Verwaltungsvorschrift der Sächsischen Staatsregierung über die Behandlung von Verschlusssachen (Verschlusssachenanweisung – VSA)

Vom 4. Januar 2008

Gemäß § 35 des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Freistaat Sachsen (Sächsisches Sicherheitsüberprüfungsgesetz – SächsSÜG) vom 19. Februar 2004 (SächsGVBl. S. 44), in der jeweils geltenden Fassung, wird zum materiellen und organisatorischen Schutz von Verschlusssachen (VS) die nachfolgende Verwaltungsvorschrift erlassen.

Sie orientiert sich im Interesse eines einheitlichen Geheimschutzes, wie ihn die Ständige Konferenz der Innenminister und -senatoren des Bundes und der Länder mit Beschluss vom 29. April 1982 empfohlen hat, im Wesentlichen an der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 31. März 2006.

Inhaltsübersicht

I. Allgemeine Bestimmungen

1. Geltungsbereich

1.1 Die Verschlusssachenanweisung (VSA) richtet sich an Behörden und öffentlich-rechtliche Einrichtungen des Freistaates Sachsen, die mit Verschlusssachen arbeiten und damit Vorkehrungen zu deren Schutz zu treffen haben.

1.2 Darüber hinaus richtet sich die VSA an Personen, die Zugang zu Verschlusssachen erhalten oder eine Tätigkeit ausüben, bei der sie sich Zugang zu Verschlusssachen verschaffen können und dabei bestimmte Schutzvorkehrungen zu beachten haben.

2. Begriff der Verschlusssache sowie sonstige Begriffsbestimmungen

2.1 Nach § 4 Abs. 1 SächsSÜG sind Verschlusssachen (VS) im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform, beispielsweise Schriftstücke, Zeichnungen, Karten, Fotokopien, Lichtbildmaterial, elektronische Dateien oder Datenträger, elektrische Signale, Geräte, technische Einrichtungen oder das gesprochene Wort. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung in Geheimhaltungsgrade eingestuft.

2.2 Zwischenmaterial, das im Zusammenhang mit einer VS anfällt, wie Dateien, Vorentwürfe, Stenogramme, Tonträger, Folien oder Fehldrucke, gilt als VS im Sinne der Nummer 2.1. Für die Behandlung von VS-Zwischenmaterial sind Abweichungen bei der Kennzeichnung und beim Nachweis sowie bei der Vernichtung gemäß Nummern 16.5 und 16.6 zugelassen.

2.3 Können wegen der Beschaffenheit einer VS Bestimmungen der VSA nicht angewendet werden, so ist sinngemäß zu verfahren. Dabei sind möglichst gleichwertige Sicherheitsmaßnahmen zu treffen.

2.4 Sonstige Begriffsbestimmungen

a) Verfügbarkeit einer VS bedeutet, dass der berechtigte Zugriff gesichert sein muss, zum Beispiel durch hinterlegte Zweitschlüssel oder Sicherheitskopien bei elektronischer Darstellung.

b) Integrität einer VS, auch als Unversehrtheit bezeichnet, bedeutet die Sicherheit, dass eine VS unverändert und vollständig ist, zum Beispiel dass nicht eine Anlage der VS entnommen ist. Dies kann durch unzureichende Sicherung (einfaches Schloss) verursacht sein.

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

d) Datenträger sind Speichermedien für Computerdaten und -programme, zum Beispiel Disketten, Festplatten, CD.

e) Personal Digital Assistent (PDA) sind tragbare Kleinstcomputer.

f) Nichtflüchtige Speichermedien: Unterschieden wird zwischen Speichermedien, die beim Abschalten den gespeicherten Dateninhalt verlieren (zumeist innerhalb von Geräten verwendet) und nichtflüchtigen Speichern, bei denen der Inhalt meistens bis zum nächsten Einschalten erhalten bleibt, zum Beispiel Disketten, CD, Festplatten.

g) Ein Dongel, auch Dongle, ist eine Vorrichtung für Computer, meist in Form eines Steckers, um Funktionen abzusichern, zum Beispiel Kopierschutz oder Zugang.

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

i) Penetrationstest ist ein Verfahren zur Prüfung des Schutzes eines Computernetzes gegen unbefugtes Eindringen in die angeschlossenen Computer.

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

k) Bluetooth ist ein Verfahren zur Kopplung elektronischer Geräte übereinander über Funk, zum Beispiel Freisprechanlagen mit Mobiltelefon.

l) Bei approved circuits handelt es sich um Leitungen, die durch besondere Maßnahmen so geschützt sind, dass ein unberechtigter Zugriff („Anzapfen“) erkennbar ist.

3. Geheimhaltungsgrade

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

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

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

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

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

4. Allgemeine Grundsätze

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

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

4.3 Der Bedrohung der VS durch Verlust der Vertraulichkeit, Verfügbarkeit und Integrität ist mit Schutzmaßnahmen entsprechend dem Stand der Technik entgegenzuwirken. Diese sind entsprechend Anlage 5 zu dokumentieren.

5. Verantwortung und Zuständigkeit

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

5.2 Die obersten Staatsbehörden bestellen, wenn sie mit VS-VERTRAULICH oder höher eingestuften VS arbeiten, gemäß § 3 Abs. 7 SächsSÜG einen Geheimschutzbeauftragten oder eine Geheimschutzbeauftragte sowie eine zur Vertretung berechtigte Person. Andere VS-verwaltende Dienststellen können Geheimschutzbeauftragte bestellen. Soweit keine Geheimschutzbeauftragten bestellt wurden, nehmen die Dienststellenleiter die Aufgaben der Geheimschutzbeauftragten wahr.

5.3 Geheimschutzbeauftragte haben in den Dienststellen für die Durchführung der VSA zu sorgen und die Dienststellenleiter in allen Fragen des Geheimschutzes zu beraten.

5.4 Geheimschutzbeauftragte haben ein unmittelbares Vortragsrecht bei den Dienststellenleitern.

5.5 Dienststellen, die VS mit Informationstechnik (IT) verarbeiten, können verantwortliche Personen mit IT-Fachkenntnissen (zum Beispiel IT-Sicherheitsbeauftragte) zur Unterstützung der Geheimschutzbeauftragten bei der Umsetzung der VS-Anweisung bestimmen. Die IT-Sicherheitsbeauftragten sollen nicht zugleich Aufgaben von Systemadministratoren bei für VS eingesetzten IT-Systemen wahrnehmen und müssen in Bezug auf die VSA besonders geschult sein. Werden Verantwortliche mit IT-Fachkenntnissen für Geheimschutzmaßnahmen nicht bestimmt, so verbleiben deren Aufgaben bei den Geheimschutzbeauftragten oder der Dienststellenleitung.

6. Geheimschutzdokumentation

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

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

6.3 Die Dokumentation kann elektronisch geführt werden. Sofern die Arbeit mit VS persönlich zugeordnet werden muss, sind entsprechende technische Maßnahmen nach Nummer 18.2 zu treffen. Diese müssen eine sichere Zuordnung zur Person erlauben und können insbesondere mittels fortgeschrittener oder qualifizierter elektronischer Signatur erfolgen.

7. Mitwirkung des Landesamtes für Verfassungsschutz

Bei der Durchführung der VSA wirkt das Landesamt für Verfassungsschutz (LfV) mit. Es berät Dienststellen, die mit VS arbeiten. Eine Verarbeitung personenbezogener Daten findet dabei nicht statt. Die Mitwirkung umfasst bei Bedarf auch technische Prüfungen und Schulungen. Das LfV kann sich zu seiner Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bedienen. Die Mitwirkung des LfV erfolgt kostenlos. Die für eine Unterstützung durch das BSI entstehenden Kosten sind von der auftraggebenden Stelle zu tragen.

II. Behandlung von VS und organisatorische Maßnahmen

8. Einstufung in Geheimhaltungsgrade

8.1 Die VS herausgebende Stelle bestimmt über die Notwendigkeit der VS-Einstufung und den Geheimhaltungsgrad. Von einer Einstufung als VS ist nur Gebrauch zu machen, soweit dies notwendig ist. Zu beachten sind die Nummern 9.1 und 9.2 sowie die Hinweise zur Einstufung von VS in Anlage 1.

8.2 Zur Arbeitserleichterung und einheitlichen Praxis kann die Dienststellenleitung Richtlinien zur Einstufung von VS für häufiger vorkommende Fälle festlegen.

9. Änderung und Aufhebung der VS-Einstufung

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

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

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

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

b) Die Verlängerung der Frist kann für einzelne VS oder pauschal für die in einem bestimmten Bereich entstehenden VS verfügt werden. Sie bedarf der Zustimmung der zuständigen obersten Landesbehörde.

c) Auf der ersten Seite des Entwurfs der VS und auf allen Ausfertigungen ist ein Hinweis auf die verlängerte Frist anzugeben: „Die VS-Einstufung endet mit Ablauf des Jahres&...“. Bei anderen Darstellungsformen von VS, beispielsweise von Geräten, ist sinngemäß zu verfahren, zum Beispiel Kennzeichnung in der zugehörigen Dokumentation.

d) Die nachträgliche Fristverlängerung ist als Änderung entsprechend Nummer 9.1 zu behandeln. Befinden sich die VS im Staatsarchiv, ist auch dieses entsprechend zu benachrichtigen.

9.4 Nummer 9.3 gilt nicht für VS-Einstufungen ausländischer und zwischenstaatlicher Stellen. Ihre VS-Einstufung kann nur von der herausgebenden Stelle geändert oder aufgehoben werden, sofern nicht zwischenstaatliche Vereinbarungen ein abweichendes Verfahren regeln.

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

10.1 VS-VERTRAULICH oder höher eingestufte VS dürfen Dritten nur mit Zustimmung der zuständigen Organisationseinheit, beispielsweise dem Referat oder der Abteilung, zugänglich gemacht werden.

