CON.11.2 Geheimschutz VS-Vertraulich oder höher

1. Beschreibung

1.1. Einleitung

Der staatliche Geheimschutz umfasst alle Maßnahmen zur Geheimhaltung von Informationen, die durch eine staatliche Stelle oder auf deren Veranlassung als Verschlusssachen (VS) eingestuft worden sind. VS sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform.

Der staatliche Geheimschutz wird durch Vorschriften des Bundes- und des Landesrechts geregelt. Rechtliche Grundlage für den staatlichen Geheimschutz des Bundes ist das Sicherheitsüberprüfungsgesetz (SÜG). Für den materiellen Geheimschutz des Bundes ist die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) maßgeblich. Diese richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit VS arbeiten.

Wird Informationstechnik zur Handhabung von VS (VS-IT) eingesetzt, dann sind die Anforderungen der VSA zu beachten. Voraussetzung für den Einsatz von VS-IT ist die Einhaltung der BSI-Standards des IT-Grundschutzes zur Informationssicherheit und der einschlägigen Mindeststandards des BSI in der jeweils geltenden Fassung. Hinzu kommen die in diesem Baustein beschriebenen Anforderungen des Geheimschutzes, die über den IT-Grundschutz hinausgehen.

Unter Zusammenschaltung von VS-IT wird die direkte oder kaskadierte Verbindung von zwei oder mehr VS-IT-Systemen für die gemeinsame Nutzung von Daten und anderen Informationsressourcen (beispielsweise Kommunikation) bezeichnet.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, dass die Anforderungen des Geheimschutzes frühzeitig in dem Sicherheitskonzept nach IT-Grundschutz berücksichtigt werden (Security-by-Design). Dieser Baustein soll die Geheimschutzbeauftragten dabei unterstützen, die Anforderungen der VSA für die elektronische Verarbeitung von VS ab dem Geheimhaltungsgrad VS-VERTRAULICH festzulegen und gemeinsam mit den Informationssicherheitsbeauftragten in das Sicherheitskonzept zu integrieren.

1.3. Abgrenzung und Modellierung

Der Baustein CON.11.2 *Geheimschutz VS-VERTRAULICH oder höher* ist einmal auf den Informationsverbund der VS-IT anzuwenden, falls VS der Geheimhaltungsgrade VS-VERTRAULICH oder höher verarbeitet werden oder werden sollen. Für diesen Informationsverbund darf der Baustein CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) nicht modelliert werden. Falls in einem Informationsverbundes Informationen bis zum Geheimhaltungsgrad VS-NfD verarbeitet werden und in einem Teil des Informationsverbundes eine Zusammenstellung vorliegt, dann sind für diesen Teilverbund die Anforderungen dieses Bausteins zu berücksichtigen. Eine Zusammenstellung liegt vor, falls einzelne Teile VS-NfD eingestuft sind, die jedoch in ihrer Gesamtheit VS-VERTRAULICH sind. Der Baustein CON.11.2 *Geheimschutz VS-VERTRAULICH oder höher* richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen, die der VSA unterliegen.

Falls der Baustein angewendet werden soll, dann ist zu beachten, dass dieser Baustein kein eigenständiges Regelwerk darstellt, sondern lediglich unterstützen soll, die VSA umzusetzen. Grundsätzlich ist zwischen Anforderungen zur Gewährleistung der Informationssicherheit und des Geheimschutzes zu unterscheiden. Der IT-Grundschutz dient der Umsetzung der Informationssicherheit und die VSA der Umsetzung des Geheimschutzes. Aus diesem Grund ersetzt eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz nicht die Freigaben von VS-IT für die Verarbeitung von VS der Geheimhaltungsgrade VS-VERTRAULICH oder höher nach VSA. Um einen durchgehenden Geheimschutz umzusetzen, müssen die Anforderungen der VSA beachtet werden.

Die Anforderungen dieses Bausteins sind aus der VSA abgeleitet und behandeln folgende Aspekte:

- allgemeine Grundsätze der VSA,
- Zugang von Personen zu VS,
- Geheimschutzdokumentation,
- Handhabung elektronischer VS,
- Absicherung von VS-IT-Räumen und -Bereichen,
- Abhörschutz,
- Abstrahlschutz,
- Einsatz von VS-IT sowie
- Wartung und Instandhaltung von VS-IT.

Dabei bauen die Anforderungen dieses Bausteins auf den Anforderungen der Informationssicherheit auf und erweitern diese um die Anforderungen des Geheimschutzes. Um den betrachteten Informationsverbund mit VS-IT abzusichern und zu gewährleisten, dass die Informationssicherheit umgesetzt ist, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. Neben den relevanten System-Bausteinen wird unter anderem die Umsetzung der folgenden Prozess-Bausteine durch diesen Baustein vorausgesetzt, da diese um die Anforderungen des Geheimschutzes erweitert werden:

- ORP.1 *Organisation*,
- ORP.2 *Personal,*
- ORP.4 *Identitäts- und Berechtigungsmanagement*,
- CON.6 *Löschen und Vernichten*,
- CON.9 *Informationsaustausch,*
- OPS.1.1.1 *Allgemeiner IT-Betrieb* sowie
- OPS.1.2.5 *Fernwartung*.

Dieser Baustein behandelt nicht:

- die Anforderungen der VSA, um VS-IT abzusichern, die für die Verarbeitung von VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH eingesetzt werden sollen (siehe CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)*),
- die allgemeinen Anforderungen der VSA, die keinen unmittelbaren Bezug zu VS-IT haben,
- den Freigabeprozess für VS-IT,
- spezielle Anforderungen, die sich aus einschlägigen Bestimmungen über- oder zwischenstaatlicher Organisationen sowie bilateraler Geheimschutzabkommen ergeben, sowie
- die Sicherheitsakkreditierung für die Verarbeitung von Verschlusssachen über- oder zwischenstaatlicher Organisationen mit VS-IT.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.11.2 *Geheimschutz VS-VERTRAULICH oder höher* von besonderer Bedeutung.

2.1. Unbefugte Kenntnisnahme

Eine wesentliche Gefährdung des Geheimschutzes stellt die Kenntnisnahme von VS durch unbefugte Personen dar. Diese kann sich ergeben, wenn die Vorgaben der VSA nicht beachtet werden.

Beispiele:

- Die Einstufung und Kennzeichnung von VS unterbleibt, erfolgt falsch oder unvollständig.
- VS werden durch IT-Produkte gelöscht, die keine Zulassungsaussage besitzen.
- Die Geheimschutzdokumentation fehlt oder wird nur mangelhaft gepflegt.

