

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

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

1. Allgemeines**1.1 Zugangsberechtigung und Weitergabe**

- a) VS des Geheimhaltungsgrades VS-NfD dürfen nur Personen zugänglich gemacht werden, die im Zusammenhang mit der Auftragsdurchführung oder bei der Auftragsanbahnung Kenntnis erhalten müssen (Grundsatz „Kenntnis nur, wenn nötig“). Den zugangsberechtigten Personen ist dieses Merkblatt vor dem Zugang zu solchen VS nachweislich bekannt zu geben; sie werden auf ihre besondere Verantwortung für den Schutz der VS gemäß diesem Merkblatt sowie eventuelle strafrechtliche oder vertragsrechtliche Konsequenzen bei Zuwiderhandlung hingewiesen. Weitergehende Maßnahmen wie zum Beispiel Sicherheitsüberprüfungen oder formale Besuchsanmeldungen sind bei diesem Geheimhaltungsgrad nicht erforderlich.
- b) Über den Inhalt der VS ist Verschwiegenheit gegenüber Nichtbeteiligten zu wahren. Mitarbeiter, die sich zum Umgang mit solchen VS als ungeeignet erwiesen oder gegen die Verpflichtung zur Geheimhaltung verstoßen haben, sind von der Bearbeitung solcher VS auszuschließen.
- c) Die Weitergabe von VS-NfD eingestuften VS darf nur an Regierungsstellen, zwischenstaatliche Organisationen oder Auftragnehmer erfolgen, die an einem Programm/Projekt/Auftrag beteiligt sind und die Zugang zu den Informationen im Zusammenhang mit der Bearbeitung des Programms/Projekts/Auftrags haben müssen. Vor der Weitergabe von VS-NfD eingestuften VS an nicht beteiligte zwischenstaatliche Organisationen oder Auftragnehmer aus nicht beteiligten Ländern ist die schriftliche Einwilligung des amtlichen VS-Auftraggebers der VS einzuholen. Grundsätzlich bedarf es hierbei einer Geheimschutzvereinbarung (siehe auch Nummer 23 VSA).
- d) Zuständige Stelle für Fragen des Geheimschutzes im nicht-öffentlichen Bereich das Staatsministerium für Wirtschaft und Arbeit. Dieses kann sich beim VS-Auftragnehmer über die Einhaltung der Bestimmungen dieses Merkblattes vergewissern. Ist Auftraggeber eine Behörde, kann auch diese die Kontrollrechte nach Satz 1 wahrnehmen.
- e) Die VS-Einstufung ist dreißig Jahre nach dem 1. Januar des auf die Einstufung folgenden Jahres aufgehoben, sofern keine andere Frist bestimmt ist (Siehe auch Nummer 9 VSA).

1.2 Bearbeitungsmaßnahmen

- a) Kennzeichnung und Handhabung beziehungsweise Verwahrung
 - aa) Dokumente sind durch schwarzen oder blauen Stempelaufdruck, Druck „VS-NUR FÜR DEN DIENSTGEBRAUCH“ am oberen Rand jeder beschriebenen Seite sowie aller entsprechend eingestuften Anlagen zu kennzeichnen beziehungsweise im Falle internationaler oder ausländischer VS mit der entsprechenden deutschen Kennzeichnung umzustempeln. Bei Büchern, Broschüren und Ähnlichem genügt die Kennzeichnung auf dem Einband und dem Titelblatt. Trägt jede beschriebene Seite eines ausländischen Buches oder einer ausländischen Broschüre den ausländischen Geheimhaltungsgrad, genügt die Kennzeichnung mit dem deutschen Geheimhaltungsgrad auf dem Einband oder dem Titelblatt.
 - bb) VS-NfD eingestuftes Material (zum Beispiel Gerät, Ausrüstung) oder Datenträger (zum Beispiel Disketten, CD's, Mikrochips, Mikrofiche) sind ebenfalls entweder deutlich sichtbar am Material selbst oder – falls dies nicht möglich ist – an den Aufbewahrungsbehältnissen des Materials zu kennzeichnen beziehungsweise grundsätzlich umzustempeln.
 - cc) Die VS sind in verschlossenen Räumen oder Behältern (Schränken, Schreibtischen und so weiter) zu verwahren. Außerhalb von solchen Räumen oder Behältnissen sind sie stets so aufzubewahren beziehungsweise zu behandeln, dass Unbefugte keinen Zugang zu oder Einblick in die VS haben.
 - dd) VS-Zwischenmaterial (zum Beispiel Vorentwürfe, Stenogramme, Tonträger, Folien) ist gegen Einsichtnahme Unbefugter in derselben Weise zu schützen wie das Bezugsdokument. VS-Zwischenmaterial, das nicht an Dritte weitergegeben und unverzüglich vernichtet wird, muss nicht als VS gekennzeichnet werden.
- b) Weitergabe
 - aa) Die Weitergabe in Deutschland erfolgt durch Boten oder Versand durch Zustelldienste in einfachem verschlossenen Umschlag beziehungsweise Behältnis. Der Umschlag beziehungsweise das Behältnis erhalten keine VS-Kennzeichnung.
 - bb) VS können durch private Zustelldienste als gewöhnlicher Brief beziehungsweise Paket oder auch als Luft- oder Seefracht in das Ausland versendet werden, es sei denn, der VS-Auftraggeber hat dieser Versendungsart ausdrücklich widersprochen oder andere Modalitäten für den Auslandsversand festgelegt. Dabei sind vom VS-Auftraggeber