10.2 In Räumen, in denen VS-VERTRAULICH oder höher eingestufte VS verwaltet werden, wie der VS-Registratur, dürfen nur Personen tätig sein, die entsprechend ermächtigt sind.

10.3 Bevor eine Person Zugang zu VS-VERTRAULICH oder höher eingestuften VS erhält, ist sie gemäß dem Sächsischen Sicherheitsüberprüfungsgesetz und der Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Ausführung des Sächsischen Sicherheitsüberprüfungsgesetzes (VwVSächsSÜG) vom 7. Juni 2004 SächsABl. S. 594) zu überprüfen und zum Zugang zu VS zu ermächtigen. Zugang zu solchen VS haben Personen, die diese bearbeiten oder anderweitig Kenntnis von ihrem Inhalt erhalten.

10.4 Bevor einer Person eine Tätigkeit übertragen wird, bei der sie sich Zugang zu VS-VERTRAULICH oder höher eingestuften VS verschaffen kann, muss sie gemäß dem Sächsischen Sicherheitsüberprüfungsgesetz und der Verwaltungsvorschrift zur Ausführung des Sächsischen Sicherheitsüberprüfungsgesetzes überprüft und für eine solche Tätigkeit zugelassen worden sein. Zugang zu VS können sich Personen verschaffen, die

a) als Boten oder Kuriere VS befördern,

b) VS-Verwahrgelasse oder Sicherheitsbereiche bewachen,

c) in einem Sicherheitsbereich tätig sind,

d) Alarmanlagen zum Schutze von VS installieren, warten oder instand setzen,

e) Schlüssel oder Zahlenkombinationen zu VS-Verwahrgelassen, VS-Schlüsselbehältern oder Alarmanlagen zum Schutze von VS verwalten,

f) im Rahmen ihrer Tätigkeit an technischen Systemen oder Komponenten, die für die Verarbeitung von VS-VERTRAULICH oder höher eingestuften VS eingesetzt sind, wesentliche Maßnahmen zum Geheimschutz unwirksam machen oder unbefugten Zugriff auf diese VS erlangen können.

11. Ermächtigungen und Zulassungen

11.1 Ermächtigungen und Zulassungen sowie ihre Erweiterung, Einschränkung oder Aufhebung nehmen die Dienststellenleitung oder in deren Auftrag die Geheimschutzbeauftragten vor. Ermächtigungen und Zulassungen sind auf das notwendige Maß zu beschränken. Sie erlöschen spätestens mit Ausscheiden der betroffenen Person aus der Dienststelle. Die VS-Registratur ist über Ermächtigungen und Zulassungen sowie deren Erweiterung, Einschränkung, Aufhebung oder Erlöschen in dem erforderlichen Umfang zu unterrichten.

11.2 Die ermächtigten oder für eine Tätigkeit nach Nummer 10.4 zugelassenen Personen sind über die wesentlichen Geheimschutzbestimmungen, Anbahnungs- und Anwerbemethoden fremder Nachrichtendienste und sonstige Gefährdungen sowie über die Möglichkeiten straf- und disziplinarrechtlicher Ahndung oder arbeitsrechtlicher Maßnahmen bei Verstößen gegen die Geheimhaltungsvorschriften zu unterrichten. Die Unterrichtung ist mindestens alle fünf Jahre zu wiederholen. Den ermächtigten Personen sind gegen Empfangsbestätigung die für ihre Tätigkeit erforderlichen Vorschriften zum Schutze von VS auszuhändigen oder anderweitig zugänglich zu machen.

11.3 Die in den Nummern 11.1 und 11.2 genannten Maßnahmen sind zu dokumentieren, wie im Muster nach Anlage 3 oder elektronisch. Sie sind, soweit die Dienststellenleiter persönlich betroffen sind, von der vorgesetzten Behörde durchzuführen.

12. Veränderungen von Ermächtigungen und Zulassungen

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

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

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

13. Allgemeine Dienstpflichten zum Schutz von VS

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

13.2 Niemand darf sich zur Preisgabe von VS an andere Personen verleiten lassen, wenn diese sich über den Vorgang unterrichtet zeigen.

13.3 Personen, die zum Zugang zu VS ermächtigt sind oder eine Tätigkeit ausüben, bei der sie sich Zugang zu VS verschaffen können (Nummer 10.4), ist der Betrieb von privaten Bild- und Tonaufzeichnungsgeräten, privater Informationstechnik und privaten mobilen Telekommunikations-Endgeräten, wie beispielsweise Mobiltelefone, Datenträger, PDA, 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.

14. Herstellung von VS

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

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

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

15. Vervielfältigung von VS

15.1 Für Vervielfältigungen, wie Kopien, Abdrucke, Abschriften, Auszüge, Nachbauten, gilt Nummer 14 sinngemäß.

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

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

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

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

15.6 Bei Benutzung von Kopiergeräten und Multifunktionsgeräten mit nichtflüchtigem Speicher sind die Festlegungen gemäß Nummer 26.4 zu berücksichtigen. Das LfV sollte bei Bedarf beratend hinzugezogen werden.

16. Kennzeichnung von VS

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

16.2 Bei der Darstellung von VS auf Sichtgeräten soll sich der Geheimhaltungsgrad auf jeder Dokumentenseite deutlich vom dargestellten Inhalt abheben, wie durch größere Schrift und Fettdruck. Nummer 16.1 gilt entsprechend.

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

16.4 Lässt die Beschaffenheit einer VS die Kennzeichnung nach den Nummern 16.1 bis 16.3 nicht zu, beispielsweise bei miniaturisierten Bauelementen, ist sinngemäß zu verfahren oder die Kennzeichnung auf der zugehörigen Dokumentation zu vermerken.

16.5 VS-Zwischenmaterial, das nicht an Dritte weitergegeben und das unverzüglich vernichtet wird, braucht nicht als VS gekennzeichnet und nicht nachgewiesen werden.

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

16.7 Für die Kennzeichnung ausländischer oder zwischenstaatlicher VS-Einstufungen ist Anlage 4 zu berücksichtigen.

17. Aufbewahrung von VS

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

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

17.3 VS-Verwahrgelasse sind Stahlschränke, Aktensicherungsräume und Ähnliches, die besonderen

Sicherheitsanforderungen entsprechen. Näheres über VS-Verwahrgelasse, ihre Bewachung oder technische Überwachung bestimmen die Nummern 30 ff.

17.4 Außerhalb der Arbeitszeit sind diese VS-Verwahrgelasse zu bewachen oder durch eine Alarmanlage technisch zu überwachen. Bei GEHEIM oder VS-VERTRAULICH eingestuften VS kann eine Bewachung beziehungsweise technische Überwachung des VS-Verwahrgelasses unterbleiben, wenn das Gebäude oder der Gebäudeteil, in dem sich das Verwahrgelass befindet, ständig bewacht oder technisch überwacht ist und die VS nur vorübergehend in dem VS-Verwahrgelass aufbewahrt werden.

17.5 Ist eine Aufbewahrung nach den Nummern 17.2 und 17.3 nicht möglich, so sind die VS bei einer anderen Dienststelle unterzubringen, welche die erforderlichen Voraussetzungen erfüllt. Außer bei STRENG GEHEIM eingestuften VS ist die Aufbewahrung in einem Bankschließfach zulässig, wenn sichergestellt ist, dass nur befugte Personen der Dienststelle dazu Zugang erhalten.

17.6 Bei GEHEIM oder VS-VERTRAULICH eingestuften VS kann auf Antrag der Dienststellenleitung die oberste zuständige Staatsbehörde zulassen, dass von der vorgeschriebenen Bewachung beziehungsweise technischen Überwachung abgewichen wird, wenn die damit verbundenen Maßnahmen unangemessen wären. Bei GEHEIM eingestuften VS muss in diesem Fall jedoch mindestens sichergestellt sein, dass ein unbefugter Zugriff auf das VS-Verwahrgelass unmittelbar erkennbar ist.

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

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

18. Nachweis von VS-VERTRAULICH oder höher eingestuften VS

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

18.2 Die Führung dieser Nachweise kann auch in elektronischer Form entsprechend Nummer 6.3 erfolgen. Hierbei sollen möglichst vom BSI zugelassene Registratursysteme eingesetzt werden. Zur Beweissicherung sind mindestens folgende Angaben automatisch revisionssicher zu protokollieren:

a) Zugriffe auf die VS-Daten,

b) Abgewiesene Zugangs- und Zugriffsversuche,

c) Übertragung von VS-Daten über Leitungen.

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

18.3 VS-Datenträger, ihr Verbleib und ihre Vernichtung sind in einem gesonderten VS-Bestandsverzeichnis nachzuweisen. Zur Erfassung genügen die Angabe eines Ordnungskriteriums, wie fortlaufende Nummern, sowie des Einsatzbereichs (Organisationseinheit, IT-Nutzer) und eine Kurzangabe des Aufgabengebietes. VS-Datenträger sind grundsätzlich nur gegen Quittung weiterzugeben. Mehrere auf einem Datenspeicher gespeicherte VS-VERTRAULICH oder höher eingestufte VS, die nicht weitergegeben werden, brauchen nicht einzeln nachgewiesen werden.

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

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

18.6 Auf Datenträgern vorliegende Sicherheitskopien von VS sind wie die ursprüngliche VS im Sinne dieser VSA zu behandeln, Schlüssel für die Kryptierung sind getrennt zu speichern.

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

19.1 VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS sowie offene Akten und Vorgänge können,

soweit sie nicht Bestandteil höher eingestufter VS sind, von diesen getrennt verwaltet und aufbewahrt werden.