Werden die Vorgaben der VSA nicht beachtet, kann dies dazu führen, dass

- bei einer fehlerhaften Handhabung von VS Geheimschutzmaßnahmen fälschlicherweise als nicht notwendig erachtet werden, wodurch diese nicht oder nicht im notwendigen Maße umgesetzt werden,
- VS so gelöscht werden, dass der Inhalt der VS wiederherstellbar ist,
- aufgrund einer fehlenden oder mangelhaften Geheimschutzdokumentation nicht nachvollzogen werden kann, ob ein erforderliches Geheimschutzniveau erreicht wird, in der Vergangenheit schon notwendige Maßnahmen zum Schutz der VS-IT getroffen wurden oder aktuell geplante Maßnahmen zu bereits umgesetzten Maßnahmen passen,
- VS mit einer IT verarbeitet werden, die keine ausreichenden Schutzmaßnahmen bietet.

Durch Anwendungen können Daten unbemerkt gespeichert oder vervielfältigt werden.

Beispiele:

- In Auslagerungsdateien oder Auslagerungspartitionen befinden sich mitunter schützenswerte Daten, z. B. Passwörter oder kryptografische Schlüssel.
- Bei der Verarbeitung von VS mit einem Textverarbeitungsprogramm können temporäre Arbeitskopien erzeugt werden, die unter bestimmten Umständen, beispielsweise nach einem Absturz des Programms, nicht gelöscht wurden.

- Auch fallen im laufenden Betrieb vieler Anwendungen Dateien an, die nicht für den produktiven Betrieb benötigt werden (z. B. Browserhistorie). Diese Dateien können sicherheitsrelevante Informationen enthalten.

Als Folge können solche Dateien ausgelesen werden, wenn die Datenträger ausgebaut und in ein anderes IT-System eingebaut werden. Wurden die Auslagerungs- oder Anwendungsdateien oder temporäre Dateien nicht sicher gelöscht, können Unbefugte Kenntnis von VS erlangen. Passwörter und Schlüssel können missbraucht werden, um unberechtigt auf VS-IT oder VS zuzugreifen.

Die Auswirkungen einer unbefugten Kenntnisnahme von VS des Geheimhaltungsgrads VS-VERTRAULICH oder höher können je nach Art und Einstufungsgrad der als VS eingestuften Informationen unterschiedlich ausfallen. So kann die unbefugte Kenntnisnahme von VS des Geheimhaltungsgrad VS-VERTRAULICH für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein. Die unbefugte Kenntnisnahme VS des Geheimhaltungsgrads STRENG GEHEIM kann hingegen den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden.

2.2. Konspirative Angriffe

Als konspirativer Angriff wird eine Form der Spionage bezeichnet, bei der Informationen verdeckt von nicht öffentlich zugänglichen Informationen durch ausländische Nachrichtendienste gewonnen werden. Bei konspirativen Angriffen versuchen Nachrichtendienste möglichst unbemerkt an für sie interessante Informationen, wie z. B. VS, zu gelangen.

Bei konspirativen Beschaffungsaktivitäten verschleiern die Nachrichtendienste ihre wahren Absichten. Die Informationen werden über den Einsatz menschlicher Quellen (z. B. Social Engineering), durch technische Mittel (z. B. Abhörmaßnahmen oder Cyber- Angriffe, bei denen Hintertüren ausgenutzt oder Schadsoftware eingesetzt wird) oder durch eine Kombination beider Möglichkeiten beschafft.

In der Folge können ausländische Nachrichtendienste auf VS zugreifen und sich einen entscheidenden Vorteil gegenüber der Bundesrepublik Deutschland oder eines ihrer Länder verschaffen. Auch andere Gruppierungen, wie beispielsweise terroristische Organisationen oder die organisierte Kriminalität, können mit den aus konspirativen Angriffen erlangten Informationen mögliche Aktivitäten effektiver planen und durchführen.

2.3. Angriffe durch Innentäter

Bei einem Angriff durch sogenannte Innentäter werden interne Informationen wie z. B. VS durch interne oder externe Mitarbeitende bewusst entwendet und gegebenenfalls an Dritte verkauft oder veröffentlicht. Innentäter verfügen über ein breites Wissen über interne Prozesse und Arbeitsabläufe ihrer Institutionen. Darüber hinaus verfügen sie über Zutritts-, Zugangs- und Zugriffsrechte, über die Außenstehende nicht verfügen. Dieses Wissen und die ihnen für ihre dienstlichen Aufgaben erteilten Rechte können sie einsetzen, um die Erfolgswahrscheinlichkeit eines Angriffs zu erhöhen. Weiterhin können sie den Zeitpunkt des Angriffs so steuern, dass dieser durchgeführt wird, wenn dieser nur schwer erkannt werden kann, beispielsweise in Wartungsfenstern.

Die Ursachen, warum sich Mitarbeitende dazu entschließen Informationen zu entwenden, sind individuell unterschiedlich.

Beispiele:

- Die Innentäter fühlen sich moralisch dazu verpflichtet, Informationen, die als VS eingestuft sind, zu veröffentlichen, um damit beispielsweise Missstände aufzudecken.
- Die Innentäter wurden von einem Nachrichtendienst angeworben.
- Die Innentäter möchten sich mit dem Verkauf von Informationen bereichern.

In der Folge können Dritte unberechtigt Zugang zu VS erlangen. Die Voraussetzungen, unter denen ein Innentäter agiert, erschweren den Schutz vor einem solchen Angriff. Viele der zum Schutz vor Angriffen eingesetzten Maßnahmen sind gegen den Angriff durch einen Innentäter nicht wirksam.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.11.2 *Geheimschutz VS-VERTRAULICH oder höher* aufgeführt. Die damit verbundenen Aufgaben nimmt, sofern bestellt, der oder die jeweilige Geheimschutzbeauftragten wahr. Dieser oder diese ist für die Umsetzung der VSA zuständig. Wurde kein oder keine Geheimschutzbeauftragte bestellt, nimmt die Dienststellenleitung diese Aufgaben wahr. Der oder die Informationssicherheitsbeauftragte (diese Rolle entspricht der in der VSA und im UP Bund definierten Rolle der IT-Sicherheitsbeauftragten) unterstützt und berät den oder die Geheimschutzbeauftragte in allen Fragen zum Einsatz von VS-IT.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Geheimschutzbeauftragte
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

Hinweis: Bei der Anwendung dieses Bausteins sind folgende Regelungen zu beachten:

- Dieser Baustein hat **keinerlei** Regelungscharakter. Es handelt sich **nicht** um ein eigenständiges Regelwerk, sondern die Anforderungen ergeben sich aus der VSA.
- Allgemeine Regelungen der VSA, die keine spezifischen Vorgaben zu VS-IT enthalten, sind **nicht** Bestandteil dieses Bausteins. Diese Regelungen sind der VSA zu entnehmen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.11.2.A1 Einhaltung der Grundsätze zur VS-Verarbeitung mit IT nach § 3, 4 und 6 VSA (B)

VS DÜRFEN NUR mit hierfür freigegebener VS-IT verarbeitet werden. Private IT DARF NICHT für die Verarbeitung von Verschlusssachen eingesetzt werden. Bei der Verarbeitung von VS mit VS-IT MUSS der Grundsatz „Kenntnis nur, wenn nötig“ eingehalten werden. Es DÜRFEN NUR Personen Kenntnis von einer VS erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis erhalten müssen. Personen DÜRFEN NICHT umfassender oder eher über eine VS unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist.

Die Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ SOLLTE, insbesondere falls die VS-IT durch mehrere Benutzende verwendet wird, primär über technische Maßnahmen sichergestellt werden.

Nach dem Grundsatz der mehrschichtigen Sicherheit MÜSSEN personelle, organisatorische, materielle und technische Maßnahmen getroffen werden, die in ihrem Zusammenwirken

- Risiken eines Angriffs reduzieren (Prävention),
- Angriffe erkennbar machen (Detektion) und
- im Falle eines erfolgreichen Angriffs die negativen Folgen begrenzen (Reaktion).

Bei der Erfüllung der Anforderungen des vorliegenden Bausteins MÜSSEN die relevanten Technischen Leitlinien des BSI (BSI TL) beachtet werden. Falls von den BSI TL abgewichen werden soll, dann DARF dies NUR in Ausnahmefällen und im Einvernehmen mit dem BSI erfolgen.

CON.11.2.A2 Erstellung und Fortschreibung der Geheimschutzdokumentation nach § 12 und Nr. 2 Anlage II zur VSA (B)

Jede Dienststelle, die VS-IT einsetzt, MUSS eine Geheimschutzdokumentation erstellen. Die Geheimschutzdokumentation MUSS alle Dokumente beinhalten, die in Nr. 2 Anlage II zur VSA aufgeführt sind.

Die Geheimschutzdokumentation MUSS bei allen geheimschutzrelevanten Änderungen aktualisiert werden. Sie MUSS zudem mindestens alle drei Jahre auf Aktualität, Vollständigkeit und Erforderlichkeit bestehender und noch zu treffender Geheimschutzmaßnahmen überprüft werden.

CON.11.2.A3 Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B)

Bei der Auswahl und dem Einsatz von IT-Sicherheitsprodukten und -komponenten nach §§ 51, 52 VSA MÜSSEN die dafür getroffenen Regelungen der VSA und der dort verankerten Dokumente Anwendung finden.

Insbesondere die Regelungen der folgenden Dokumente MÜSSEN dabei angewendet werden:

- Katalog der Produktklassen und –typen (VS-Produktkatalog) nach § 52, Abs. 2 VSA,
- aktuelle Liste zugelassener IT-Sicherheitsprodukte und –komponenten (BSI Schrift 7164) nach § 52 Abs. 2 VSA,
- Mitwirkungspflichten in Zulassungsverfahren (Technische Leitlinie BSI TL IT – 01) nach § 52 Abs. 1 VSA.

CON.11.2.A4 Beschaffung von VS-IT und Beauftragung von Dienstleistern nach §§ 25 und 49 VSA (B)

Bevor VS-IT beschafft wird, MUSS sichergestellt werden, dass deren Sicherheit während des gesamten Lebenszyklus ab dem Zeitpunkt, zu dem feststeht, dass die IT zur VS-Verarbeitung eingesetzt werden soll, bis zur Aussonderung kontinuierlich gewährleistet wird. Um einen durchgehenden Geheimschutz sicherzustellen, MÜSSEN die Vergabeunterlagen so formuliert werden, dass die Anforderungen der VSA vollständig erfüllt werden können.

Bei Beschaffungsaufträgen für VS-IT MÜSSEN die notwendigen IT-Sicherheitsfunktionen der jeweiligen IT-Produkte vorab festgelegt werden. Bei der Formulierung der Vergabeunterlagen MÜSSEN insbesondere die

- Aufbewahrung,
- Archivierung,
- Löschung von elektronischer VS,
- Abstrahlsicherheit,
- Aussonderung sowie
- Wartung und Instandsetzung von VS-IT

berücksichtigt werden. Sofern ein zu beschaffendes IT-Produkt eine Zulassungsrelevanz besitzt, MUSS ein IT-Produkt aus der Liste der zugelassenen IT-Sicherheitsprodukte beschafft werden (vgl. CON.11.2.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA*). In diesem Fall MUSS die Befristung der Zulassungsaussage des IT-Sicherheitsproduktes bzw. der Zeitraum für die Durchführung eines Zulassungsverfahrens berücksichtigt werden, um zukünftig anfallende Ersatzbeschaffungen frühzeitig miteinzuplanen.

Verträge MÜSSEN derart gestaltet werden, dass bei einer Rückgabe von defekten oder geleasten IT-Produkten deren Datenträger oder sonstige Komponenten, auf denen VS gespeichert sein könnten, im Besitz der Dienststelle verbleiben.

Falls ein nichtöffentlicher Dienstleister beauftragt werden soll, der beispielsweise die VS-IT betreiben soll, dann MÜSSEN vor der Beauftragung beim BMWK Sicherheitsbescheide (Facility Security Clearance, FSC) über die zu beteiligende nichtöffentliche Stelle angefordert werden. Der nichtöffentliche Dienstleister MUSS sich in der geheimschutzbetreuten Wirtschaft befinden. Mit dem nichtöffentlichen Dienstleister MUSS ein VS-Auftrag geschlossen werden. Die Vorgaben des Geheimschutzhandbuches der Wirtschaft MÜSSEN grundsätzlich eingehalten werden. Insbesondere MUSS dem nichtöffentlichen Dienstleister eine VS-Einstufungsliste zur Verfügung gestellt werden.

Falls der nichtöffentliche Dienstleister für eine VS-IT als Betreiber nach § 50 Abs. 6 auftreten soll, MUSS weiterhin die VSA angewendet werden.

