Anlage 7 zur VS-Anweisung

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

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

I. Allgemeines

1. Zugangsberechtigung und Weitergabe

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

Weitergehende Maßnahmen wie ein Geheimschutzverfahren des Bundesministeriums für Wirtschaft und Technologie (BMWi), Sicherheitsüberprüfungen oder formale Besuchsanmeldungen sind bei diesem Geheimhaltungsgrad nicht erforderlich.

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

1.3. Die Weitergabe von als VS -NfD eingestuften VS darf nur an Regierungsstellen, zwischenstaatliche Organisationen oder Auftragnehmer erfolgen, die an einem Programm/Projekt/Auftrag beteiligt sind und die Zugang zu den Informationen im Zusammenhang mit der Bearbeitung des Programms/Projekts/Auftrags haben müssen. Vor der Weitergabe von VS-NfD eingestuften VS an nicht beteiligte zwischenstaatliche Organisationen oder Auftragnehmer aus nicht beteiligten Ländern ist die schriftliche Einwilligung des amtlichen VS-Auftraggebers der VS einzuholen. Grundsätzlich bedarf es hierbei einer Geheimschutzvereinbarung (Siehe auch § 23 VSA).

1.4. In Deutschland kann sich das BMWi beim VS-Auftragnehmer über die Einhaltung der Bestimmungen dieses Merkblattes vergewissern. Ist Auftraggeber eine Behörde, kann auch diese die Kontrollrechte nach Satz 1 wahrnehmen.

1.5. Die VS-Einstufung ist dreißig Jahre nach dem 1. Januar des auf die Einstufung folgenden Jahres aufgehoben, sofern keine andere Frist bestimmt ist. Bei internationalen Aufträgen ist das BMWi zu konsultieren, sofern keine Programm - oder Projektvereinbarungen bestehen (Siehe auch § 26 VSA) .

2. Bearbeitungsmaßnahmen

2.1. Kennzeichnung und Handhabung bzw. Verwahrung

Dokumente und Material des Geheimhaltungsgrades VS-NfD sind wie folgt zu kennzeichnen, zu behandeln und zu verwahren:

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

2.1.2. VS-NfD eingestuftes Material (z.B. Gerät, Ausrüstung) oder Datenträger (z.B. Disketten, CDs, Mikrochips, Mikrofiche) sind ebenfalls entweder deutlich sichtbar am Material selbs t oder – falls dies nicht möglich ist – an den Aufbewahrungsbehältnissen des Materials zu kennzeichnen bzw. grundsätzlich umzustempeln.

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

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

2.2. Weitergabe

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

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

2.3. Vernichtung/Rückgabe

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

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

2.4 Verlust, unbefugte Weitergabe, Auffinden von VS oder Nichtbeachtung des Merkblatts

Der Verlust, die unbefugte Weitergabe sowie das Auffinden von VS oder die Nichtbeachtung dieses Merkblattes ist unverzüglich dem deutschen VS-Auftraggeber und ggf. dem BMWi mitzuteilen, um einen eventuell entstandenen Schaden zu begrenzen und den Vorfall aufzuklären.

2.5. Besuche

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

2.6. Aufträge

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

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

2.6.3. VS-Auftragnehmer/-Unterauftragnehmer im Ausland sind vertraglich zu verpflichten, die Vorschriften ihrer zuständigen Sicherheitsbehörde für die Behandlung von VS vergleichbaren Geheimhaltungsgrades zu beachten. Gibt es keinen vergleichbaren Geheimhaltungsgrad in dem Land eines VS-Auftragnehmers/-Unterauftragnehmers, ist das BMWi einzuschalten, das Regelungen für den Schutz mit der zuständigen ausländischen Sicherheitsbehörde vereinbart. Die Weitergabe darf dann erst nach Zustimmung des BMWi erfolgen.

II. Nutzung von Informationstechnik (IT)

1. Bearbeitung

1.1. Wird IT für die Bearbeitung von VS-NfD eingestuften VS genutzt, sind zum Schutz der VS (entsprechend Teil I 1.1 und 1.2) geeignete informationstechnische Maßnahmen und / oder materielle und orga nisatorische Maßnahmen zu treffen.