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

19.3 Weiteres zur Arbeit mit VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS kann dem als Anlage 7 beigefügten VS-NfD-Merkblatt entnommen werden.

20. Verwaltungspersonal

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

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

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

20.4 Bei vorübergehender Vertretung von VS-Verwaltern, wie bei Urlaub oder Krankheit, ist nach Nummer 20.3 Satz 1 zu verfahren. Es reicht aus, die Übergabe aktenkundig zu machen.

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

21. Grundsätze zu Weitergabe und Versand von VS

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

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

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

21.4 Für die Weitergabe von VS an Unternehmen gilt Folgendes:

a) Den Geheimschutz im Bereich der Wirtschaft regelt das Bundesministerium für Wirtschaft und Technologie. Zuständige Landesbehörde ist gemäß § 26 Abs. 1 SächsSÜG das Staatsministerium für Wirtschaft und Arbeit, soweit nicht die Zuständigkeit des Bundesministeriums für Wirtschaft und Technologie gegeben ist.

b) Vor Weitergabe VS-VERTRAULICH oder höher eingestufter VS sind Sicherheitsbescheide über die beteiligten Unternehmen anzufordern.

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

d) Bei VS-NUR FÜR DEN DIENSTGEBRAUCH genügt es, das VS-NfD-Merkblatt gemäß Anlage 7 zum Vertragsbestandteil zu machen oder die Privatperson auf diese Bestimmungen hinzuweisen.

21.5 Vorzimmerberechtigte sollen VS-VERTRAULICH oder höher eingestufte VS grundsätzlich persönlich entgegennehmen. Die Geheimschutzbeauftragten können mit Zustimmung der

zuständigen obersten Landesbehörde Ausnahmen zulassen, so zum Beispiel bei hohem Aufkommen an VS die Annahme durch Vorzimmerkräfte erlauben, wenn der Vorzimmerberechtigte anwesend ist und die VS bis zur Übergabe in persönlichem Gewahrsam oder nach Nummer 17.2 aufbewahrt wird. Die Ausnahmeregelung ist in der Geheimschutzdokumentation nachzuweisen.

21.6 Zu Weitergabe und Versand von VS sind im Übrigen die Hinweise der Anlage 6 zu beachten.

22. Eingehende Sendungen

22.1 Elektronisch oder postalisch eingehende Sendungen mit VS-VERTRAULICH oder höher eingestuften VS sind der VS-Registratur umgehend zuzuleiten. Jede Sendung ist zu prüfen, ob sie unbeschädigt und vollständig ist. Zeigen sich Spuren unbefugter Kenntnisnahme oder ist die Sendung unvollständig, so sind die Geheimschutzbeauftragten und die Absender unverzüglich zu benachrichtigen.

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

22.3 Bei elektronischer Übermittlung von VS genügt eine elektronische Empfangsbestätigung. Sofern mehrere VS übermittelt werden oder auf Datenträgern eingehen, sind diese einzeln nachzuweisen, beispielsweise in einem Verzeichnis der Dateinamen oder als Telefax-Sendebericht.

23. Weitergabe von VS an Empfänger außerhalb des Bundesgebietes

23.1 Die Weitergabe von deutschen VS an Dienststellen ausländischer Staaten und internationaler Organisationen setzt ein Geheimschutzabkommen beziehungsweise Geheimschutzübereinkommen voraus, das die Bestimmungen für den Austausch regelt. Hinweise zur Kennzeichnung nichtdeutscher VS enthält Anlage 4.

23.2 VS-VERTRAULICH oder höher eingestufte VS an Dienststellen ausländischer Staaten sind durch den Kurierdienst des Auswärtigen Amtes zur zuständigen Auslandsvertretung der Bundesrepublik Deutschland zu versenden; ist diese nicht selbst Empfängerin, so ist sie um sichere Weiterleitung an die Dienststellen der ausländischen Staaten zu ersuchen. Das nähere Verfahren regelt Anlage 6 Nr. 5.

23.3 VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS von und zu deutschen Auslandsvertretungen sind ebenfalls durch den Kurierdienst des Auswärtigen Amtes zu versenden. Sendungen an andere Stellen im Ausland können mit der Deutschen Post AG oder einem anderen privaten Zustelldienst versandt werden.

24. Mitnahme von VS außerhalb des Dienstgebäudes

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

24.2 Die Mitnahme von VS auf Dienstreisen und zu Konferenzen, Sitzungen, Besprechungen und so weiter außerhalb des Dienstgebäudes beziehungsweise einer geschlossenen Gebäudegruppe ist auf notwendige Fälle zu beschränken. Die Regelungen der Anlage 6 Nr. 3 gelten entsprechend. Sie bedarf bei STRENG GEHEIM oder GEHEIM, bei Auslandsdienstreisen auch bei VS-VERTRAULICH eingestuften VS der Genehmigung des Dienststellenleiters, bei den obersten Staatsbehörden sowie den allgemeinen und besonderen Staatsbehörden des zuständigen Abteilungsleiters.

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

24.4 Nach außerhalb des Bundesgebietes sind VS-VERTRAULICH oder höher eingestufte VS möglichst an die zuständige Auslandsvertretung voraus zu senden und nach Erledigung des Dienstgeschäftes durch diese zurückzusenden. Ist dies nicht möglich, so versiegelt das Auswärtige Amt oder die zuständige Auslandsvertretung die verpackten VS und stellt eine Bescheinigung aus, nach der ihr Inhaber zur Mitnahme des versiegelten Stückes als „Kuriergepäck“ berechtigt ist. Die VS sind ständig in persönlichem Gewahrsam zu halten oder bei der Auslandsvertretung zu hinterlegen. Die persönliche Mitnahme ist ohne Mitwirkung des Auswärtigen Amtes gestattet, wenn sich die VS auf einem vom BSI zugelassenen IT-System oder

einem entsprechend geschützten VS-Datenträger befinden. Die persönliche Mitnahme von STRENG GEHEIM eingestuften VS im grenzüberschreitenden Verkehr ist unzulässig. In besonderen Fällen können die Geheimschutzbeauftragten Ausnahmen zulassen.

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

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

25. Erörterung von VS in Konferenzen, Sitzungen, Besprechungen und so weiter

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

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

25.3 Vor Beginn der Konferenz, Sitzung, Besprechung und so weiter hat die Veranstaltungsleitung auf die Geheimhaltungsbedürftigkeit der Erörterungen hinzuweisen und sich zu vergewissern, dass alle teilnehmenden Personen ausreichend ermächtigt sind. Aufzeichnungen bedürfen der Genehmigung und sind gegebenenfalls als VS zu behandeln. Das Mitführen von Bild- und Tonaufzeichnungsgeräten, mobilen Telekommunikationsendgeräten, wie Mobiltelefone, PDA, und sonstiger Informationstechnik soll von der Veranstaltungsleitung vorher erlaubt oder untersagt werden.

25.4 Bei Erörterung von STRENG GEHEIM oder GEHEIM eingestuften VS sollen, soweit vorhanden, abhörsichere oder abhörgeschützte Räume benutzt werden. Vor Konferenzen auf hoher Ebene oder von besonderer Bedeutung ist bezüglich notwendiger Abhörschutzmaßnahmen das LfV rechtzeitig beratend hinzuzuziehen.

III. Aussonderung von VS

26. Grundsätze der Aussonderung von VS

26.1 Nicht mehr benötigte VS sind aus dem Bestand der Dienststelle zur Archivierung oder Vernichtung nach den Nummern 27 und 28 auszusondern.

26.2 Zugelassenes Kryptomaterial (Geräte, Schlüssel) ist unter Mitwirkung des LfV auszusondern.

26.3 Bei Aussonderung von Gerätschaft zur weiteren Verwendung außerhalb des VS-Bereichs sind VS auf enthaltenen nichtflüchtigen Speichern, wie Festplatten, entsprechend Nummer 28 zu vernichten.

27. Archivierung von VS

Die Archivierung von VS richtet sich nach den Maßgaben des Archivgesetzes für den Freistaat Sachsen (SächsArchivG) vom 17. Mai 1993 (SächsGVBl. S. 449), in der jeweils geltenden Fassung.

28. Vernichtung von VS

28.1 VS, die das zuständige Archiv nicht übernimmt, sind zu vernichten. Stehen VS zur Vernichtung an, sind diese so zu vernichten, dass ihr Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.

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

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

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

Aufsicht bedarf es nicht.

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

IV. Materielle und technische Maßnahmen

29. Räumliche Sicherheitsmaßnahmen

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

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

29.3 Sofern Umfang und Bedeutung der VS es erfordern, sind mit Zustimmung der zuständigen obersten Staatsbehörde 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.

29.4 Für VS-IT-Räume gilt die Zustimmung der zuständigen obersten Staatsbehörde nach Nummer 29.3 als gegeben.

29.5 Die in einem Sicherheitsbereich tätigen Personen sind beim Betreten des Sicherheitsbereiches anhand des Dienstausweises oder auf andere geeignete Weise zu identifizieren. Besucher sind nach Identitätsfeststellung während des Aufenthalts im Sicherheitsbereich zu beaufsichtigen. Bei Besuchern, die nachweislich, zum Beispiel durch eine Konferenzbescheinigung nach Anlage 3, Muster 9, nach dem Sächsischen Sicherheitsüberprüfungsgesetz und der Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Ausführung des Sicherheitsüberprüfungsgesetzes überprüft sind, kann die Beaufsichtigung entfallen. Fremdpersonal, wie Handwerker, Reinigungskräfte, ist gemäß dem Sächsischen Sicherheitsüberprüfungsgesetz und der Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Ausführung des Sächsischen Sicherheitsüberprüfungsgesetzes zu überprüfen und, soweit erforderlich, zu beaufsichtigen. In Ausnahmefällen genügt eine Beaufsichtigung.

