu dokumentieren.
- (5) In den Ausnahmefällen nach den Absätzen 3 und 4 sind folgende Vorsichtsmaßnahmen, die den Mitarbeitern zur Kenntnis zu geben sind, zu beachten, damit das Risiko eines Informationsabflusses weitgehend reduziert wird:
 1. Die Identität des Kommunikationspartners soll vor Beginn der Kommunikation festgestellt werden,
 2. die Kommunikation ist so zu führen, dass der Sachverhalt Dritten nicht verständlich wird und ein unmittelbarer Rückschluss auf den VS-Charakter nicht möglich ist,
 3. die übermittelten Verschlusssachen dürfen keine Kennzeichnungen oder Hinweise aufweisen, die sie von einer nicht eingestuften Information unterscheiden. Die Kennzeichnungspflicht nach § 20 ist in diesem Fall aufgehoben und
 4. die Kommunikationspartner sind auf anderem Wege (zum Beispiel über andere technische Kommunikationsverbindungen, durch Post oder Kurier) unverzüglich über die Einstufung der Verschlusssachen zu unterrichten, außer, dies ist im Einzelfall nicht möglich oder nicht zweckmäßig.

§ 56 Vernichtung und Aussonderung von Datenträgern und registrierten IT-Produkten

- (1) Bevor IT-Produkte, Datenträger und mobile IT im Sinne von § 54 ihre gesicherte Einsatzumgebung dauerhaft verlassen, ist sicherzustellen, dass alle auf ihnen gespeicherten Verschlusssachen gelöscht werden. Die Löschung muss mittels vom Bundesamt für Sicherheit in der Informationstechnik nach § 51 dafür zugelassener beziehungsweise zur Freigabe empfohlener IT-Sicherheitsprodukte erfolgen.
- (2) Ist eine Löschung nicht möglich, sind die Speichermedien physisch zu vernichten.
- (3) Die Löschung beziehungsweise Vernichtung ist in der Geheimschutzdokumentation zu dokumentieren.
- (4) Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 57 Abstrahlschutzmaßnahmen

Bei VS-IT, die für VS-VERTRAULICH oder höher eingestufte Verschlusssachen eingesetzt wird, sind Abstrahlschutzmaßnahmen (zum Beispiel nach dem Zonenmodell) zu treffen und zu dokumentieren. Einzelheiten sind einer Technischen Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik zu entnehmen.

§ 58 Zusammenschaltung von VS-IT

- (1) Vor der Zusammenschaltung von VS-IT mit anderer VS-IT ist zu prüfen, ob und inwieweit Informationen zwischen diesen Systemen unter Berücksichtigung

1. des jeweiligen Schutzniveaus und
2. des Prinzips „Kenntnis nur, wenn nötig“

ausgetauscht werden dürfen. In Abhängigkeit zum Ergebnis der Prüfung sind IT-Sicherheitsfunktionen nach § 52 zum Schutz der Systemübergänge zu implementieren.

- (2) Die direkte oder kaskadierte Zusammenschaltung von bis zum Geheimhaltungsgrad STRENG GEHEIM freigegebener VS-IT mit offener oder ungeschützter IT ist nicht zulässig.

Abschnitt IX: Kryptopersonal und Handhabung von Kryptomitteln

§ 59 Kryptomittel

- (1) Nationale Kryptomittel im Sinne dieser Vorschrift sind Produkte, Geräte und die dazugehörigen Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen, die vom Bundesamt für Sicherheit in der Informationstechnik oder für den Geschäftsbereich des Bundesministeriums der Verteidigung vom Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr als solche festgelegt werden. Internationale Kryptomittel werden nach den einschlägigen über- oder zwischenstaatlichen Vorschriften sowie den jeweiligen nationalen Vorschriften anderer Staaten festgelegt.
- (2) Eingestufte Kryptomittel erhalten einen der Warnvermerke „KRYPTO“ (für „KRYPTOSICHERHEIT“) oder „CRYPTO“ (für „CRYPTOSECURITY“). Nicht eingestufte Kryptogeräte sowie zugehörige kryptographische Komponenten und andere zugehörige Bauteile, die sicherheitsempfindliche Funktionen ausführen, erhalten den Warnvermerk „CCI“ (für „Controlled COMSEC Item“).
- (3) Alle Kryptomittel unterliegen einer Nachweisführung. Die Nachweisführung erfolgt entsprechend der Nachweisführung für Verschlusssachen der Einstufung VS-VERTRAULICH oder höher. Dazu sind eigene Bestandsverzeichnisse anzulegen.

