Bundesamt
für Sicherheit in der
Informationstechnik

Community Draft

CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

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 bis zum Geheimhaltungsgrad VS-NUR FÜR DEN

DIENSTGEBRAUCH (VS-NfD) festzulegen und gemeinsam mit den Informationssicherheitsbeauftragten in das Sicherheitskonzept zu integrieren.

1.3. Abgrenzung und Modellierung

Der Baustein CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* ist einmal auf den Informationsverbund der VS-IT anzuwenden, falls VS des Geheimhaltungsgrades VS-NfD verarbeitet werden oder werden sollen. Falls in einem Teil des Informationsverbundes eine Zusammenstellung von VS vorliegt, dann sind für diesen Teilverbund die Anforderungen des Bausteins CON.11.2 *Geheimschutz VS-VERTRAULICH* oder höher zu berücksichtigen. Eine Zusammenstellung liegt vor, falls einzelne Teile VS-NfD eingestuft sind, die jedoch in ihrer Gesamtheit VS-VERTRAULICH sind. Sollen hingegen auch VS der Geheimhaltungsgrade VS-VERTRAULICH oder höher verarbeitet werden, dann darf dieser Baustein nicht angewendet werden. Stattdessen ist der Baustein CON.11.2 *Geheimschutz VS-VERTRAULICH oder höher* anzuwenden. Dieser Baustein 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. Eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz kann bei Berücksichtigung dieses Bausteins eine Voraussetzung für die Freigabe von VS-IT für die Verarbeitung von VS des Geheimhaltungsgrades VS-NfD nach VSA sein. 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,
- VS-IT-Dokumentation,
- Handhabung elektronischer VS,
- 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 der Geheimhaltungsgrade VS-VERTRAULICH oder höher eingesetzt werden sollen (siehe *CON.11.2 Geheimschutz VS-VERTRAULICH oder höher*),
- die bauliche und technische Absicherung von Gebäuden und Räumen, in denen VS des Geheimhaltungsgrades VS-NfD verarbeitet werden, diese werden in den entsprechenden Bausteinen der Schicht INF *Infrastruktur* behandelt,
- 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.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* 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 VS-IT-Dokumentation 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 VS-IT-Dokumentation 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 Geheimhaltungsgrades VS-NfD können für die Bundesrepublik Deutschland oder eines ihrer Länder von Nachteil sein. Diese können je nach Art der als VS eingestuften Informationen unterschiedlich ausfallen. Wenn beispielsweise eingestufte Netzpläne oder Informationssicherheitskonzepte offengelegt werden, dann können diese Informationen genutzt werden, um in IT-Systeme einzudringen. Erhalten Unbefugte beispielsweise Kenntnis von diplomatischen Informationen über ein anderes Land, dann kann dies die diplomatischen Beziehungen zwischen Deutschland und diesem Land belasten.

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 strategischen Vorteil gegenüber der Bundesrepublik Deutschland oder eines ihrer Länder verschaffen. Beispielsweise könnten andere Staaten diese Informationen nutzen, um ihre Verhandlungsposition gegenüber der Bundesrepublik Deutschland zu stärken. 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 und -täterinnen

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. Dies kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein. 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.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* aufgeführt. Die Gesamtverantwortung für den Geheimschutz trägt die jeweilige Dienststellenleitung. 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.11.1.A1 Einhaltung der Grundsätze zur VS-Verarbeitung mit IT nach § 3, 4 und 6 und Nr. 1 Anlage V zur 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.11.1.A2 Erstellung und Fortschreibung der VS-IT-Dokumentation nach § 12 und Nr. 2.2 Anlage II zur VSA (B)

Jede Dienststelle, die VS-IT einsetzt, MUSS als Teil der Geheimschutzdokumentation eine VS-IT-Dokumentation erstellen. Die VS-IT-Dokumentation MUSS alle Dokumente beinhalten, die in Nr. 2.2 Anlage II zur VSA aufgeführt sind.

Die VS-IT-Dokumentation 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.11.1.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.11.1.A4 Beschaffung von VS-IT und Beauftragung von Dienstleistern nach §§ 25, 49 und Anlage V Nr. 6.6 zur 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,
- 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.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA*). In diesem Fall MUSS die Befristung der Zulassungsaussage des IT-Sicherheitsproduktes 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 MUSS ein Vertrag geschlossen werden, in dem die Bestimmungen des VS-NfD-Merkblatts des Handbuchs für den Geheimschutz in der Wirtschaft (Geheimschutzhandbuch) Eingang gefunden haben.