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

29.7 Verfügt eine Dienststelle über einen Sicherheitsbereich nach Nummer 29.3, sollen (soweit erforderlich) abhörgeschützte und abhörsichere Besprechungsräume möglichst in diesem Sicherheitsbereich eingerichtet werden.

30. Technische Sicherung von VS

30.1 Technische Mittel zur Sicherung von VS müssen vom BSI auf die Erfüllung der in Nummer 30.2 genannten Anforderungen geprüft und für geeignet befunden worden sein. Das LfV berät die Dienststellen und erteilt Auskünfte zu technischen Mitteln, welche die in Nummer 30.2 genannten Anforderungen erfüllen oder einen vergleichbaren Schutz bieten.

30.2 Die nachstehend genannten technischen Mittel zur Sicherung von VS müssen folgenden Anforderungen entsprechen:

a) VS-Verwahrgelasse und VS-Schlüsselbehälter müssen so beschaffen sein, dass

aa) ein Zugang einer Person zum Inhalt erst nach deren zuverlässiger Identifizierung/Authentisierung durch Besitz und Wissen möglich ist; Besitz, zum Beispiel Schlüssel, soll gegen Nachfertigung durch Unbefugte geschützt sein; anstelle von Besitz oder Wissen oder ergänzend können auch biometrische Merkmale genutzt werden;

bb) ein Zugriff Unbefugter auf den Inhalt erkennbar wird und

cc) ein angemessener Schutz gegen gewaltsamen Zugriff auf den Inhalt gegeben ist.

b) Alarmanlagen müssen so beschaffen und installiert sein, dass

aa) sie einen Eindringling sicher erkennen,

bb) sie erst nach zuverlässiger Identifizierung/Authentisierung einer Person durch

Besitz und Wissen durch diese unscharf geschaltet werden können; anstelle von Besitz oder Wissen oder ergänzend können auch biometrische Merkmale genutzt werden;

cc) der Alarm sicher zu der zu alarmierenden Stelle übertragen wird und

dd) die Alarmanlage nicht unbemerkt überwunden werden kann.

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

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

30.3 Die Dienststelle hat zu veranlassen, dass die zum Schutz von VS eingesetzten technischen Mittel bei der Planung beziehungsweise erstmaligen Nutzung von VS-Aktensicherungsräumen und Alarmanlagen zum Schutz von VS grundsätzlich sowie darüber hinaus gelegentlich stichprobenweise und bei Manipulationsverdacht durch das LfV auf korrekte Ausführung und mögliche Manipulation überprüft werden. Nummer 30.1 gilt entsprechend.

30.4 In Wiederanlauf-Vorkehrungen bei größeren IT-Systemen sind die erforderlichen Geheimschutzmaßnahmen einzubeziehen.

31. Bewachung und technische Überwachung von VS

31.1 Die Bewachung eines

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

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

31.2 Die technische Überwachung eines

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

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

31.3 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.

32. Abhörschutzmaßnahmen

32.1 Das Staatsministerium des Innern legt die Dienststellen fest, in denen aufgrund des Umfangs und der Bedeutung von VS sowie der Aufgabenstellung eine besondere Abhörgefahr besteht. Bei Dienststellen nach Nummer 45 gilt die besondere Abhörgefahr als gegeben.

32.2 Dienststellen nach Nummer 32.1 haben Vorkehrungen zu treffen, damit ihre Telekommunikations- und Informationstechnik nicht dazu missbraucht werden kann, um Raum- und Telefongespräche abzuhören.

32.3 In Dienststellen nach Nummer 32.1 legen die Geheimschutzbeauftragten die Räume fest, in denen aufgrund des Umfangs und der Bedeutung der dort geführten Gespräche eine besondere Abhörgefahr besteht. Bei Räumen, in denen nicht nur ausnahmsweise Gespräche mit GEHEIM oder STRENG GEHEIM eingestuftem Inhalt geführt werden, gilt die besondere Abhörgefahr als gegeben.

32.4 Räume nach Nummer 32.3 müssen abhörgeschützt und abhörsicher sein. Diese Räume müssen mindestens

a) vor unbemerktem Zutritt Unbefugter geschützt sein,

b) eine akustische Dämpfung aufweisen, die ein Mithören von außen ohne technische Hilfsmittel hinreichend ausschließt,

c) bei Ausstattung mit Kommunikationseinrichtungen Vorkehrungen enthalten, damit Raumgespräche nicht über diese Einrichtungen abgehört werden können,

d) so gestaltet sein (Einrichtungen, Installationen), dass Versteckmöglichkeiten für Abhörgeräte nach Möglichkeit beschränkt sind und technische Prüfungen nach

Nummer 32.5 wirksam und in angemessener Zeit durchgeführt werden können und

e) Vorkehrungen enthalten, damit Leitungen, die in diese Räume führen, nicht für Abhörzwecke missbraucht werden können.

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

32.5 In Dienststellen nach Nummer 32.1 sind nach Fertigstellung und anschließend regelmäßig sowie bei Manipulationsverdacht technische Prüfungen durchzuführen, um festzustellen, ob

a) Telekommunikations- oder IT-Einrichtungen für Abhörzwecke missbraucht werden können oder

b) in den Räumen nach Nummer 32.3 Abhöreinrichtungen vorhanden sind und

c) die Anforderungen der Technischen Leitlinien nach Nummer 32.8 erfüllt sind.

32.6 Bei Abhörverdacht oder aus Anlass von Konferenzen auf höherer Ebene oder von besonderer Bedeutung sollen ebenfalls technische Prüfungen nach Nummer 32.5 durchgeführt werden. In diesem Fall ist der Umfang der Prüfung mit den Geheimschutzbeauftragten oder sonstigen Verantwortlichen in Abhängigkeit von den örtlichen und zeitlichen Gegebenheiten und der spezifischen Bedrohungslage abzustimmen.

32.7 Für die nach den Nummern 32.5 und 32.6 geforderten technischen Prüfungen haben die Dienststellen die für die Prüfungen erforderliche Unterstützung zu gewähren.

32.8 Zu Sicherheitsvorgaben für abhörsichere und abhörgeschützte Räume sowie Konferenzen auf höherer Ebene oder von besonderer Bedeutung und zur Umsetzung der Abhörschutzmaßnahmen ist auf die Beratung des LfV auf der Grundlage der vom BSI herausgegebenen Technischen Leitlinien zurückzugreifen.

33. Sicherung von Schlüsseln und sonstigen Zugangsmitteln zu VS

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

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

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

33.4 Bei der Vergabe, Änderung und Rücknahme von Rechten muss gewährleistet sein, dass

a) ein dazu erforderlicher Antrag von einer berechtigten Stelle stammt,

b) die zu berechtigende Person eine ausreichende VS-Ermächtigung besitzt,

c) der Grundsatz „Kenntnis nur, wenn nötig“ beachtet wird und

d) keine bezüglich der Sicherheit unvereinbare Bündelung von Funktionen entsteht.

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

33.5 Die Verwendung gegenständlicher Zugangsmittel zu IT-System und Komponenten, wie Magnet- und Chip-Karten, Dongel, Lochstreifen, sowie Einzelheiten über die Auswahl, Vergabe, Kontrolle und den Wechsel von Kennworten oder persönlichen Identifikationsnummern (PIN) sollen in einer Dienstanweisung festgelegt sein.

34. Zahlenkombinationen als Zugangsmittel zu VS

34.1 Die Zahlenkombination zum Zugang eines VS-Verwahrgelasses oder VS-Schlüsselbehälters oder zum Ein- und Ausschalten einer Alarmanlage darf nur dem Benutzer bekannt sein. Sie darf nicht aus leicht zu ermittelnden Zahlen oder Zusammenstellungen, wie beispielsweise persönlichen Daten, Fernsprechnummern oder arithmetischen Reihen, bestehen.

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

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

a) nach Beschaffung,

b) bei Wechsel der Benutzer,

c) nach Öffnung in Abwesenheit der Benutzer,

d) wenn der Verdacht besteht, dass die Zahlenkombination Unbefugten bekannt geworden ist,

e) regelmäßig alle 12 Monate oder häufiger.

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

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

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

35. Planung, Beschaffung und Abnahmeprüfung

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

35.2 Bei der Planung und Durchführung von Baumaßnahmen sind rechtzeitig die notwendigen Geheimschutzvorkehrungen zu treffen. Hierbei sollte das LfV beratend hinzugezogen werden.

35.3 Bei der Planung und Abnahmeprüfung von VS-Aktensicherungsräumen, Alarmanlagen zum Schutz von VS. Telekommunikationsanlagen und abhörsicheren oder abhörgeschützten Räumen ist das LfV beratend hinzuzuziehen.

35.4 Ist geplant, IT für VS einzusetzen, so sind die Geheimschutzbeauftragten und deren Verantwortliche mit IT-Fachkenntnissen bereits zu Planungsbeginn zu beteiligen. Bei komplexen IT-Systemen oder besonderen IT-Anwendungen für VS sollte das LfV bereits bei Planungsbeginn beratend hinzugezogen werden.

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

a) Produkte mit IT-Sicherheitsfunktionen die erforderliche Zulassung aufweisen und sicherheitsgerecht implementiert werden,

b) Produkte mit IT-Sicherheitsfunktionen ab dem Zeitpunkt, zu dem feststeht, dass sie für VS eingesetzt werden sollen, geschützt aufbewahrt und transportiert werden,

c) eine sicherheitsgerechte Wartung und Instandsetzung erfolgt,

d) bei Vergabe des IT-Einsatzes an Dritte die erforderlichen Geheimschutzmaßnahmen erfolgen.

V. IT-spezifische Maßnahmen

36. Freigabe und Betrieb von IT-Systemen

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

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

dokumentieren.