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

1.3. Bei der Bearbeitung von VS-NfD eingestuften VS kommen insbesondere folgende Maßnahmen in Betracht:

• Übersicht über die Zugriffsberechtigungen,
• Nutzung von Identifizierungs - und Authentisierungsmechanismen (z.B. Login, Passwort), • geeignete IT-Sicherheitsanweisung (einzelplatz- oder unternehmensbezogen).

Funktastaturen und Funk-Netzwerke dürfen nur eingesetzt werden, wenn sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind.

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

1.5 Transportable Datenträger (z.B. Disketten, CDs, Wechselplatten), die VS-NfD eingestufte Daten unkryptiert enthalten, sind gemäß Teil I 2.1.2 zu kennzeichnen und gemäß Teil I 2.1.3 aufzubewahren.

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

1.7 Informationstechnik und Datenträger sind auf Virenbefall (insbesondere Trojanische Pferde oder Würmer) zu überprüfen bevor VS-NfD damit bearbeitet werden. Diese Prüfung ist in regelmäßigen Zeitabständen zu wiederholen.

1.8 Private Informationstechnik (z.B. Laptops), Software oder Datenträger dürfen nicht für die Bearbeitung eingesetzt werden. In für VS-NfD genutzten Informationssystemen dürfen keine private Software oder private Datenträger verwendet werden.

1.9 Auf fest installierten Datenträgern, die VS-NfD eingestufte Daten unkryptiert enthalten, sind die Verschlusssachen gemäß 1.6 zu löschen, bevor die Datenträger im Rahmen von Wartungs- oder Reparaturarbeiten an IT-Systemkomponenten den Bereich der zugriffsberechtigten Personen verlassen. Ist eine Löschung nicht möglich, sind die Datenträger auszubauen und zurückzubehalten bzw. ist die Wartungs -/Reparaturfirma vertraglich auf die Einhaltung der Regeln dies es Merkblattes zu verpflichten.

2. Übertragung

2.1. Bei der elektronischen Übermittlung auf Telekommunikations - oder anderen technischen Kommunikationsverbindungen (einschließlich Onlinedienste wie WWW, FTP, TELNET, E-Mail etc.) in Deutschland sind die VS mit einem vom BSI zugelassenen, zertifizierten (§ 40 VSA) oder vom BMWi freigegebenen Kryptosystem zu kryptieren. Abweichend davon ist ausnahmsweise eine unkryptierte Übertragung zulässig:

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

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

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

3. Maßnahmen zum Schutz der Vertraulichkeit

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

Drei unterschiedliche Ausgangsituationen sind zu unterscheiden:

3.1. Einzelplatz-PC oder Netzwerke mit geschlossenen Nutzergruppen, die nicht mit anderen Netzen verbunden sind

- Das Betriebssystem muss ein differenziertes Benutzerprofil und Zugriffschutz bis auf Dateiebene gewährleisten, damit der Grundsatz „Kenntnis nur, wenn nötig“ sichergestellt wird (z. B. Unix/Linux; Win NT; Win 2000, Win XP).

- Es muss ein Login und ein Passwort vorhanden sein. Das Passwort muss mindestens 6 alphanumerische Stellen, Sonderzeichen; Groß- und Kleinbuchstaben enthalten.

- Das BIOS muss ebenfalls durch ein Passwort geschützt sein.
- Ein Booten des IT-Systems darf grundsätzlich nur von der Festplatte aus möglich sein.
- Es sollte – falls möglich – eine RAM-Disk für die Temp-Dateien enthalten (Nutzungshilfe).
- Ein aktuelles Virenschutzprogramm muss eingesetzt sein.
- Bei Netzwerken sollte eine eigene Partition zum Speichern der VS-Daten auf dem Server installiert werden. **3.2. Geschlossene Netze mit E-Mail-Anschluss nach außen**

Zusätzlich zu den unter Nummer. 3.1 festgelegten Punkten muss
- ein serverbasiertes Netz vorhanden sein, bei dem der Server im zugangsgeschützten Bereich steht,

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

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

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

3.3. Standalone-PC oder Geschlossene Netze mit E-Mail- und Internetanschluss

Zusätzlich zu den unter Nummer. 3.1 und Nummer. 3.2 festgelegten Punkten müssen

- eine Firewall und ein Application-Gateway vorhanden sein,

- die Regelungen des BSI-Grundschutzhandbuchs für Passwörter angewendet werden,

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

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