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

CON.11.1.A5 Verpflichtung bei Zugang zu VS nach § 4 VSA und Anlage V zur VSA (B)

Bevor eine Person Zugang zu VS des Geheimhaltungsgrades VS-NfD erhält, MUSS sie auf Anlage V zur VSA verpflichtet werden. Ein Exemplar der Anlage V zur VSA MUSS jeder Person gegen Empfangsbestätigung zugänglich gemacht werden.

Wird Personal von nichtöffentlichen Stellen Zugang zu VS gewährt, so MUSS Nr. 6.6 Anlage V zur VSA beachtet werden. Von der Verpflichtung einer Person DARF NUR abgesehen werden, falls an VS-IT nur kurzzeitig gearbeitet und währenddessen ein Zugriff auf VS ausgeschlossen werden kann.

CON.11.1.A6 Beaufsichtigung und Begleitung von Fremdpersonal für VS-IT nach §§ 3, 4 VSA (B)

Nicht verpflichtetes Fremdpersonal, das sich Zutritt zu Räumen und Bereichen mit VS-IT aber keinen Zugriff auf VS verschaffen kann, MUSS während der gesamten Zeit begleitet und beaufsichtigt werden. Falls ein Zugriff auf VS nicht ausgeschlossen werden kann, MUSS das Fremdpersonal verpflichtet sein (vgl. CON.11.1.A5 *Verpflichtung bei Zugang zu VS nach § 4 VSA und Anlage V zur VSA*). Die beaufsichtigenden Personen MÜSSEN über die notwendigen Fachkenntnisse verfügen, um die Tätigkeiten kontrollieren zu können. Für Fremdpersonal von nichtöffentlichen Stellen MÜSSEN die Vorgaben des Geheimschutzhandbuches der Wirtschaft beachtet werden.

CON.11.1.A7 Kennzeichnung von elektronischen VS und Datenträgern nach §§ 20, 54 und Anlage III, V und VIII 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 diese 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. E-Mails MÜSSEN entsprechend des Musters 11 der Anlage VIII zur VSA gekennzeichnet werden.

Falls eine elektronische Kennzeichnung von VS (im Sinne von Metadaten) verwendet werden soll, dann MUSS geprüft werden, ob diese IT-Sicherheitsfunktionen übernimmt (siehe CON.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA)*.

Datenträger, auf denen elektronische VS des Geheimhaltungsgrades VS-NfD durch Produkte ohne Zulassungsaussage verschlüsselt gespeichert sind, MÜSSEN mit dem Geheimhaltungsgrad der darauf gespeicherten VS gekennzeichnet werden. Falls sich durch die Zusammenstellung der VS auf dem Datenträger ein Datenbestand ergibt, der eine höhere Einstufung erforderlich macht, dann MUSS der Datenträger selbst als VS des Geheimhaltungsgrades VS-VERTRAULICH behandelt und gekennzeichnet werden.

CON.11.1.A8 Verwaltung und Nachweis von elektronischen VS nach § 21 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 (keine Nachweisführung für VS des Geheimhaltungsgrades VS-NfD erforderlich). Elektronische VS, die als VS-NfD eingestuft sind, DÜRFEN NUR unter Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig" in offenen (elektronischen) Registraturen verwaltet werden.

CON.11.1.A9 Speicherung elektronischer VS nach § 23 und Nr. 5 Anlage V zur VSA (B)

Elektronische VS MÜSSEN mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt gespeichert oder entsprechend den Vorgaben der VSA materiell gesichert werden (siehe CON.11.1.A15 *Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA*).

CON.11.1.A10 Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA (B)

Falls VS elektronisch übertragen werden sollen, MÜSSEN die Regelungen der VSA zur Weitergabe von VS (§ 24 VSA) eingehalten werden. Für die Weitergabe an Parlamente, Landesbehörden und nicht öffentliche Stellen MÜSSEN zusätzlich die besonderen Regelungen nach §§ 25 und 26 VSA beachtet werden.

Die VS-IT aller Kommunikationspartner MUSS für die Verarbeitung von VS des Geheimhaltungsgrades VS-NfD freigegeben sein. Werden VS elektronisch übertragen, MÜSSEN sie grundsätzlich durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt werden. Auf eine Verschlüsselung DARF NUR verzichtet werden, falls:

- die verwendete VS-IT nach § 50 VSA freigegeben wurde,
- sich der Versender vergewissert hat, dass der Empfänger nach § 24 Abs. 2 zur Annahme oder Kenntnisnahme der VS berechtigt ist und
- auch das Transportnetz und die VS-IT des Empfängers nach § 50 VSA freigeben sind.

