



# 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 ein Informationssicherheitskonzept nach den BSI-Standards des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik 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 den Informationssicherheitskonzepten 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 Informationssicherheitskonzept zu integrieren.

### 1.3. Abgrenzung und Modellierung

Der Baustein CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* ist einmal auf den gesamten Informationsverbund der VS-IT anzuwenden, falls VS des Geheimhaltungsgrades VS-NfD verarbeitet werden oder werden sollen. 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. Aus diesem Grund ersetzt eine ISO27001-Zertifizierung auf Basis von IT-Grundschutz nicht die Freigaben 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,
- 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*,
- CON.6 *Löschen und Vernichten* 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,
- 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 sowie
- den Freigabeprozess für 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 einige 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 Geheimhaltungsgrad 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 möchten Nachrichtendienste möglichst unbemerkt an für sie interessante Informationen, wie z. B. VS, 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 und -täterinnen werden interne Informationen, wie z. B. VS, durch interne oder externe Mitarbeitende bewusst entwendet und gegebenenfalls an Dritte verkauft oder veröffentlicht. Innentäter und -täterinnen 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 und -täterinnen fühlen sich moralisch dazu verpflichtet, Informationen, die als VS eingestuft sind, zu veröffentlichen, um damit beispielsweise Missstände aufzudecken.
- Die Innentäter und -täterinnen wurden von einem Nachrichtendienst angeworben.
- Die Innentäter und -täterinnen 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 Innentäter und -täterinnen agieren, erschweren den Schutz vor einem solchen Angriff. Viele der zum Schutz vor Angriffen eingesetzten Maßnahmen sind gegen den Angriff durch Innentäter und -täterinnen 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 Geheimschutzbeauftragte 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	Geheimchutzbeauftragte
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 des Geheimhaltungsgrades VS-NfD **DÜRFEN NUR** mit VS-IT verarbeitet, die hierfür freigegeben ist. 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 Geheimchutzdokumentation eine VS-IT-Dokumentation erstellen. Die VS-IT-Dokumentation **MUSS** alle Dokumente beinhalten, welche in Nr. 2.2 Anlage II zur VSA aufgeführt sind.

Die VS-IT-Dokumentation **MUSS** bei allen geheimchutzrelevanten Änderungen aktualisiert werden. Sie **MUSS** zudem mindestens alle drei Jahre auf Aktualität, Vollständigkeit und Erforderlichkeit bestehender und noch zu treffender Geheimchutzmaßnahmen überprüft werden.

### **CON.11.1.A3 Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B)**

Auf Basis der im VS-Produktkatalog für einzelne Produkttypen vom BSI festgelegten Zulassungsrelevanz und insbesondere basierend auf den Ergebnissen der Strukturanalyse MÜSSEN alle für die geplante VS-IT relevanten IT-Sicherheitsfunktionen identifiziert werden. Diese lassen sich den folgenden Kategorien gemäß § 52 VSA zuordnen:

- Zugangs- und Zugriffskontrolle,
- Identifikation und Authentisierung,
- kryptographische Unterstützung,
- Sicherheitsmanagement,
- Informationsflusskontrolle,
- interner Schutz der Benutzerdaten,
- Selbstschutz der Sicherheitsfunktionen und ihrer Daten,
- Netztrennung,
- Schutz der Unversehrtheit,
- Verfügbarkeitsüberwachung oder
- Sicherheitsprotokollierung und Nachweisführung.

Anschließend MÜSSEN die identifizierten IT-Sicherheitsfunktionen den jeweiligen Teilkomponenten der VS-IT unter Berücksichtigung des VS-Produktkataloges des BSI zugeordnet werden. Jede identifizierte und für den Schutz von VS wesentlich verantwortliche Teilkomponente MUSS als IT-Sicherheitsprodukt gemäß VSA festgelegt und behandelt werden

Sofern das identifizierte IT-Sicherheitsprodukt einem Produkttyp angehört für das eine Zulassungsaussage gemäß BSI TL - IT 01 erforderlich ist, MUSS ein entsprechendes Produkt gemäß BSI Schrift 7164 (Liste der zugelassenen Produkte) verwendet werden. Sofern dort keine IT-Sicherheitsprodukte gelistet sind, MUSS Kontakt mit der Zulassungsstelle des BSI aufgenommen werden. Bei der Verwendung von IT-Sicherheitsprodukten mit Zulassungsaussage MÜSSEN zusätzlich die Bestimmungen des BSI für den Einsatz und Betrieb (SecOPs) des jeweiligen Produktes eingehalten werden.