CON.11.2.A5 Verpflichtung, Ermächtigung und Zulassung nach §§ 3, 4 VSA (B)

Die Regelungen der VSA zu Verpflichtung, Ermächtigung und Zulassung MÜSSEN eingehalten werden, falls eine Person Zugang zu VS erhält oder sich Zugang zu solcher verschaffen kann.

Für den Einsatz an VS-IT zur Verarbeitung von VS MUSS das Fremdpersonal entsprechend sicherheitsüberprüft, sowie zugelassen oder ermächtigt sein. Fremdpersonal nichtöffentlicher Stellen DARF NUR für VS-IT eingesetzt werden, wenn sich die nichtöffentliche Stelle in der Geheimschutzbetreuung des BMWK befindet.

Für Fremdpersonal nichtöffentlicher Stellen MÜSSEN die Vorgaben des Geheimschutzhandbuches der Wirtschaft beachtet werden.

CON.11.2.A6 Beaufsichtigung und Begleitung von nicht zugelassenem oder nicht ermächtigtem Personal nach §§ 3, 4 VSA (B)

Eine nicht zugelassene oder nicht ermächtigte Person, die sich Zutritt zu Räumen und Bereichen, in denen VS-IT betrieben wird, verschaffen kann, MUSS während der gesamten Zeit begleitet und beaufsichtigt werden. Die beaufsichtigenden Personen MÜSSEN über die notwendigen Fachkenntnisse verfügen, um die Tätigkeiten kontrollieren zu können.

CON.11.2.A7 Kennzeichnung von elektronischen VS und Datenträgern nach §§ 20, 54 und Anlage III und VII zur VSA (B)

Elektronische VS MÜSSEN nach den Vorgaben der VSA gekennzeichnet werden. Die Kennzeichnung MUSS bei der Verarbeitung von VS mit VS-IT während der gesamten Dauer ihrer Einstufung jederzeit erkennbar sein. Die Kennzeichnung MUSS auch bei kopierten, elektronisch versendeten oder ausgedruckten VS erhalten bleiben. Falls die Beschaffenheit elektronischer VS eine Kennzeichnung nach VSA nicht zulässt, dann MÜSSEN VS sinngemäß gekennzeichnet werden.

Der Dateiname einer elektronischen VS SOLLTE eine Kennzeichnung enthalten, die den VS-Charakter des Inhalts erkennen lässt, ohne die VS öffnen zu müssen.

Falls eine elektronische Kennzeichnung von VS (im Sinne von Metadaten) verwendet werden soll, dann MUSS geprüft werden, ob diese IT-Sicherheitsfunktionen übernimmt (siehe CON.11.2.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA)*.

Datenträger, auf denen elektronische VS durch Produkte ohne Zulassungsaussage verschlüsselt gespeichert sind, MÜSSEN mit dem höchsten Geheimhaltungsgrad der darauf gespeicherten VS gekennzeichnet werden (vgl. unter anderem Muster 13 der Anlage VIII zur VSA). Falls sich durch die Zusammenstellung der VS auf dem Datenträger ein Datenbestand ergibt, welcher eine höhere Einstufung erforderlich macht, dann MUSS der Datenträger selbst als VS des höheren Geheimhaltungsgrades behandelt und gekennzeichnet werden.

CON.11.2.A8 Verwaltung und Nachweis von elektronischen VS nach § 21 und Nr. 2 Anlage IV zur VSA (B)

Für die Verwaltung von elektronischen VS MÜSSEN die Grundsätze ordnungsgemäßer Aktenführung (gemäß Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien) und die Vorgaben der VSA zur Verwaltung und Nachweisführung von VS eingehalten werden.

Sofern die Verwaltung elektronischer VS in elektronischen VS-Registratursystemen erfolgt, MÜSSEN für diese die Vorgaben der VSA für VS-IT eingehalten werden. Elektronische VS-Registratursysteme MÜSSEN gegen unbefugten Zugriff geschützt werden. Sie SOLLTEN auf nicht-vernetzten Einzelplatzrechnern oder in einem isolierten, ausschließlich für den Zweck der VS-Nachweisführung genutzten Netz betrieben werden. In elektronischen VS-Registratursystemen MUSS bei der Registrierung für jede VS unter einer eigenen fortlaufenden Nummer ein eigener Datensatz angelegt werden. Für jede Anlage und Vervielfältigung einer VS MUSS jeweils ein eigener Datensatz unter derselben fortlaufenden Nummer angelegt werden. Elektronische VS-Registratursysteme MÜSSEN Funktionen bereitstellen, die die Ausgabe aller für die VS-Nachweisführung relevanten Daten nach bestimmten Auswahl- und Sortierungskriterien ermöglichen.

Die Nachweisführung in VS-Registratursystemen MUSS die Anforderungen an die Nachweisführung in Papier-Form und die elektronische Nachweisführung erfüllen. Das Anlegen von Ordnungsstrukturen, das Ändern und Löschen von Datensätzen sowie die Aussonderung von VS DÜRFEN bei elektronischer VS-Bearbeitung NUR auf Weisung eines zeichnungsbefugten VS-Bearbeiters durch VS-Registratoren vorgenommen werden. Produkte, die innerhalb von VS-IT insbesondere zur Nachweisführung IT-Sicherheitsfunktionen nach § 52 VSA übernehmen, MÜSSEN eine Zulassungsaussage besitzen.

CON.11.2.A9 Umgang mit VS-Zwischenmaterial nach § 33 VSA (B)

VS-Zwischenmaterial MUSS grundsätzlich als VS behandelt werden. Auf eine Kennzeichnung und Nachweisführung DARF NUR verzichtet werden, falls das VS-Zwischenmaterial nicht an Dritte weitergegeben und unverzüglich vernichtet wird. Falls es nicht unverzüglich vernichtet wird, dann MUSS es mit dem entsprechenden Geheimhaltungsgrad und dem Zusatz "VS-Zwischenmaterial" gekennzeichnet werden. Falls VS-Zwischenmaterial an Dritte weitergegeben wird, dann MUSS ein Nachweis über die Weitergabe erfolgen.

Falls VS-Zwischenmaterial auf einem Datenträger gespeichert wird, dann MUSS dieser Datenträger entsprechend gehandhabt werden, als sei dort VS gespeichert (vgl. CON.11.2.A21 *Handhabung von Datenträgern und IT-Produkten nach §§ 21, 22, 54 VSA*). Für den Umgang mit VS-Zwischenmaterial MÜSSEN Vorgaben für die Mitarbeitenden festgelegt werden.