36.3 Geheimschutzrelevante Änderungen bei freigegebenen IT-Systemen, insbesondere der Einsatz für höher eingestufte VS, bedürfen der vorherigen Zustimmung der zuständigen Geheimschutzbeauftragten. Die Nummern 36.1 und 36.2 gelten entsprechend.

36.4 Für den Betrieb der IT-Systeme gelten die Nummern 4.3 und 18.2 sinngemäß.

37. Produkte mit IT-Sicherheitsfunktionen zur Verwendung für VS

37.1 Produkte mit Funktionen zur

a) Herstellung von Schlüsselmitteln,

b) Verschlüsselung (Kryptierung),

c) Löschung oder Vernichtung von VS-Datenträgern

d) Abstrahlsicherheit oder

e) Sicherung von Übertragungsleitungen,

f) Trennung von Netzen mit unterschiedlichen maximalen Einstufungen der verarbeiteten VS

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

37.2 Produkte mit Funktionen zur

a) Zugangs-/Zugriffskontrolle zu den Systemen,

b) Erstellung von VS,

c) Protokollierung/Beweissicherung und Protokollauswertung oder

d) Abwehr von Manipulationen an IT-Systemen,

e) Registratur und zum Bestandsnachweis,

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

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

a) in Räumen nach Nummer 29.1 oder entsprechend geschützten Räumen aufzubewahren,

b) unter ständiger Kontrolle von nach den Nummern 10.3 und 10.4 ermächtigtem oder zugelassenem Personal zu transportieren oder so zu verpacken, dass ein Zugriff Unbefugter erkennbar wird,

c) durch nach den Nummern 10.3 und 10.4 ermächtigtes oder zugelassenes Personal zu installieren, zu warten und instand zu setzen, soweit nicht durch organisatorische Maßnahmen, zum Beispiel keine Verarbeitung oder Übertragung von VS in Anwesenheit der Personen oder Beaufsichtigung derselben, ein Zugang zu VS auszuschließen ist, und

d) in einem Bestandsverzeichnis nachzuweisen.

38. Abstrahlsicherheit

38.1 IT-Hardware, die VS-VERTRAULICH oder höher eingestufte VS unkryptiert führt, soll unter Beachtung der Hinweise des BSI zur Abstrahlsicherheit installiert sein. Das LfV sollte beratend hinzugezogen werden.

38.2 Durch die Geheimschutzbeauftragten ist zu prüfen, inwieweit mit einer erheblichen Gefährdung der Geheimhaltung von VS-VERTRAULICH oder höher eingestuften VS durch Nutzung von kompromittierender Abstrahlung durch Unbefugte zu rechnen ist. Ist mit einer erheblichen Gefährdung zu rechnen, so muss die IT-Hardware in vom BSI zugelassenen abstrahlsicheren Räumen betrieben werden, eine Zulassung des BSI für den Betrieb innerhalb einer bestimmten Sicherheitszone (Zonenmodell) aufweisen und innerhalb einer solchen betrieben werden oder vom BSI als abstrahlsicher zugelassen sein. Das LfV sollte beratend hinzugezogen werden. Die Entscheidung trifft die Dienststellenleitung.

39. Technische Prüfungen

39.1 Geheimschutzbeauftragte haben bei IT-Systemen, die für STRENG GEHEIM oder nicht nur

ausnahmsweise für GEHEIM eingestufte VS eingesetzt werden, vor dem erstmaligen Einsatz für VS und danach in angemessenen zeitlichen Abständen unter Beteiligung des LfV folgende technische Prüfungen durch das BSI zu veranlassen:

a) eine Prüfung des IT-Systems unter den spezifischen Einsatzbedingungen, ob die erforderlichen IT-Sicherheitsfunktionen sachgerecht implementiert sind, keine erkennbaren Manipulationen aufweisen und auch nach Implementierung in das jeweilige IT-System wirksam greifen, nicht über einen Systemweg manipuliert oder umgangen werden können und auch bei einem Verbund mit anderen IT-Systemen diese Sicherheit aufweisen,

b) Abstrahlsicherheits- und Manipulationsprüfungen bei abstrahlsicheren Räumen/Behältern, bei zonenvermessenen Räumen und bei für VS eingesetzter Hardware und

c) eine Überprüfung von Sicherheitszonen auf mögliche Einrichtungen zur Erfassung oder Übertragung kompromittierender Nahbereichsabstrahlung.

39.2 Die Ergebnisse werden den Geheimschutzbeauftragten durch das BSI über das LfV mitgeteilt.

39.3 Bei vernetzten IT-Systemen, die für VS eingesetzt werden, ist in den Dienststellen nach Nummer 5.3 durch die Geheimschutzbeauftragten ein Penetrationstest zu veranlassen.

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

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

40.2 Abweichend von Nummer 40.1 Satz 1 ist in folgenden Fällen eine unkryptierte Übertragung zulässig:

a) wenn die Erledigung der Angelegenheit dringlich ist und die schriftliche oder sonstige sichere Übermittlung einen unvertretbaren Zeitverlust bedeuten würde, kann

   aa) bei Telefongesprächen mit VS-VERTRAULICH eingestuftem Inhalt eine für VS-NUR FÜR DEN DIENSTGEBRAUCH zugelassene Verbindung nach Absatz 1 Satz 1 und

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

   verwendet werden. Die Gespräche sind möglichst so zu führen, dass der Sachverhalt Dritten nicht verständlich wird. Ist der Gesprächspartner nicht mit Sicherheit zu identifizieren, ist ein Kontrollanruf erforderlich. Besondere Vorsicht ist bei Funkfernsprechanschlüssen, wie Mobilfunk, DECT oder Bluetooth, geboten.

b) bei dringlichen E-Mails, Fernkopien und Fernschreiben des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn zwischen Absender und Empfänger für die erforderliche Übertragungsart keine Kryptiermöglichkeiten und auch keine anderen Schutzmöglichkeiten, wie zum Beispiel ein Kennwort, bestehen. Die absendende Stelle hat durch geeignete Maßnahmen vor Übertragung zu gewährleisten, dass die Nachricht den berechtigten Empfänger erreicht.

c) in außergewöhnlichen Fällen mit Einwilligung der Dienststellenleitung auch über die vorstehenden Ausnahmen hinaus bei der Übertragung von VS-VERTRAULICH oder GEHEIM eingestuften VS (sofern sie keine besonderen VS-Behandlungskennzeichen wie Krypto aufweisen), wenn

   aa) zwischen Absender und Empfänger keine Kryptiermöglichkeit besteht und

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

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

40.3 Bei der Übertragung von VS kann über die bestehenden Ausnahmen nach Nummer 40.2 hinaus eine Kryptierung unterbleiben

a) innerhalb eines zutrittsgeschützten IT-Betriebsraumes,

b) wenn die Übertragungseinrichtungen so geschützt sind, dass ein Zugriff Unbefugter unverzüglich erkannt wird (approved circuits), oder

c) wenn in einem Netz der Dienststelle

aa) VS-NUR FÜR DEN DIENSTGEBRAUCH übertragen werden,

bb) nur VS-VERTRAULICH oder ausnahmsweise GEHEIM eingestufte VS übertragen werden,

cc) ein Zugriffskontrollsystem nach Nummer 37.2 eingesetzt ist und

dd) die Übertragungseinrichtungen sich vollständig in einem Bereich mit zuverlässiger Zutrittskontrolle befinden oder außerhalb gegen unmittelbaren Zugriff Unbefugter geschützt sind;

bei Verbindung mit einem anderen Kommunikationsnetz muss dieses und die Verbindung zu diesem mindestens gemäß Doppelbuchstaben cc und dd geschützt sein.

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

40.5 Sicherheitsvorgaben für Telekommunikationsanlagen, über die Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt unkryptiert geführt werden, bestimmt eine Technische Leitlinie des BSI. Das LfV ist bei Bedarf beratend hinzuzuziehen.

40.6 Bei der Kommunikation mit ausländischen oder zwischenstaatlichen Stellen, wie die NATO, gehen die jeweiligen internationalen Bestimmungen und Abkommen vor, sofern nicht nationale Bestimmungen höhere Geheimschutzmaßnahmen erfordern.

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

41.1 Vor Wartungs- oder Instandsetzungsarbeiten sollen diese VS aus dem IT-System entfernt werden, beispielsweise durch Entfernen des Datenträgers. Ist dies nicht möglich, ist nach den Nummern 10.3 und 10.4 ermächtigtes oder zugelassenes Wartungs- oder Instandsetzungspersonal einzusetzen. Während der Verarbeitung oder Übertragung von VS ist eine Wartung oder Instandsetzung des IT-Systems nicht zulässig.

41.2 Eine Fernwartung ist nur zulässig, wenn

a) sie durch nach den Nummern 10.3 und 10.4 ermächtigtes oder zugelassenes Personal erfolgt,

b) für die Übertragungen im Rahmen der Fernwartung Kryptosysteme eingesetzt sind,

c) eine zuverlässige Zugriffskontrolle, Beweissicherung und Überprüfung der Protokolle erfolgt und

d) eine gesonderte Freischaltung und Beendigung jedes Fernwartungsvorganges durch die Dienststelle erfolgt.

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

41.3 Die Geheimschutzbeauftragten können abweichend von Nummer 41.2 zulassen, dass ein Unternehmen die Fernwartung durchführt, wenn

a) ihm ein Sicherheitsbescheid des Bundesministeriums für Wirtschaft und Technologie über das Unternehmen vorliegt oder die gemäß § 26 Abs. 1 SächsSÜG zuständige Landesbehörde für die erforderlichen Geheimschutzmaßnahmen bei dem Unternehmen gesorgt hat,

b) eine gesonderte Freischaltung und Beendigung jedes Fernwartungsvorganges und Monitoring durch die Dienststelle erfolgt und

c) nach Nummer 41.2 Satz 1 Buchst. b und c und Nr. 41.2 Satz 2 verfahren wird,

d) mit dem Unternehmen zuvor ein Vertrag oder eine Vertragsergänzung über die erforderlichen Sicherheitsmaßnahmen abgeschlossen wurde.