Es DARF NUR innerhalb von Räumen und Bereichen, die gegen unkontrollierten Zutritt geschützt sind, von einem Zugriffsschutz ausgegangen werden.

VS DÜRFEN NUR in Ausnahmefällen nach § 55 Abs. 3-5 VSA unter Einhaltung der dort genannten Anforderungen und Vorsichtsmaßnahmen auf anderem Wege elektronisch übertragen werden. Falls im Vorhinein zu erwarten ist, dass VS elektronisch übertragen werden könnten, DARF die Ausnahmeregelung nach § 55 VSA NICHT angewendet werden.

Falls die VS an nichtdeutsche Stellen übertragen werden soll, MUSS geprüft werden, ob es 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.11.1.A11 Mitnahme elektronischer VS nach § 28 VSA und Nr. 7 Anlage V zur VSA (B)

Elektronische VS DÜRFEN NUR auf Dienstreisen und zu Dienstbesprechungen mitgenommen werden, soweit dies dienstlich notwendig ist und sie angemessen gegen unbefugte Kenntnisnahme gesichert werden. Werden diese persönlich mitgenommen, MÜSSEN diese folgendermaßen gespeichert werden:

- auf hierfür freigegebener VS-IT,
- auf einem Datenträger, der in einem verschlossenen Umschlag transportiert wird,

- auf einem Datenträger, der mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurde, oder
- durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt, falls der Datenträger selbst nicht durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurde.

Falls VS des Geheimhaltungsgrades VS-NfD in Privatwohnungen verarbeitet werden sollen, dann DÜRFEN diese NUR elektronisch mit hierfür freigegebener VS-IT verarbeitet werden.

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 Exportkontrollgesetzgebung 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 oder der eigenen Geheimschutzbeauftragten erfolgen.

CON.11.1.A12 Archivierung elektronischer VS nach §§ 30, 31 VSA (B)

VS MÜSSEN entsprechend dem Bundesarchivgesetz wie nicht eingestufte Informationen ausgesondert werden. Schon bei Einführung von Systemen zur elektronischen Schriftgutverwaltung und Vorgangsbearbeitung MÜSSEN die technischen Verfahren zur Aussonderung frühzeitig mit dem zuständigen Archiv abgestimmt werden. Falls das zuständige Archiv VS nicht übernehmen möchte, MÜSSEN VS gemäß CON.11.1.A13 *Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur VSA* sicher gelöscht bzw. vernichtet werden.

CON.11.1.A13 Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur 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.11.1.A14 Zugangs- und Zugriffsschutz nach § 3 VSA (B)

Die VS-IT MUSS so geschützt werden, dass ein Zugang zur VS-IT und ein Zugriff auf VS nur für verpflichtete Personen (siehe CON.11.1.A5 *Verpflichtung bei Zugang zu VS nach § 4 und Anlage V zur VSA*) möglich ist. Der Schutz der VS MUSS sichergestellt werden über:

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

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

CON.11.1.A15 Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA (B)

Datenträger und IT-Produkte MÜSSEN bei Nichtgebrauch in verschlossenen Behältern oder Räumen aufbewahrt werden, falls:

- der Datenträger bzw. das IT-Produkt selbst als VS-NfD eingestuft ist,

- auf dem Datenträger bzw. IT-Produkt unverschlüsselte VS des Geheimhaltungsgrades VS-NfD gespeichert sind oder
- auf dem Datenträger bzw. IT-Produkt VS des Geheimhaltungsgrades VS-NfD durch ein Produkt ohne Zulassungsaussage verschlüsselt gespeichert sind.

CON.11.1.A16 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.11.1.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 Informationen höher einzustufen ist.

Falls der Gesamtbestand der Informationen höher einzustufen ist, dann MUSS der IT-Grundschutz-Baustein *CON.11.2 Geheimschutz VS-VERTRAULICH oder höher* angewendet werden.

Wird VS-IT für die Verarbeitung von VS des Geheimhaltungsgrades VS-NfD 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.11.1.A17 Wartungs- und Instandsetzungsarbeiten von VS-IT nach § 3 Abs. 3 VSA (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.

Nach Abschluss der Wartungs- und Instandsetzungsarbeiten MUSS der oder die Geheimschutzbeauftragte bewerten, ob sich geheimschutzrelevante Änderungen an der VS-IT ergeben haben.

CON.11.1.A18 Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B)

Vor dem erstmaligen Einrichten der Fernwartungsverbindung 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.11.1.A10 *Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA* abgesichert werden.