CON.11.2.A10 Elektronische Vervielfältigung von VS nach § 22 VSA (B)

Elektronische Vervielfältigungen im Sinne einer absichtlichen Herstellung von weiteren Exemplaren von Ausfertigungen MÜSSEN entsprechend den Vorgaben der VSA gekennzeichnet (vgl. CON.11.2.A7 *Kennzeichnung von elektronischen VS und Datenträgern nach §§ 20, 54 und Anlage III und VII zur VSA*) und gehandhabt werden. Die Vervielfältigung von VS DARF NUR durch hierfür ermächtigtes Personal oder durch VS-Registratoren erfolgen.

Falls Kopien von VS auf Backup Datenträgern gespeichert werden, MUSS die Anforderung CON.11.2.A21 *Handhabung von Datenträgern und IT-Produkten nach §§ 21, 22, 54 VSA* berücksichtigt werden.

CON.11.2.A11 Aufbewahrung elektronischer VS nach § 23 VSA (B)

Elektronische VS SOLLTEN mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt gespeichert werden.

Falls die Speicherung elektronischer VS unverschlüsselt oder verschlüsselt durch ein Produkt ohne Zulassungsaussage erfolgt, dann MÜSSEN die Datenträger und IT-Produkte, auf denen die VS gespeichert sind:

- entsprechend den Vorgaben der VSA materiell gesichert werden und
- gemäß des höchsten Geheimhaltungsgrades der darauf gespeicherten VS gehandhabt werden (vgl. CON.11.2.A21 *Handhabung von Datenträgern und IT-Produkten nach § 54 VSA*).

CON.11.2.A12 Elektronische Übertragung von VS nach §§ 24, 53, 55 VSA (B)

Bei elektronischer Übertragung MÜSSEN VS über technische Kommunikationsverbindungen mittels hierfür freigegebener VS-IT weitergegeben werden. Die VS MÜSSEN bei der Übertragung durch IT-Sicherheitsprodukte mit Zulassungsaussage oder materielle Schutzmaßnahmen vor unbefugtem Zugriff geschützt werden. Falls die VS unverschlüsselt übertragen werden soll, dann MUSS die gesamte Übertragungsstrecke gemäß BSI TL 01101-3 materiell abgesichert sein oder sich innerhalb eines VS-IT-Raumes oder -Bereiches befinden.

Die Regelungen der VSA zur Weitergabe von VS (§ 24 VSA) MÜSSEN auch bei elektronischer Weitergabe eingehalten werden. Die Weitergabe von VS SOLLTE über die VS-Registraturen erfolgen. Die Weitergabe MUSS nachgewiesen werden. Falls die elektronische Übertragung nicht zwischen zwei VS-Registraturen erfolgt, dann MUSS sichergestellt werden, dass der Empfänger die VS der VS-Registratur unverzüglich bekannt macht (vgl. CON.11.2.A8 *Verwaltung und Nachweis von elektronischen VS nach § 21 und Nr. 2 Anlage IV zur VSA*).

Bevor VS an Dritte elektronisch übertragen werden, MUSS festgestellt werden:

- an welche Stellen die VS übertragen werden sollen und
- welche Vorschriften einschlägig sind.

Die Übertragung von VS DARF NUR erfolgen, falls der Empfänger zur Annahme oder Kenntnisname berechtigt ist und die IT des Empfängers für die Verarbeitung von VS des entsprechenden Geheimhaltungsgrades freigegeben ist. Für die Weitergabe an Parlamente, Landesbehörden und nichtöffentliche Stellen MÜSSEN auch bei der elektronischen Übertragung von VS die besonderen Regelungen der VSA (vgl. §§ 25 und 26 VSA) eingehalten werden.

Von diesen Regelungen DARF NUR in Ausnahmefällen und nur für die Kommunikation von VS-VERTRAULICH gemäß § 55 VSA unter Einhaltung der dort genannten Anforderungen abgewichen werden. Dort, wo die Notwendigkeit zur elektronischen Übertragung von VS zu erwarten ist, MUSS die Infrastruktur für eine VSA-konforme Übertragung geschaffen werden. In diesen Fällen DARF diese Ausnahmeregelung NICHT angewendet werden. Eine VSA-konforme Übertragung MUSS für alle potentiellen Übertragungswege umgesetzt werden. Dies MUSS auch in dem Fall umgesetzt werden, falls die Kommunikation nicht zum täglichen Dienstbetrieb notwendig ist.

Falls die VS an nichtdeutsche Stellen übertragen werden soll, MUSS geprüft werden, ob es über- oder zwischenstaatliche Regelungen oder bilateraler Geheimschutzabkommen zum Austausch von VS gibt. Bei Empfang und der Verarbeitung von VS von internationalen Stellen MÜSSEN insbesondere die Regelungen der §§ 34 - 36 VSA eingehalten werden.

CON.11.2.A13 Mitnahme elektronischer VS nach § 28 VSA (B)

Bei Mitnahme auf Dienstreisen oder zu Dienstbesprechungen MÜSSEN elektronische VS innerhalb des Bundesgebiets grundsätzlich vorab mittels technischer Kommunikationsverbindungen nach § 55 VSA an eine Dienststelle am Zielort übertragen werden, die selbst VS verwaltet oder aufbewahrt.

VS sowie Datenträger, auf denen VS unverschlüsselt oder durch ein IT-Sicherheitsprodukt ohne Zulassungsaussage verschlüsselt gespeichert wurden, SOLLTEN nach außerhalb des Bundesgebiets durch den Kurierdienst des Auswärtigen Amtes an die zuständige Auslandsvertretung vorausgesendet werden. Alternativ SOLLTEN die elektronischen VS mittels technischer Kommunikationsverbindungen nach § 55 VSA übertragen werden. Nach Erledigung des Dienstgeschäftes SOLLTEN die VS bzw. Datenträger auf demselben Weg zurückgesendet werden.

Bei der persönlichen Mitnahme von VS-VERTRAULICH oder GEHEIM eingestufter VS nach außerhalb des Bundesgebiets MUSS das Auswärtige Amt eingebunden werden. Hiervon DARF NUR abgewichen

werden, falls sich die VS in elektronischer Form auf hierfür freigegebener VS-IT befinden oder mit einem IT-Sicherheitsprodukt mit Zulassungsaussage auf einem Datenträger verschlüsselt sind.