zwischenstaatliche Vereinbarungen beziehungsweise besondere Programm- oder Projektvereinbarungen zu berücksichtigen.

- c) Vernichtung/Rückgabe
 - aa) Um größere Bestände von VS zu vermeiden, sind nicht mehr benötigte VS zu vernichten oder an den VS-Auftraggeber zurückzugeben.
 - bb) VS, auch VS-Zwischenmaterial, sind so zu vernichten, dass der Inhalt nicht mehr erkennbar ist und nicht mehr erkennbar gemacht werden kann.
- d) Verlust, unbefugte Weitergabe, Auffinden von VS oder Nichtbeachtung des Merkblattes sind unverzüglich dem deutschen VS-Auftraggeber mitzuteilen, um einen eventuell entstandenen Schaden zu begrenzen und den Vorfall aufzuklären.
- e) Besuche in das oder aus dem Ausland mit Zugang zu VS-NfD oder vergleichbarem Geheimhaltungsgrad werden in der Regel unmittelbar zwischen der entsendenden und der zu besuchenden Einrichtung vereinbart. Es gibt keine besonderen Formvorschriften.
- f) Aufträge
 - aa) Alle VS-Auftragnehmer/-Unterauftragnehmer sind vom VS-Auftraggeber vertraglich zu verpflichten, die Regelungen dieses Merkblattes zu beachten. Dabei ist darauf hinzuweisen, dass eine Nichtbeachtung die Auflösung des Vertrages beziehungsweise von Teilen des Vertrages zur Folge haben kann.
 - bb) Bei Angeboten beziehungsweise der Aufforderung zur Abgabe von Angeboten und nach Auftragsdurchführung sind VS bis zur Aufhebung der Einstufung vorschriftsmäßig zu verwahren, baldmöglichst zu vernichten oder zurück zu geben.
 - cc) VS-Auftragnehmer/-Unterauftragnehmer im Ausland sind vertraglich zu verpflichten, die Vorschriften ihrer zuständigen Sicherheitsbehörde für die Behandlung von VS vergleichbaren Geheimhaltungsgrades zu beachten. Gibt es keinen vergleichbaren Geheimhaltungsgrad in dem Land eines VS-Auftragnehmers/-Unterauftragnehmers, ist das Staatsministerium für Wirtschaft und Arbeit einzuschalten. Die Weitergabe darf dann erst nach Zustimmung des Staatsministeriums für Wirtschaft und Arbeit erfolgen.