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

VI. Abschließende Regelungen

42. Kontrollen

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

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

b) die vorhandenen VS nach der VSA behandelt werden.

Die Kontrollen sind durch die Geheimschutzbeauftragten oder besonders beauftragte Mitarbeiter, wie zum Beispiel Geheimschutzbeamte, durchzuführen.

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

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

a) die Ermächtigungen zum Zugang zu VS und die Zulassungen für eine Tätigkeit nach Nummer 10.2 im vorliegenden Umfang erforderlich sind,

b) die zum Zugang zu VS ermächtigten oder die für eine Tätigkeit nach Nummer 10.2 zugelassenen Personen ausreichend überprüft und über die von ihnen zu beachtenden Geheimschutzbestimmungen unterrichtet sind,

c) die VS vorschriftsmäßig hergestellt, vervielfältigt, gekennzeichnet, nachgewiesen, aufbewahrt und weitergegeben sowie nicht mehr benötigte VS vorschriftsmäßig vernichtet oder an das zuständige Staatsarchiv abgegeben werden,

d) der Grundsatz „Kenntnis nur, wenn nötig“ in der Praxis ausreichend beachtet wird.

42.4 Durch die für IT-Geheimschutzmaßnahmen Verantwortlichen ist insbesondere zu kontrollieren, ob

a) IT-Sicherheitskomponenten sicherheitsgerecht eingesetzt, gewartet und instand gesetzt werden,

b) Zugriffsrechte in der erteilten Form korrekt zugewiesen und erforderlich sind,

c) die Mittel zur Identifizierung/Authentisierung vorschriftsmäßig geschützt sind,

d) die freigegebene Hard- und Software unverändert ist.

42.5 Die protokollierten Daten im Rahmen der Beweissicherung sind regelmäßig daraufhin zu überprüfen, ob

a) Zugangs- oder Zugriffsversuche abgewiesen wurden und

b) Zugriffe auf VS-Daten offensichtlich ungerechtfertigt erfolgten.

42.6 Über die Durchführung der Kontrollen sowie über sicherheitserhebliche Feststellungen ist ein Nachweis zu führen. Dieser ist fünf Jahre aufzubewahren.

43. Benachrichtigung der Geheimschutzbeauftragten bei Verletzung von Geheimschutzvorschriften

Wird bekannt oder besteht der Verdacht, dass

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

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

c) Geheimschutzvorschriften verletzt sind oder

d) sonst ein unter dem Gesichtspunkt des Geheimschutzes beachtlicher Sachverhalt, wie defekte Sicherungseinrichtungen oder außergewöhnliches Interesse bestimmter Personen an VS, vorliegt,

sind die Geheimschutzbeauftragten unverzüglich zu benachrichtigen.

44. Maßnahmen bei Verletzung von Geheimschutzvorschriften oder Bekanntwerden von Sicherheitsschwächen

44.1 Die Geheimschutzbeauftragten stellen in Fällen der Verletzung von Geheimschutzvorschriften oder bei Bekanntwerden von Sicherheitsschwachstellen den Sachverhalt fest. Sie treffen die erforderlichen Maßnahmen, um Schaden zu verhüten oder zu verringern und um Wiederholungen zu vermeiden. Ist nach den ersten Ermittlungen ein nachrichtendienstlicher Hintergrund oder eine Verratstätigkeit anderer Art nicht auszuschließen, ist das LfV zu beteiligen.

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

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

44.4 War das LfV bei einem Vorkommnis nach Nummer 44.1 beteiligt, so hat es die Leitung der betreffenden Dienststelle unverzüglich über seine Feststellungen zu unterrichten. Die Dienststellenleitung trifft die gegebenenfalls noch erforderlichen Maßnahmen.

44.5 Verstöße gegen die VSA können, auch wenn sie nicht nach den Bestimmungen des Strafgesetzbuches zu verfolgen sind, disziplinarrechtlich geahndet werden oder arbeitsrechtliche Maßnahmen bis hin zu einer Kündigung nach sich ziehen.

45. Besondere Dienststellen

Dienststellen, die nach Feststellung des Staatsministeriums des Innern in besonderem Maße Ziel von Angriffen auf Vertraulichkeit, Integrität und Verfügbarkeit von VS sein können, treffen in Zusammenarbeit mit dem LfV weitere Sicherheitsvorkehrungen. Hierzu gehören insbesondere

a) intensive Unterrichtung der Beschäftigten,

b) Bestellung von Geheimschutzbeauftragten und deren Schulung zur Verstärkung von Kontrollen,

c) häufigere schwerpunktmäßige Kontrollen, bei Bedarf unter fachlicher Unterstützung durch das LfV,

d) regelmäßige umfassende Beratungen, mindestens jedoch alle vier Jahre, durch das LfV,

e) die Bildung von Sicherheitsbereichen,

f) die Einrichtung von abhörsicheren oder zumindest abhörgeschützten Räumen,

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

46. Schlussbestimmungen

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

46.2 Das Staatsministerium des Innern kann die VSA im Einvernehmen mit den obersten Staatsbehörden ändern und sie durch Hinweise und Richtlinien ergänzen.

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

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

47. Inkrafttreten

Diese Verwaltungsvorschrift tritt mit Wirkung vom 31. Dezember 2007 in Kraft.

Dresden, den 4. Januar 2008

Der Ministerpräsident
Prof. Dr. Georg Milbradt

Der Staatsminister des Innern
Dr. Albrecht Buttolo

Anlage 1
(zu Nummer 16.1)

Hinweise zur VS-Einstufung

1. Allgemeines

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

a) die tatsächlich geheimhaltungsbedürftigen Informationen effektiv geschützt und

b) unnötige Sicherheitskosten vermieden werden.

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

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

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

Insbesondere ist zu prüfen, ob das Schutzbedürfnis zur VS-Einstufung nur zeitlich begrenzt besteht (siehe Nummer 9.2 VSA).
Im Falle einer VS-Einstufung muss schlüssig darlegbar sein, welche Gefährdungen, Schäden oder Nachteile für die Bundesrepublik Deutschland oder eines ihrer Länder konkret entstehen können, wenn Unbefugte von den Informationen Kenntnis erlangen.
Eine VS-Einstufung kommt grundsätzlich nur bei Informationen in Betracht, die die

a) äußere Sicherheit,

b) auswärtigen Beziehungen,

c) innere Sicherheit oder

d) durch die Bundesrepublik Deutschland beziehungsweise durch den Freistaat Sachsen zu schützende Belange Dritter

betreffen.

VS-Einstufung, die durch die Bundesrepublik Deutschland beziehungsweise den Freistaat Sachsen zu schützende Belange Dritter betreffen, bedürfen der Billigung durch die zuständige oberste Staatsbehörde.

Für andere schutzwürdige Informationen sind die hierfür bestehenden Regelungen, zum Beispiel Pflicht zur Wahrung von Dienst- oder Steuergeheimnissen, Schutz personenbezogener Daten nach dem Sächsischen Datenschutzgesetz, dem Sächsischen Archivgesetz oder interne Geschäftsordnungen, anzuwenden.

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

3. Beispiele für VS-Einstufungen

3.1 Eine Einstufung in STRENG GEHEIM kommt zum Beispiel in Betracht für

a) das Informationsaufkommen des Bundesnachrichtendienstes,

b) Zusammenstellungen, deren Einzelheiten GEHEIM eingestuft sind, die jedoch in ihrer Gesamtheit STRENG GEHEIM einzustufen sind.

3.2 Eine Einstufung in GEHEIM kommt zum Beispiel in Betracht für

a) Maßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,

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

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

3.3 Eine Einstufung in VS-VERTRAULICH kommt zum Beispiel in Betracht für

a) Ermittlungsberichte in Spionageverdachtsfällen

b) Erkenntnisse über die Arbeitsweise extremistischer oder terroristischer Organisationen, deren Preisgabe die weitere Beobachtung beziehungsweise Aufklärung gefährden würde,

c) Pläne der Computernetze und Konfigurationsdaten der eingesetzten Systeme von Dienststellen nach Nummer 5.3 VSA

d) Zusammenstellungen, deren Einzelheiten VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind, die jedoch in ihrer Gesamtheit VS-VERTRAULICH einzustufen sind. Dies können beispielsweise Computernetze sein, in denen verschiedene Bearbeiter gelegentlich VS-NUR FÜR DEN DIENSTGEBRAUCH bearbeiten. Auf den einzelnen Arbeitsplätzen liegen dann zwar auch bei einer größeren Dienststelle nur wenige VS vor; auf den Servern kann die Zusammenstellung aber schon einen Umfang an Informationen annehmen, dass beim Verlust der Vertraulichkeit ein Schaden für den Freistaat Sachsen eintreten kann. Schnittstelle für die Einstufung ist dann das Netz oberhalb der Leitungen der einzelnen Arbeitsplatz-Computer. Des Weiteren kommen Zusammenstellungen polizeilicher Ermittlungen in Frage, die einzeln nicht oder lediglich VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind, in ihrer Gesamtheit aber polizeiliche Arbeitsweisen offenlegen.