### **CON.11.1.A4 Beschaffung von VS-IT nach § 49 VSA (B)**

Bevor VS-IT beschafft wird, MUSS sichergestellt werden, dass deren Sicherheit während des gesamten Lebenszyklus ab dem Zeitpunkt, zu dem fest steht, 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 und
- Löschung von elektronischer VS sowie
- Aussonderung,
- Wartung und Instandsetzung von VS-IT

berücksichtigt werden. Sofern einem zu beschaffenden IT-Produkt eine IT-Sicherheitsfunktion zugeordnet ist, SOLLTE ein IT-Produkt aus der Liste der zugelassenen IT-Sicherheitsprodukte beschafft

werden. Wird stattdessen ein Produkt ohne Zulassungsaussage ausgewählt, dann SOLLTE im Vorhinein mit dem BSI abgeklärt werden, ob es zugelassen werden kann. Zusätzlich SOLLTE in der Ausschreibung aufgenommen werden, dass der Hersteller an einem Zulassungsverfahren mitwirken muss (siehe BSI TL - IT 01). Verträge MÜSSEN derart gestaltet werden, dass bei einer Rückgabe von defekten oder geleasteten IT-Produkten deren Datenträger oder sonstige Komponenten, auf denen VS gespeichert sein könnten, im Besitz der Dienststelle verbleiben.

### **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 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 an VS-IT arbeitet, MUSS während der gesamten Zeit begleitet und beaufsichtigt werden. Die begleitenden Personen MÜSSEN über die notwendigen Fachkenntnisse verfügen, um die Tätigkeiten kontrollieren zu können.

### **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 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. 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, welcher 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 Geheimhaltungsgrads 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:

- VS ausschließlich leitungsgebunden übertragen werden und die Übertragungseinrichtungen, einschließlich Kabel und Verteiler, gegen unbefugten Zugriff geschützt sind, oder
- neben den Hausnetzen zusätzlich das Transportnetz für die Verarbeitung von VS freigegeben ist.

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. 2-4 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.

## **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.

## **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 abgesprochen 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 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 VS oder Datenträger zu löschen, die mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, MUSS der Schlüssel unter Beachtung der SecOPs gelöscht werden.

Sollen elektronische VS gelöscht werden, die nicht durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, dann MUSS der gesamte Datenträger oder das IT-Produkt, auf dem VS gespeichert sind, mittels eines IT-Sicherheitsprodukts mit Zulassungsaussage gelöscht werden.

Die Datenträger oder IT-Produkte MÜSSEN gelöscht werden, bevor sie die gesicherte Einsatzumgebung dauerhaft verlassen. Sie MÜSSEN physisch vernichtet werden, falls sie nicht gelöscht werden können. Für die Vernichtung 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)**

VS-IT, die für VS-NfD eingestufte VS eingesetzt wird, 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 zusammenschaltet werden darf, MUSS geprüft werden, ob und inwieweit Informationen zwischen der zusammenschalteten 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 und ob durch die Zusammenschaltung eine besondere Gefährdung der einzelnen Teilsysteme entsteht. Es MUSS geprüft werden, ob der durch

die Zusammenschaltung von VS-IT entstandene Gesamtbestand der Daten höher einzustufen ist und weitere Geheimschutzmaßnahmen notwendig werden.

Wird VS-IT für die Verarbeitung von VS des Geheimhaltungsgrads 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)**

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)**

Wird VS-IT ferngewartet, dann MUSS die Fernwartungsverbindung verschlüsselt sein. Für die Verschlüsselung MÜSSEN IT-Sicherheitsprodukte mit Zulassungsaussage eingesetzt werden.

Die IT, mit der die Fernwartung durchgeführt wird, sowie die Übertragungstrecken MÜSSEN als VS-IT behandelt und als Schutzobjekte definiert werden.

Die Fernwartungsverbindung MUSS durch die Dienststelle auf- und abgebaut werden. Die Dienststelle MUSS 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.

## **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.

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

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

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