2. Nutzung von Informationstechnik (IT)

2.1 Bearbeitung

- a) Wird IT für die Bearbeitung von VS-NfD eingestuft VS genutzt, sind zum Schutz der VS (entsprechend Nummer 1.1 Buchst. a und Buchst. b) geeignete informationstechnische Maßnahmen und/oder materielle und organisatorische Maßnahmen zu treffen.
- b) Vor der Bearbeitung oder Speicherung von VS-NfD eingestuft VS ist sicherzustellen, dass das Gerät oder das interne Netzwerk nicht unmittelbar (zum Beispiel ohne Schutz durch eine Firewall) mit dem Internet verbunden ist, sofern nicht weitergehende Maßnahmen entsprechend Nummer 3.3 ergriffen worden sind.
- c) Bei der Bearbeitung von VS-NfD eingestuft VS kommen insbesondere folgende Maßnahmen in Betracht:
 - aa) Übersicht über die Zugriffsberechtigungen,
 - bb) Nutzung von Identifizierungs- und Authentisierungsmechanismen (zum Beispiel Login, Passwort),
 - cc) geeignete IT-Sicherheitsanweisung (einzelplatz- oder unternehmensbezogen).
- d) Funktastaturen und Funk-Netzwerke dürfen nur eingesetzt werden, wenn sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind. Nähere Auskünfte erteilt das Landesamt für Verfassungsschutz Sachsen.
- e) Werden für die Bearbeitung oder Speicherung von VS-NfD eingestuft Daten tragbare IT-Systeme (zum Beispiel Notebooks oder Handhelds) eingesetzt, sind die verwendeten Speichermedien durch vom BSI zugelassene Produkte zu verschlüsseln. Sofern Programme und Geräte mit BSI-Zulassung nicht verfügbar sind, können durch das BSI nach Common Criteria, Prüftiefe mindestens EAL 3, zertifizierte Produkte verwendet werden. Auskünfte erteilt das Landesamt für Verfassungsschutz Sachsen.
- f) Transportable Datenträger (zum Beispiel Disketten, CD's, Wechselplatten), die VS-NfD eingestufte Daten unverschlüsselt enthalten, sind gemäß Nr. 1.2 Buchst. a Doppelbuchst. bb zu kennzeichnen und gemäß Nummer 1.2 Buchst. a Doppelbuchst. cc aufzubewahren.
- g) Das Löschen von Datenträgern hat mit Hilfe von Softwareprodukten zu erfolgen, die mindestens ein zweifaches Überschreiben vorsehen. Hierbei soll auf vom BSI empfohlene Produkte zurückgegriffen werden.
- h) IT und Datenträger sind auf Virenbefall (insbesondere sogenannte 'Trojaner' oder 'Würmer') zu überprüfen, bevor VS-NfD damit bearbeitet werden. Diese Prüfung ist in regelmäßigen Zeitabständen zu wiederholen.
- i) Private IT (zum Beispiel Laptops), Software oder Datenträger dürfen nicht für die Bearbeitung eingesetzt werden. In für VS-NfD genutzten IT-Systemen dürfen keine private Software oder private Datenträger verwendet werden.
- j) Auf fest installierten Datenträgern, die VS-NfD eingestufte Daten unverschlüsselt enthalten, sind die Verschlusssachen gemäß Buchstabe g zu löschen, bevor die Datenträger im Rahmen von Wartungs- oder Reparaturarbeiten an IT-Systemkomponenten den Bereich der zugriffsberechtigten

Personen verlassen. Ist eine Löschung nicht möglich, sind die Datenträger auszubauen und zurückzubehalten beziehungsweise ist das Wartungs- beziehungsweise Reparaturunternehmen vertraglich auf die Einhaltung der Regeln dieses Merkblattes zu verpflichten.