Vor der Mitnahme von VS-IT ins Ausland MUSS geprüft werden, ob der Export bzw. die Verbringung der VS-IT aus Deutschland eventuell der deutschen Exportgesetzgebung unterliegt. Vor einer Dienstreise ins Ausland MUSS geprüft werden, ob die VS-IT bei der Ausreise aus dem Zielland einer dortigen Exportkontrollgesetzgebung unterliegt. Um zu verhindern, dass diese Gesetzgebung unter Umständen zu einem Verstoß gegen die Bestimmungen des BSI für den Einsatz und Betrieb (SecOPs) eines mitgeführten IT-Sicherheitsproduktes führt, MUSS vorab eine Abstimmung mit dem eigenen Geheimschutzbeauftragten erfolgen.

Die persönliche Mitnahme von STRENG GEHEIM eingestuften elektronischen Verschlusssachen im grenzüberschreitenden Verkehr DARF NICHT erfolgen.

CON.11.2.A14 Archivierung elektronischer VS nach §§ 30, 31 VSA (B)

Die VS MUSS entsprechend der VS-Archivrichtlinie (Anlage VI zur VSA) ausgesondert werden. Schon bei Einführung von Systemen zur elektronischen Schriftgutverwaltung (beispielsweise ein VS-Registratursystem) und Vorgangsbearbeitung MÜSSEN die technischen Verfahren zur Aussonderung frühzeitig mit dem zuständigen Geheimarchiv abgestimmt werden. Falls das zuständige Geheimarchiv VS nicht übernehmen möchte, MÜSSEN die VS gemäß CON.11.2.A15 *Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 VSA* sicher gelöscht bzw. vernichtet werden.

CON.11.2.A15 Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 VSA (B)

Um dauerhaft eine unbefugte Kenntnisnahme von elektronischen VS zu verhindern, die mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, MUSS der Schlüssel unter Beachtung des SecOPs des zur Verschlüsselung eingesetzten IT-Sicherheitsproduktes gelöscht werden. Analoge und digitale Datenträger MÜSSEN gelöscht werden, bevor sie die gesicherte Einsatzumgebung dauerhaft verlassen. Sie MÜSSEN physisch vernichtet werden, falls sie nicht gelöscht werden können. Für die Vernichtung von VS MÜSSEN Produkte oder Verfahren eingesetzt oder Dienstleister beauftragt werden, die die Anforderungen der BSI TL – M 50 erfüllen.

Die zuvor beschriebenen Teilanforderungen MÜSSEN auch bei defekten Datenträgern und IT-Produkten eingehalten werden.

CON.11.2.A16 Absicherung von VS-Arbeitsbereichen nach §§ 38, 39, 45 VSA (B)

VS-Arbeitsbereiche (VS-IT-Räume und andere Räume in denen VS-VERTRAULICH oder höher eingestufte VS verarbeitet werden) MÜSSEN identifiziert werden. Die Be- und Verarbeitung von VS mittels VS-IT MUSS in VS-IT-Räumen oder VS-IT-Bereichen erfolgen. Alle Räume eines VS-Arbeitsbereiches MÜSSEN die Vorgaben der BSI TL - M 10 sowie auf die in ihr verwiesenen BSI TL in der jeweils gültigen Fassung für die Planung und Errichtung von räumlichen Sicherungsmaßnahmen nach § 39 VSA erfüllen.

Die Sicherungsmaßnahmen für Räume und Bereiche, in denen VS verarbeitet werden, MÜSSEN in der Geheimschutzdokumentation festgelegt werden. Die Räume und Bereiche MÜSSEN so geschützt werden, dass Unbefugte am Zutritt gehindert werden. Unberechtigte Zutrittsversuche SOLLTEN automatisiert aufgezeichnet werden. VS-IT-Räume SOLLTEN, sofern vorhanden, in Sicherheitsbereichen eingerichtet oder zu Sicherheitsbereichen (vgl. § 39 VSA) erklärt werden. Bei der Planung von VS-Arbeitsbereichen MUSS das BSI beratend hinzugezogen werden.

CON.11.2.A17 Abhörschutz nach § 41 VSA (B)

Dienststellen MÜSSEN Vorkehrungen treffen, damit ihre Telekommunikations- und Informationstechnik nicht dazu missbraucht werden kann, um Raum- und Telefongespräche abzuhören. In der Geheimschutzdokumentation MUSS festgelegt werden, ob für einen VS-Arbeitsplatz besondere Maßnahmen zum Abhörschutz erforderlich sind.

Werden in bestimmten Räumen häufig oder regelmäßig Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt geführt, MÜSSEN diese Räume abhörgeschützt oder abhörsicher eingerichtet werden. Falls die Dienststelle über einen Sicherheitsbereich verfügt, SOLLTEN die abhörgeschützten oder abhörsicheren Räume innerhalb dieses Sicherheitsbereiches eingerichtet werden. Die organisatorischen Anforderungen zu Abhörschutzmaßnahmen für diese Räume MÜSSEN gemäß BSI TL – L 10 erfüllt werden. Zusätzlich zur BSI TL - L 10 MÜSSEN:

- für abhörgeschützte Büroräume die Anforderungen der BSI TL – L 11,
- für abhörgeschützte Besprechungsräume die Anforderungen der BSI TL – L 12,
- für abhörsichere Besprechungsräume die Anforderungen der BSI TL – L 13 und
- für VS-Sprechstellen die Anforderungen der BSI TL - L 14 erfüllt werden.

Häufige oder regelmäßige Gespräche mit VS-VERTRAULICH oder GEHEIM eingestuftem Inhalt MÜSSEN in einem abhörgeschützten Raum geführt werden. Gespräche mit STRENG GEHEIM eingestuftem Inhalt, die häufig oder regelmäßig stattfinden, MÜSSEN in einem abhörsicheren Raum geführt werden.

Falls selten und unregelmäßig Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt geführt werden, MÜSSEN:

- der Ort, an dem diese stattfinden, entsprechend den Vorgaben eines VS-Arbeitsbereichs abgesichert sein (vgl. *11.2.A16 Absicherung von VS-Arbeitsbereichen nach §§ 38, 39, 45 VSA (B)*) und
- in Abstimmung mit den Geheimschutzbeauftragten Maßnahmen getroffen werden, um das unzulässige Abhören von Gesprächsinhalten zu verhindern oder zumindest signifikant zu erschweren.

Wird für die Übertragung der Inhalte mit einem Geheimhaltungsgrad ab VS-VERTRAULICH ein Videokonferenzsystem verwendet, MÜSSEN die Anforderungen der BSI TL – L 16 erfüllt sein.