Falls die Fernwartung nicht durch Mitarbeitende der Dienststelle selbst durchgeführt wird, dann SOLLTE die Dienststelle die Fernwartungsverbindung auf- und abbauen. Zusätzlich MUSS die Dienststelle

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

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.

CON.11.1.A19 Verwendung von Videokonferenzsystemen (B)

Falls ein Videokonferenzsystem für die Verarbeitung von VS verwendet werden soll, dann MÜSSEN die Vorgaben der BSI TL - L 15 eingehalten 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 - M 50 „Löschen und Vernichten von Verschlusssachen auf Datenträgern“ und die BSI TL - L 15 „Videokonferenz VS-NfD“ sind über die zuständigen Geheimschutzbeauftragten zu beziehen.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.

Änderungsdokument zum Baustein CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

Kapitel 1.1: Einleitung

- Die Voraussetzungen für den Einsatz von VS-IT wurden an die novellierte Fassung der VSA angepasst.

Kapitel 1.2: Zielsetzung

- Konkretisierung der Zielsetzung, dass die Anforderungen des Geheimschutzes im Sicherheitskonzept nach IT-Grundschutz berücksichtigt werden sollen.

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung gegenüber dem Baustein CON.11.2 Geheimschutz VS-VERTRAULICH oder höher.
- Ergänzung der Information welcher Baustein im Falle einer Zusammenstellung von VS zu verwenden ist, falls die Gesamtheit der Zusammenstellung VS-VERTRAULICH einzustufen ist.
- Ergänzung des Verweises auf die Bausteine ORP.4 Identitäts- und Berechtigungsmanagement und CON.9 Informationsaustausch.
- Ergänzung der Informationen, dass dieser Baustein keine speziellen Anforderungen aus einschlägigen Bestimmungen über- oder zwischenstaatlicher Organisationen sowie bilateraler Geheimschutzabkommen enthält.
- Ergänzung der Information, dass dieser Baustein die Sicherheitsakkreditierung für die Verarbeitung von Verschlusssachen über- oder zwischenstaatlicher Organisationen mit VS-IT nicht behandelt.

Kapitel 3: Anforderungen

Neue Anforderungen

- CON.11.1.A19 *Verwendung von Videokonferenzsystemen*

Änderungen an bestehenden Anforderungen

- CON.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B):* Die Anforderung wurde gekürzt und verweist nun auf die drei relevanten Dokumente.
- CON.11.1.A4 *Beschaffung von VS-IT und Beauftragung von Dienstleistern nach §§ 25, 49 und Anlage V Nr. 6.6 zur VSA (B):* Die Anforderung wurde um den Aspekt der Beauftragung von Dienstleistern erweitert.
- CON.11.1.A6 *Beaufsichtigung und Begleitung von Fremdpersonal für VS-IT nach §§ 3, 4 VSA (B):* Die Anforderung wurde um die Berücksichtigung der Vorgaben des Geheimschutzhandbuches der Wirtschaft erweitert.
- CON.11.1.A10 *Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA (B):* Die Anforderung wurde an die Vorgaben der novellierten VSA angepasst. Zusätzlich wurde die Anforderung um den Aspekt zur Übertragung an nichtdeutsche Stellen erweitert.
- 11.1.A11 Mi*tnahme elektronischer VS nach § 28 VSA und Nr. 7 Anlage V zur VSA (B*): Die Anforderung wurde um den Aspekt der Mitnahme von VS-IT ins Ausland ergänzt.
- CON.11.1.A13 *Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur VSA (B)*: Die Anforderung wurde an die neuen Vorgaben des VS-Produktkataloges angepasst.
- 11.1.A17 *Wartungs- und Instandsetzungsarbeiten von VS-IT nach § 3 Abs. 3 VSA (B):* Die Anforderung wurde um den Aspekt ergänzt, dass im Vorhinein festzulegen ist welche Wartungstätigkeiten an den Komponenten der VS-IT durchgeführt werden können. Zusätzlich wurden die Aspekte zu den geheimschutzrelevanten Änderungen konkretisiert und an die novellierte VSA angepasst.
- 11.1.A18 *Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B):* Die Anforderung wurde dahingehend konkretisiert, dass zwischen Mitarbeitenden der Dienststelle und externen Mitarbeitenden unterschieden wird.

Kapitel 4: Weiterführende Informationen

- Ergänzung von Hinweisen zum wichtigem Thema Einsatz von IT-Sicherheitsprodukten.
- Ergänzung von Informationen zum Abruf der Technischen Leitlinien