3.4 Eine Einstufung in VS-NUR FÜR DEN DIENSTGEBRAUCH kommt zum Beispiel in Betracht für

a) Abschlussberichte über Sicherheitsüberprüfungen von Personen,

b) Fahndungsunterlagen aus den Bereichen Terrorismus und Extremismus,

c) Zusammenstellungen über Geheimschutzmaßnahmen (Geheimschutzdokumentation),

d) besondere Dienstanweisungen und Dienstpläne,

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

Anlage 2
(zu Nummer 16.1)

Hinweise zur VS-Kennzeichnung

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

1. Bei STRENG GEHEIM oder GEHEIM eingestuften VS wird der Geheimhaltungsgrad mit dem Zusatz „amtlich geheim gehalten“ in roter Farbe durch Stempel oder Druck am oberen und unteren Rand jeder beschriebenen Seite angebracht. Die beschriebenen Seiten sind zu nummerieren; ihre Gesamtzahl ist auf der ersten Seite anzugeben. Die VS sind mit Geschäftszeichen und Datum zu versehen. Das Geschäftszeichen ist am Schluss durch die Abkürzung „str.geh.“ beziehungsweise „geh.“ zu ergänzen; bei STRENG GEHEIM eingestuften VS ist es auf jeder beschriebenen Seite anzubringen.
2. Bei VS-VERTRAULICH eingestuften VS wird der Geheimhaltungsgrad mit dem Zusatz „amtlich geheim gehalten“ in schwarzer oder blauer Farbe durch Stempel, Druck oder Maschinenschrift am oberen Rand jeder beschriebenen Seite angebracht. Die beschriebenen Seiten sind zu nummerieren. Die VS sind mit Geschäftszeichen und Datum zu versehen. Das Geschäftszeichen ist am Schluss durch die Abkürzung „VS-Vertr.“ zu ergänzen.
3. Bei VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS wird der Geheimhaltungsgrad in schwarzer oder blauer Farbe durch Stempel, Druck oder Maschinenschrift am oberen Rand jeder beschriebenen Seite angebracht. Die VS sind mit Geschäftszeichen und Datum zu versehen. Das Geschäftszeichen ist am Schluss durch die Abkürzung VS-NfD zu ergänzen. Bei Büchern, Broschüren und Ähnlichem genügt die Kennzeichnung auf dem Einband oder dem Titelblatt.
4. Die äußeren Vorder- und Rückseiten sowie gegebenenfalls die Rücken von Schriftgutbehältern (Lauf-, Klebe-, Sammelmappen, Ordner, Hefter), in denen STRENG GEHEIM, GEHEIM oder VS-VERTRAULICH eingestufte VS befördert oder verwahrt werden, sind wie folgt zu kennzeichnen:

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

   b) bei GEHEIM mit einem roten Diagonalstreifen,

   c) bei VS-VERTRAULICH mit einem blauen Diagonalstreifen.

   Von dieser äußeren Kennzeichnung sind VS-Transportbehälter ausgenommen.

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

Anlage 3
(zu Nummern 11, 12, 18, 20, 21, 25, 29)

Hinweise und Muster für den Nachweis von VS

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

1. Hinweise zum Führen von VS-Bestandsverzeichnissen

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

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

1.2 Die Seiten gebundener VS-Bestandsverzeichnisse sind zu nummerieren. Bei VS-Bestandsverzeichnissen in Karteiform sind die Karteikarten fortlaufend zu nummerieren und mit Dienstsiegel zu kennzeichnen. Bei VS-Bestandsverzeichnissen in elektronischer und in Loseblattform ist das Landesamt für Verfassungsschutz beratend hinzuzuziehen.

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

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

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

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

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

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

2. Muster für Nachweise

Nachfolgende Muster befinden sich im Anhang und werden bei Bedarf als Dateivorlage zur Verfügung gestellt:

Muster 1	Verpflichtung zur Geheimhaltung von VS
Muster 2	Ermächtigung und Zulassung
Muster 3	Wiederholung der Unterrichtung
Muster 4	Aufhebung der Ermächtigung oder Zulassung
Muster 5	VS-Begleitzettel
Muster 6	VS-Übergabeprotokoll
Muster 7	VS-Vernichtungsprotokoll
Muster 8	VS-Empfangsschein
Muster 9	Konferenzbescheinigung
Muster 10	VS-Bestandsverzeichnis
Muster 11	VS-Quittungsbuch

Anlage 4
(zu Nummer 23.1 VSA)

Hinweise zur Kennzeichnung nichtdeutscher VS

Nichtdeutsche VS sind wie folgt zu kennzeichnen:

1. Nichtdeutsche VS sind mit dem deutschen Geheimhaltungsgrad, der dem zugeordneten nichtdeutschen Geheimhaltungsgrad entspricht, zu kennzeichnen. Nummer 12.1 VSA ist anzuwenden. Es genügt die Kennzeichnung mit dem deutschen Geheimhaltungsgrad auf der ersten Seite (Anlagen oder Teile gesondert).
2. Bei Übersetzungen, bei denen die nichtdeutsche Herkunft nicht erkennbar ist, ist diese auf der ersten Seite neben dem vergleichbaren deutschen Geheimhaltungsgrad kenntlich zu machen.
   Beispiele:
   SECRET DEFENSE
   GEHEIM
   amtlich geheimgehalten
   COSMIC TOP SECRET
   STRENG GEHEIM
   amtlich geheimgehalten
3. Nachstehend sind die vergleichbaren Geheimhaltungsgrade der Organisationen und Staaten aufgeführt, denen gegenüber vertragliche Verpflichtungen gemäß Nummer 1 bestehen. Daneben bestehen mit weiteren Staaten Teilabkommen für bestimmte Gebiete der Zusammenarbeit, die den dafür zuständigen Stellen bekannt sind (Ressortabkommen, Projektabkommen). Im Zweifelsfall erteilt das Bundesministerium des Innern, das eine Übersicht über alle Geheimschutzabkommen führt, Auskunft.

Den deutschen Geheimhaltungsgraden entsprechen		VS-NUR FÜR DEN DIENSTGEBRAUCH	VS-VERTRAULICH	GEHEIM	STRENG GEHEIM
A. Bei internationalen Organisationen:					
1.	NATO (1)	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
2	WEU (1)	WEU RESTRICTED	WEU CONFIDENTIAL	WEU SECRET	FOCAL TOP SECRET
3	EURATOM (1)	EURA NUR FÜR DEN DIENSTGEBRAUCH	EURA VERTRAULICH	EURA GEHEIM	EURA STRENG GEHEIM
4.	EUROCONTROL (1)	EUROCONTROL RESTRICTED	EUROCONTROL CONFIDENTIAL	EUROCONTROL SECRET	–

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

23.	Tschechische Republik (5)	VYHRAZENE	DUVIRNE	TAJNE	POISNI TAJNE
24.	Ukraine	–	Таємно	Цілком таємно	–
25.	Ungarn (5)	TITKOS	SZIGORUAN TITKOS	SZIGORUAN TITKOS	–
26.	Vereinigte Staaten (2/5)	–	CONFIDENTIAL	SECRET	TOP SECRET

Anmerkungen:

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

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

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

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

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

Anlage 5
(zu Nummern 4, 6, 35)

Hinweise zur Geheimschutzdokumentation

1. Die VS-Vorschriften einschließlich Rundschreiben, Erlasse und behördeneigene VS-Dienstanweisungen müssen den Mitarbeitern der Dienststelle jederzeit auf einfache Weise zugänglich sein.
2. In Dienststellen, die mit VS arbeiten, ist ein auf die Dienststelle bezogenes Geheimschutzkonzept zu erstellen, in dem die Informationen und vorgesehenen Maßnahmen entsprechend den nachfolgenden Absätzen dieser Anlage sowie insbesondere sonstige nach den Nummern 4.3, 18.1 und 25 der VSA dokumentiert sind. In Dienststellen mit geringem Aufkommen an VS-VERTRAULICH oder höher eingestuften VS können das Geheimschutzkonzept oder dessen Teile in anderen Dienstvorschriften oder Konzepten enthalten sein oder auf diese verweisen (zum Beispiel IT-Sicherheitskonzept).
3. Liste der nach Nummer 10 VSA zum Zugang zu VS ermächtigten oder zugelassenen Personen
4. VS-Sicherungsdokumentation

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

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

4.3 Lagepläne und Zutrittsregelungen von Sicherheitsbereichen sowie von abhörgeschützten und

abhörsicheren Räumen,

4.4 Nachweis über durchgeführte Kontrollen, ob

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

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

c) die VS gemäß der VSA hergestellt, vervielfältigt, gekennzeichnet, nachgewiesen, aufbewahrt und weitergegeben sowie nicht mehr benötigte VS gemäß Nummer 26 VSA aus dem Bestand der Dienststelle ausgesondert werden,

d) der Grundsatz „Kenntnis nur, wenn nötig“ in der Praxis beachtet wird.

5. IT-spezifische Dokumentation

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

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

5.3 Dokumentation der Nutzungs- und Zugriffsrechte,

5.4 Dokumentation der Abnahme und Freigabe,

5.5 Nachweise über durchgeführte Kontrollen, ob

a) IT-Sicherheitskomponenten wie vorgesehen eingesetzt, gewartet und instandgesetzt werden,

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

c) unbefugte Zugangs- und Zugriffsversuche erfolgten und abgewiesen wurden und

d) Zugriffe auf VS-Daten offensichtlich ungerechtfertigt erfolgten.

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

Anlage 6
(zu Nummern 21, 23, 24)

Hinweise zu Weitergabe und Versand von VS

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

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

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

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

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

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

2. Weitergabe von VS durch Boten

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

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

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

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

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

2.4 Der Empfänger hat die Unversehrtheit und den Verschluss des VS-Transportbehälters beziehungsweise Umschlages zu prüfen und ihn persönlich zu öffnen. Er überprüft anhand der Eintragungen im VS-Quittungsbuch die für die Beförderung benötigte Zeit sowie bei VS-Transportbehältern den Zählwerkstand. Er trägt das Datum, die Uhrzeit und bei VS-Transportbehältern den Zählwerkstand in das VS-Quittungsbuch ein und quittiert die VS.