CON.11.2.A18 Schutz von Zutritts- und Zugangsmitteln nach § 46 VSA (B)

Gegenständliche Zutrittsmittel für VS-IT-Räume und -Bereiche, Sicherheitsbereiche, VS-Verwahrgelasse, abhörgeschützte und abhörsichere Räume sowie gegenständliche Zugangsmittel für VS-IT MÜSSEN so geschützt werden, dass Unbefugte keinen Zugriff auf VS erhalten.

Gegenständliche Zutritts- und Zugangsmittel MÜSSEN grundsätzlich während der Dienstzeit in persönlichem Gewahrsam gehalten werden. Vor Verlassen des Dienstgebäudes MÜSSEN diese in einem VS-Verwahrgelass oder VS-Schlüsselbehälter verschlossen werden.

Wissensbasierte Zutritts- und Zugangsmittel DÜRFEN NUR den Berechtigten bekannt sein. Sie MÜSSEN geändert werden:

- vor der erstmaligen Nutzung,
- bei einem Wechsel der Berechtigten,
- nach deren Nutzung in Abwesenheit des Berechtigten,
- bei einem Verdacht, dass sie bekannt geworden sind und
- mindestens alle zwölf Monate.

Zutritts- und Zugangsmittel MÜSSEN zentral verwaltet werden. Die Ausgabe MUSS dokumentiert werden. Die wissensbasierten Zutritts- und Zugangsmittel SOLLTEN personalisiert sein. Es SOLLTE eine Dienstanweisung für deren Umgang erstellt werden. Die Dienstanweisung SOLLTE den Mitarbeitenden bekannt gemacht werden.

Für Notfälle SOLLTEN Reservezutritts- und -zugangsmittel entsprechend den Vorgaben der VSA vorgehalten werden. In der Geheimschutzdokumentation SOLLTE festgehalten werden, wo sich diese befinden und wer dazu Zugang hat.

CON.11.2.A19 Zugangs- und Zugriffsschutz nach § 3 VSA (B)

Die VS-IT MUSS so geschützt werden, dass ein Zugang zu dieser nur durch berechtigte Personen (vgl. CON.11.2A.5 *Verpflichtung, Ermächtigung und Zulassung nach §§ 3, 4 VSA*) erfolgen kann. Der Schutz der VS MUSS sichergestellt werden über:

- IT-Sicherheitsprodukte mit Zulassungsaussage,
- materielle,
- organisatorische oder
- personelle Maßnahmen.

Für den Zugangs- und Zugriffsschutz MUSS eine Mehr-Faktor-Authentisierung genutzt werden.

Die VS-IT MUSS so geschützt werden, dass nur Personen Zugriff auf VS erhalten oder sich Zugang zu dieser verschaffen können, die für den Umgang mit VS des entsprechenden Geheimhaltungsgrades ermächtigt oder zugelassen wurden.

CON.11.2.A20 Abstrahlschutzmaßnahmen nach § 57 VSA (B)

Für den Raum, in dem die VS-IT eingesetzt werden soll, MUSS eine Zonenbewertung durch das BSI erfolgen.

Auf Basis der ermittelten Zone MUSS geeignete abstrahlgeprüfte Hardware eingesetzt werden (vgl. BSI-TL 03305 bzw. "Liste abstrahlgeprüfter Produkte nach SDIP 27 Level A"). Falls dies nicht möglich ist, MÜSSEN bauliche Maßnahmen zur Reduktion der Abstrahlung umgesetzt werden (vgl. BSI-TL 03304 oder BSI-TR-03209-x).

Eine Beratung durch das BSI SOLLTE in Anspruch genommen werden. Falls Neubau- oder große Umbaumaßnahmen geplant sind, SOLLTE das BSI frühzeitig eingebunden werden.

Eine erneute Abstrahlprüfung von abstrahlgeprüfter Hardware MUSS durchgeführt werden, falls:

- nachträglich weitere Komponenten angeschlossen wurden (zweiter Monitor, Webcam, Headset etc.),
- Komponenten ausgetauscht wurden (z. B. Tastatur, Monitor) oder
- Modifikationen, Reparaturen oder sonstige Änderungen am eigentlichen Gerät oder abstrahlgeprüften Komponenten vorgenommen wurden.

In diesem Fall DARF KEINE weitere Verarbeitung von VS des Geheimhaltungsgrades VS-VERTRAULICH oder höher mit diesen Komponenten erfolgen.

CON.11.2.A21 Handhabung von Datenträgern und IT-Produkten nach §§ 21, 22, 54 VSA (B)

Bei Datenträgern und Backup-Datenträgern, auf denen VS gespeichert sind, MÜSSEN der Verbleib und die Vernichtung in einem gesonderten VS-Bestandsverzeichnis nachgewiesen werden. Es MUSS jederzeit nachvollziehbar sein, welche VS auf einem Datenträger gespeichert wurden. Für die eindeutige Identifizierbarkeit der Datenträger MUSS ein eindeutiges Ordnungskriterium vergeben werden. Werden Datenträger zur Vervielfältigung und Weitergabe von VS genutzt, so MÜSSEN diese wie entsprechende Papier-VS gehandhabt werden.

Datenträger, beispielsweise Backup-Datenträger oder USB-Sticks, auf denen VS gespeichert sind, die nicht mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, MÜSSEN entsprechend des höchsten mit dem Datenträger verarbeiteten Geheimhaltungsgrad geschützt werden.

Die Räume und Bereiche, in denen Komponenten der VS-IT stehen, die VS verarbeiten, MÜSSEN entsprechend dem höchsten Geheimhaltungsrad der verarbeitenden VS materiell abgesichert sein (vgl. CON.11.2.A16 *Absicherung von VS-IT-Räumen und -Bereichen nach §§ 38, 39, 45 VSA*).

CON.11.2.A22 Zusammenschaltung von VS-IT nach § 58 VSA (B)

Bevor VS-IT mit anderer VS-IT zusammengeschaltet werden darf, MUSS geprüft werden, ob und inwieweit Informationen zwischen der zusammengeschalteten VS-IT ausgetauscht werden dürfen. Bei der Prüfung MUSS das jeweilige Schutzniveau und der Grundsatz „Kenntnis nur, wenn nötig" berücksichtigt werden.

Abhängig vom Ergebnis der Prüfung MÜSSEN IT-Sicherheitsfunktionen zum Schutz der Systemübergänge implementiert werden (siehe CON.11.2.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA*). Vor der Zusammenschaltung der VS-IT MUSS bewertet und dokumentiert werden, ob:

- diese für das angestrebte Szenario zwingend erforderlich ist,
- durch die Zusammenschaltung eine besondere Gefährdung der einzelnen Teilsysteme entsteht und
- der durch die Zusammenschaltung von VS-IT entstandene Gesamtbestand der Daten höher einzustufen ist.