§ 60 Nationale Verteilerstellen für Kryptomittel

- (1) Das Bundesamt für Sicherheit in der Informationstechnik nimmt die Aufgaben der zentralen Nachweisführung, Verwaltung und Verteilung von Kryptomitteln als zivile nationale Verteilerstelle für Kryptomittel (Civil National Distribution Authority) wahr.
- (2) Das Zentrum für Informationstechnik der Bundeswehr nimmt die Aufgaben der militärischen nationalen Verteilerstelle für Kryptomittel (Military National Distribution Authority) wahr.

§ 61 Kryptoverwaltung

- (1) Dienststellen, die Kryptomittel handhaben, bestellen mindestens einen Kryptoverwalter und eine zur Vertretung berechtigte Person (Kryptoverwaltung). Große Kryptoverwaltungen, die mehrere Kryptoverwalter benötigen, bestimmen einen leitenden Kryptoverwalter. Kryptoverwalter und die zur Vertretung berechtigten Personen müssen die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde erwerben.
- (2) Der Name des (leitenden) Kryptoverwalters, der zur Vertretung berechtigten Person und die Behördenanschrift sowie Änderungen sind der jeweils zuständigen nationalen Verteilerstelle für Kryptomittel mitzuteilen.
- (3) Haben sich während der Abwesenheit des Kryptoverwalters Veränderungen im Kryptobestand ergeben, so führt dieser unmittelbar nach Rückkehr eine Bestandsprüfung durch. Beim Wechsel des Kryptoverwalters ist der Bestand zu überprüfen und ein Bestandsbericht (Übergabeprotokoll) zu fertigen.
- (4) Weitere Aufgaben der Kryptoverwaltung sind der Anlage I zu entnehmen. Näheres zur Handhabung von Kryptomitteln regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 62 Kryptopersonal

Personen, die Zugang zu Kryptomitteln erhalten (Kryptopersonal), sind vom Geheimschutzbeauftragten nach Muster der Anlage VIII zu belehren und zu berechtigen (Kryptoberechtigung). Die Belehrung und die Berechtigung sind zu dokumentieren.

Abschnitt X: Aufrechterhaltung des Geheimschutzes

§ 63 Kontrollen

- (1) Die Geheimschutzbeauftragten sollen in ihrer Dienststelle in angemessenen Zeitabständen kontrollieren, ob die Einstufung, die Befristung und die Handhabung der Verschlusssachen den Vorschriften der Verschlusssachenanweisung entsprechen. Die Kontrollen können auch durch besonders beauftragte Mitarbeiter durchgeführt werden. Soweit die Bearbeitung von Verschlusssachen mit IT betroffen ist, werden die Geheimschutzbeauftragten hierbei von den IT-Sicherheitsbeauftragten unterstützt.
- (2) Alle Bediensteten haben die Durchführung von Kontrollen zu unterstützen und hierfür auf Verlangen Zugang zu allen Verschlusssachen zu gewähren.
- (3) Die obersten Bundesbehörden können in angemessenen Abständen bei den Behörden ihres jeweiligen Geschäftsbereichs kontrollieren, ob die dortigen Regelungen, Maßnahmen und Verfahren der Verschlusssachenanweisung entsprechen.
- (4) Die Durchführung der Kontrollen und deren Ergebnisse sind in angemessener Weise zu dokumentieren.