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

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

Einer Verwendung von VS-Transportbehältern bedarf es nicht. Unterbleibt eine Quittung bei der Weitergabe, so ist der Klebestreifen durch das Datum und die Uhrzeit beim Absenden zu ergänzen. Im Übrigen gelten die Nummern 21.2 bis 21.4 VSA entsprechend.

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

3. Versand von VS

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

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

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

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

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

3.5 GEHEIM oder VS-VERTRAULICH eingestufte VS können durch VS-Kurier oder private

Zustelldienste befördert werden. Bei Benutzung eines privaten Zustelldienstes müssen folgende Voraussetzungen erfüllt sein:
Beim Absender

a) eindeutige Adressierung und zuverlässige Verpackung,

b) Absendung zum letztmöglichen Zeitpunkt für eine Zustellung bis zum Mittag des folgenden Arbeitstages.

Beim privaten Zustelldienst

a) Abholung beim Absender mit Zustellgarantie bis zum Mittag des folgenden Arbeitstages,

b) Nachweis der Annahme und Auslieferung der Sendung,

c) lückenlose DV-gestützte Verfolgung der Sendungen von der Annahme bis zur Auslieferung.

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

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

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

4.1 VS, die dem Landtag zugänglich gemacht werden sollen, sind von der obersten Staatsbehörde grundsätzlich der VS-Registratur der Verwaltung des Sächsischen Landtages zur Registrierung zu übersenden.

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

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

4.4 Für die Weitergabe von VS-VERTRAULICH oder höher eingestuften VS an Unternehmen gilt Nummer 21.4 VSA.

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

5. Versand von VS an Empfänger im Ausland

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

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

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

6. Verpackung für den Versand

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

6.2 Die inneren Umschläge müssen so beschaffen sein, dass ein unbefugter Zugriff auf den Inhalt

erkennbar ist. Das LfV kann im Verdachtsfall eine entsprechende Prüfung durchführen.

6.3 Der innere Umschlag ist mit folgenden Angaben zu versenden:

a) Empfänger und Absender,

b) Bezeichnung des Empfangsberechtigten mit dem Zusatz „oder Vertreter im Amt“ (o. V. i. A.),

c) Geheimhaltungsgrad sowie

d) Geschäftszeichen.

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

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

6.6 Kuriersendungen sind abweichend von Nummer 6.1 im einfachen Umschlag zu verpacken und mit dem Geschäftszeichen einschließlich des abgekürzten Geheimhaltungsgrades oder einer Ausgangsnummer zu versehen. Die Übergabe ist vom Kurier und vom Empfänger zu quittieren.

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

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

7. Aufbewahrung von VS-Transportbehältern

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

Anlage 7
(zu Nummer 19 und 21)

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

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

1. Allgemeines

1.1 Zugangsberechtigung und Weitergabe

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

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

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

hierbei einer Geheimschutzvereinbarung (siehe auch Nummer 23 VSA).

d) Zuständige Stelle für Fragen des Geheimschutzes im nicht-öffentlichen Bereich das Staatsministerium für Wirtschaft und Arbeit. Dieses kann sich beim VS-Auftragnehmer über die Einhaltung der Bestimmungen dieses Merkblattes vergewissern. Ist Auftraggeber eine Behörde, kann auch diese die Kontrollrechte nach Satz 1 wahrnehmen.

e) Die VS-Einstufung ist dreißig Jahre nach dem 1. Januar des auf die Einstufung folgenden Jahres aufgehoben, sofern keine andere Frist bestimmt ist (Siehe auch Nummer 9 VSA).

1.2 Bearbeitungsmaßnahmen

a) Kennzeichnung und Handhabung beziehungsweise Verwahrung

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

bb) VS-NfD eingestuftes Material (zum Beispiel Gerät, Ausrüstung) oder Datenträger (zum Beispiel Disketten, CD's, Mikrochips, Mikrofiche) sind ebenfalls entweder deutlich sichtbar am Material selbst oder – falls dies nicht möglich ist – an den Aufbewahrungsbehältnissen des Materials zu kennzeichnen beziehungsweise grundsätzlich umzustempeln.

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

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

b) Weitergabe

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

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

c) Vernichtung/Rückgabe

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

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

d) Verlust, unbefugte Weitergabe, Auffinden von VS oder Nichtbeachtung des Merkblattes sind unverzüglich dem deutschen VS-Auftraggeber mitzuteilen, um einen eventuell entstandenen Schaden zu begrenzen und den Vorfall aufzuklären.

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

f) Aufträge

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

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

cc) VS-Auftragnehmer/-Unterauftragnehmer im Ausland sind vertraglich zu verpflichten, die Vorschriften ihrer zuständigen Sicherheitsbehörde für die Behandlung von VS vergleichbaren Geheimhaltungsgrades zu beachten. Gibt es keinen vergleichbaren Geheimhaltungsgrad in dem Land eines VS-Auftragnehmers/-Unterauftragnehmers, ist das Staatsministerium für Wirtschaft und Arbeit einzuschalten. Die Weitergabe darf dann erst nach Zustimmung des Staatsministeriums für Wirtschaft und Arbeit erfolgen.

2. Nutzung von Informationstechnik (IT)

2.1 Bearbeitung

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

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

c) Bei der Bearbeitung von VS-NfD eingestuften VS kommen insbesondere folgende Maßnahmen in Betracht:

aa) Übersicht über die Zugriffsberechtigungen,

bb) Nutzung von Identifizierungs- und Authentisierungsmechanismen (zum Beispiel Login, Passwort),

cc) geeignete IT-Sicherheitsanweisung (einzelplatz- oder unternehmensbezogen).

d) Funktastaturen und Funk-Netzwerke dürfen nur eingesetzt werden, wenn sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind. Nähere Auskünfte erteilt das Landesamt für Verfassungsschutz Sachsen.

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

f) Transportable Datenträger (zum Beispiel Disketten, CD's, Wechselplatten), die VS-NfD eingestufte Daten unkryptiert enthalten, sind gemäß Nr. 1.2 Buchst. a Doppelbuchst. bb zu kennzeichnen und gemäß Nummer 1.2 Buchst. a Doppelbuchst. cc aufzubewahren.

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

h) IT und Datenträger sind auf Virenbefall (insbesondere sogenannte ãTrojaner‘ oder ãWürmer‘) zu überprüfen, bevor VS-NfD damit bearbeitet werden. Diese Prüfung ist in regelmäßigen Zeitabständen zu wiederholen.

i) Private IT (zum Beispiel Laptops), Software oder Datenträger dürfen nicht für die Bearbeitung eingesetzt werden. In für VS-NfD genutzten IT-Systemen dürfen keine private Software oder private Datenträger verwendet werden.

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

2.2 Übertragung

a) Bei der elektronischen Übermittlung auf Telekommunikations- oder anderen technischen Kommunikationsverbindungen (einschließlich Onlinedienste wie WWW, FTP, TELNET, E-Mail et cetera) in Deutschland sind die VS mit einem vom BSI zugelassenen, zertifizierten (Nummer 40 VSA) Kryptosystem zu kryptieren. Abweichend hiervon ist im Ausnahmefall

eine unkryptierte Übertragung zulässig

aa) innerhalb von Festnetzen bei Telefongesprächen, bei Videokonferenzen und bei Fernkopien und Fernschreiben, wenn zwischen Absender und Empfänger für die erforderliche Übertragungsart keine Kryptiermöglichkeit besteht und der VS-Auftraggeber bei der Auftragsvergabe nicht ausdrücklich eine Kryptierung verlangt. Die absendende Stelle hat sich vor der Übertragung möglichst zu vergewissern, dass sie mit dem richtigen Empfänger verbunden ist.

bb) innerhalb eines geschlossenen Netzes (LAN), wenn es ausschließlich auf einem örtlich zusammenhängenden firmeneigenen Gelände betrieben wird und die Übertragungseinrichtungen gegen unmittelbaren Zugriff Unbefugter geschützt sind.

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

2.3 Maßnahmen zum Schutz der Vertraulichkeit

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

Drei unterschiedliche Ausgangssituationen sind zu unterscheiden:

a) Einzelplatz-PC oder Netzwerke mit geschlossenen Nutzergruppen, die nicht mit anderen Netzen verbunden sind

aa) Das Betriebssystem muss ein differenziertes Benutzerprofil und Zugriffsschutz bis auf Dateiebene gewährleisten, damit der Grundsatz „Kenntnis nur, wenn nötig“ sichergestellt wird (zum Beispiel Unix/Linux, Win NT, Win 2000, Win XP).

bb) Es muss ein Login und ein Passwort vorhanden sein. Das Passwort muss mindestens sechs alphanumerische Stellen, Sonderzeichen, Groß- und Kleinbuchstaben enthalten.

cc) Das BIOS muss ebenfalls durch ein Passwort geschützt sein.

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

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

ff) Ein aktuelles Virenschutzprogramm muss eingesetzt sein.

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

b) Geschlossene Netze mit E-Mail-Anschluss nach außen
Zusätzlich zu den unter Buchstabe a festgelegten Punkten müssen

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

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

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

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

c) Standalone-PC oder geschlossene Netze mit E-Mail und Internetanschluss
Zusätzlich zu den unter Buchstaben a und b festgelegten Punkten müssen

aa) eine Firewall und ein Application-Gateway vorhanden sein,

bb) die Regelungen des BSI-Grundschutzhandbuches für Passwörter angewendet werden,

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

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

Muster

Zuletzt enthalten in

Verwaltungsvorschrift der Sächsischen Staatsregierung über die geltenden Verwaltungsvorschriften der Staatsregierung

vom 17. Dezember 2019 (SächsABl. SDr. S. S 334)