Falls der Gesamtbestand der Daten höher einzustufen ist, dann MUSS geprüft werden, ob weitere Geheimschutzmaßnahmen notwendig werden. Falls ein Sicherheitsgefälle zwischen der zusammengeschalteten VS-IT besteht, dann SOLLTE der Verbindungsaufbau aus der VS-IT heraus erfolgen, mit der die höher eingestufte VS verarbeitet wird.

Wird VS-IT direkt oder kaskadiert mit VS-IT für die Verarbeitung von VS des Geheimhaltungsgrades STRENG GEHEIM gekoppelt, dann MUSS sichergestellt werden, dass keine Verbindungen zu ungeschützten oder öffentlichen Netzen hergestellt werden.

CON.11.2.A23 Wartungs- und Instandsetzungsarbeiten von VS-IT nach § 3 Abs. 3 (B)

Für alle Komponenten der VS-IT MUSS im Vorhinein festgelegt werden:

- welche Wartungsarbeiten durch das Wartungspersonal erfolgen dürfen und
- ab wann der Hersteller in die Wartung miteinbezogen werden muss.

Sobald Wartungs- und Instandsetzungsarbeiten an Komponenten der VS-IT anstehen, MÜSSEN die Geheimschutzbeauftragten darüber informiert werden. Die Geheimschutzbeauftragten MÜSSEN in die Lage versetzt werden, zu entscheiden, ob es sich dabei um eine geheimschutzrelevante Änderung handelt. Falls es sich um eine geheimschutzrelevante Änderung handelt, DÜRFEN die Arbeiten NICHT durchgeführt werden, bevor die Geheimschutzbeauftragten den Änderungen zugestimmt haben.

Die Wartungs- und Instandsetzungsarbeiten an Komponenten der VS-IT SOLLTEN innerhalb der eigenen Dienstliegenschaft durchgeführt werden. Ist dies nicht möglich, MUSS sichergestellt werden, dass die Anforderungen der VSA sowohl während des Transports als auch bei den Wartungs- und Instandsetzungsarbeiten erfüllt werden.

Während der Wartungs- und Instandsetzungsarbeiten SOLLTE die Verarbeitung von VS in dem von der Wartung betroffenen Bereich der VS-IT eingestellt werden. Ist dies nicht möglich, MUSS während des Zeitraums der Wartungs- und Instandsetzungsarbeiten lückenlos sichergestellt werden, dass keine VS abfließen können.

Falls Wartungs- oder Instandsetzungsarbeiten an abstrahlvermessenen Komponenten der VS-IT durchgeführt wurden, dann MUSS geprüft werden, ob eine erneute Abstrahlmessung notwendig wird (vgl. CON.11.2.A20 *Abstrahlschutzmaßnahmen nach § 57 VSA*).

CON.11.2.A24 Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B)

Vor dem erstmaligen Einrichten der MUSS geprüft werden, ob eine Fernwartung von VS-IT zwingend notwendig ist. Die IT, mit der die Fernwartung durchgeführt wird, sowie die Übertragungsstrecken MÜSSEN als VS-IT behandelt und als Schutzobjekte definiert werden.

Die Übertragungsstrecken zwischen den zur Fernwartung verwendeten Arbeitsplätzen und der zu administrierten VS-IT MÜSSEN gemäß der Anforderung CON.11.2.A12 *Elektronische Übertragung von VS nach §§ 24, 53, 55 VSA* abgesichert werden.

Falls die Fernwartung nicht durch ermächtigte oder zugelassene Mitarbeitende der Dienststelle selbst durchgeführt wird, dann MUSS die Dienststelle

- die Fernwartungsverbindung auf- und abbauen,
- die durchgeführten Arbeiten dauerhaft überwachen und
- in der Lage sein, die Verbindung bei Auffälligkeiten auch während der Wartung zu unterbrechen.

Das Auf- und Abbauen der Fernwartungsverbindung SOLLTE unter Beachtung des 4-Augen-Prinzips durchgeführt werden.

Für die Fernwartung von VS-IT MUSS ein Informationssicherheitskonzept erstellt werden, das alle Komponenten, die an der Fernwartung beteiligt sind, berücksichtigt. Hierbei MÜSSEN insbesondere die Netzübergänge und die VS-IT, aus dem die Fernwartung gesteuert wird, betrachtet werden.

3.2. Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Gesetzliche Grundlage für den Geheimschutz bildet das „Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG).“

Die auf der Grundlage des SÜG erlassene „Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA)“ enthält die Vorgaben für den materiellen Geheimschutz in der Bundesverwaltung.

Das BMWK veröffentlicht für den nichtöffentlichen Bereich das Geheimschutzhandbuch der Wirtschaft (GHB).

Das BSI gibt zur Umsetzung der VSA Technische Leitlinien heraus. Die BSI-TL-03304, "Anforderungen an abstrahlsichere IT-Räume" und die BSI TL - M 50 „Löschen und Vernichten von Verschlusssachen auf Datenträgern“ sind über die zuständigen Geheimschutzbeauftragten zu beziehen.

Die Listen der zugelassenen Geräte BSI-TL-03305, "Liste abstrahlgeprüfter Produkte nach dem Nationalen Zonenmodell", die "Liste abstrahlgeprüfter Produkte nach SDIP 27 Level A" und die BSI-TR-03209-x, "Elektromagnetische Schirmung von Gebäuden", sind auf der BSI-Webseite veröffentlicht.

Das BSI gibt mit der „BSI-Schrift 7164“ eine Liste heraus, die alle IT-Sicherheitsprodukte mit gültiger Zulassungsaussage auflistet. Diese Liste ist auf der BSI-Webseite veröffentlicht.

Die BSI TL – IT 01 „Mitwirkungspflichten in Zulassungsverfahren“ regelt die Mitwirkungspflichten der an Zulassungsverfahren für IT-Sicherheitsprodukte (VS-Produkt) im Zulassungsschema des BSI beteiligten Parteien und ist auf der BSI-Webseite veröffentlicht.

Weitergehende Informationen zur Zulassung von IT-Sicherheitsprodukten und einer genaueren Beschreibung der einzelnen IT-Sicherheitsfunktionen bietet das Dokument „VS-Produktkatalog des BSI“, das auf der BSI-Webseite veröffentlicht ist.

Die Grundsätze ordnungsgemäßer Aktenführung sind in der „Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien“, die vom BMI herausgegeben wird, festgelegt.