§ 64 Behandlung von Geheimschutzvorkommnissen

- (1) Wird bekannt oder besteht der Verdacht, dass Geheimschutzvorschriften verletzt wurden oder Sicherheitsvorkehrungen den Geheimschutz nicht gewährleisten, sind die betroffenen Geheimschutzbeauftragten unverzüglich zu unterrichten. Die Geheimschutzbeauftragten stellen in diesen Fällen den Sachverhalt fest und treffen die erforderlichen Maßnahmen.
- (2) Werden Dienststellen geheimschutzbezogene Vorkommnisse mit Bezug zu VS-VERTRAULICH oder höher eingestuften nationalen Verschlussachen von wesentlicher Bedeutung bekannt, unterrichten sie unverzüglich das Bundesministerium des Innern und für Heimat, wenn die Besorgnis einer Bekanntgabe an Dritte besteht. Gleiches gilt für nichtdeutsche Verschlussachen, unabhängig von deren Geheimhaltungsgrad.
- (3) Ist ein nachrichtendienstlicher Hintergrund oder eine Verratstätigkeit anderer Art nicht auszuschließen, so ist das Bundesamt für Verfassungsschutz, im Geschäftsbereich des Bundesministeriums der Verteidigung das Bundesamt für den Militärischen Abschirmdienst zu beteiligen.
- (4) Dienststellen, denen geheimschutzbezogene Vorkommnisse bekannt werden, die für die technische Sicherung von Verschlussachen oder für die Sicherheit der Informations- und Kommunikationstechnik des Bundes von Bedeutung sind, unterrichten unverzüglich das Bundesamt für Sicherheit in der Informationstechnik. Das Bundesamt für Sicherheit in der Informationstechnik unterrichtet im Anschluss unverzüglich das Bundesministerium des Innern und für Heimat.

§ 65 Verhalten in außergewöhnlichen Gefahrenlagen

Sofern im Katastrophen-, Alarm- oder Verteidigungsfall oder in vergleichbaren außergewöhnlichen Gefahrenlagen die Möglichkeit besteht, dass Unbefugte sich Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlussachen verschaffen können, und eine Aufbewahrung nach § 23 nicht möglich ist, sind die Verschlussachen zu vernichten. Die Dienststellen treffen in ihren Geheimschutzdokumentationen Handlungsanweisungen für die Vernichtung in diesen Fällen.

Abschnitt XI: Abschließende Regelungen

§ 66 Schlussbestimmungen

- (1) Das Bundesministerium des Innern und für Heimat kann in besonderen Ausnahmefällen Abweichungen von dieser Verschlussachenanweisung unter der Voraussetzung zulassen, dass der mit der Verschlussachenanweisung beabsichtigte Schutz durch andere Sicherheitsvorkehrungen erreicht wird.
- (2) Jede Dienststelle kann über die Verschlussachenanweisung hinaus verschärfte Sicherheitsvorkehrungen treffen, soweit sie die notwendige einheitliche Behandlung der Verschlussachen im gesamten VS-Verkehr nicht stören.

§ 67 Inkrafttreten

Diese Allgemeine Verwaltungsvorschrift tritt am 1. April 2023 in Kraft. Gleichzeitig tritt die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlussachenanweisung - VSA) vom 10. August 2018 (GMBL 2018, 826) außer Kraft.

Es gelten folgende Anlagen zu dieser Vorschrift

- Anlage I: Hinweise zur Geheimschutzorganisation
- Anlage II: Hinweise zur Geheimschutzdokumentation
- Anlage III: Hinweise zur Einstufung
- Anlage IV: Hinweise zur Handhabung von Verschlussachen
- Anlage V: Merkblatt zur Behandlung von Verschlussachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)
- Anlage VI: Richtlinie für die Abgabe von Verschlussachen an das Geheimarchiv des Bundesarchivs (VS-Archivrichtlinie)
- Anlage VII: Hinweise zur Handhabung von Verschlussachen ausländischer Staaten sowie über- oder zwischenstaatlicher Organisationen
- Anlage VIII: Muster

Berlin, den 13. März 2023

Bundesministerium des Innern und für Heimat
In Vertretung

Engelke