2.2 Übertragung

- a) Bei der elektronischen Übermittlung auf Telekommunikations- oder anderen technischen Kommunikationsverbindungen (einschließlich Onlinedienste wie WWW, FTP, TELNET, E-Mail et cetera) in Deutschland sind die VS mit einem vom BSI zugelassenen, zertifizierten (Nummer 40 VSA) Kryptosystem zu kryptieren. Abweichend hiervon ist im Ausnahmefall eine unverschlüsselte Übertragung zulässig
 - aa) innerhalb von Festnetzen bei Telefongesprächen, bei Videokonferenzen und bei Fernkopien und Fernschreiben, wenn zwischen Absender und Empfänger für die erforderliche Übertragungsart keine Kryptiermöglichkeit besteht und der VS-Auftraggeber bei der Auftragsvergabe nicht ausdrücklich eine Kryptierung verlangt. Die absendende Stelle hat sich vor der Übertragung möglichst zu vergewissern, dass sie mit dem richtigen Empfänger verbunden ist.
 - bb) innerhalb eines geschlossenen Netzes (LAN), wenn es ausschließlich auf einem örtlich zusammenhängenden firmeneigenen Gelände betrieben wird und die Übertragungseinrichtungen gegen unmittelbaren Zugriff Unbefugter geschützt sind.
- b) Bei grenzüberschreitenden elektronischen Übermittlungen müssen die Verschlüsselungsverfahren zwischen den nationalen Sicherheitsbehörden der beteiligten Staaten abgestimmt werden. Sofern in einem Programm/Projekt besondere Sicherheitsanweisungen für die Übermittlung vereinbart wurden, sind diese zu beachten. Bei Bedarf erteilt das Landesamt für Verfassungsschutz Sachsen weitere Auskünfte.

2.3 Maßnahmen zum Schutz der Vertraulichkeit

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

Drei unterschiedliche Ausgangssituationen sind zu unterscheiden:

- a) Einzelplatz-PC oder Netzwerke mit geschlossenen Nutzergruppen, die nicht mit anderen Netzen verbunden sind
 - aa) Das Betriebssystem muss ein differenziertes Benutzerprofil und Zugriffsschutz bis auf Dateiebene gewährleisten, damit der Grundsatz „Kenntnis nur, wenn nötig“ sichergestellt wird (zum Beispiel Unix/Linux, Win NT, Win 2000, Win XP).
 - bb) Es muss ein Login und ein Passwort vorhanden sein. Das Passwort muss mindestens sechs alphanumerische Stellen, Sonderzeichen, Groß- und Kleinbuchstaben enthalten.
 - cc) Das BIOS muss ebenfalls durch ein Passwort geschützt sein.
 - dd) Ein Booten des IT-Systems darf grundsätzlich nur von der Festplatte aus möglich sein.
 - ee) Es sollte – falls möglich – eine RAM-Disk für die Temp-Dateien enthalten (Nutzungshilfe).
 - ff) Ein aktuelles Virenschutzprogramm muss eingesetzt sein.
 - gg) Bei Netzwerken sollte eine eigene Partition zum Speichern der VS-Daten auf dem Server installiert werden.
- b) Geschlossene Netze mit E-Mail-Anschluss nach außen
Zusätzlich zu den unter Buchstabe a festgelegten Punkten müssen
 - aa) ein serverbasiertes Netz vorhanden sein, bei dem der Server im zugangsgeschützten Bereich steht,
 - bb) eine Firewall vorhanden sein, entweder auf dem Server oder als eigenes IT-System (und gegebenenfalls zusätzlich E-Mailserver) auch im zugangsgeschützten Bereich, ein Paketfilter eingesetzt werden, ein Application Gateway ist möglich.
 - cc) jede weitere IP-Adresse außer der Server-IP nach außen verborgen werden (DNS-Server),
 - dd) die Übertragung von VS-NfD verschlüsselt erfolgen, wobei für die Verschlüsselung nur vom BSI freigegebene Produkte eingesetzt werden dürfen; Schlüssel sind grundsätzlich nicht auf der Festplatte abzulegen. Es müssen verbindliche Anwenderregelungen innerhalb des Unternehmens festgelegt und geschult werden. Die neuesten Sicherheits-Updates der genutzten Software sind nach Verfügbarkeit insbesondere auch der Firewall einzubinden.
- c) Standalone-PC oder geschlossene Netze mit E-Mail und Internetanschluss
Zusätzlich zu den unter Buchstaben a und b festgelegten Punkten müssen
 - aa) eine Firewall und ein Application-Gateway vorhanden sein,
 - bb) die Regelungen des BSI-Grundschrifthandbuches für Passwörter angewendet werden,
 - cc) VS-NfD-Daten auf dem Server in einer eigenen Partition beziehungsweise in einem speziell geschützten Datenbereich gehalten werden; die dadurch gegebenen Schutzmechanismen sind entsprechend anzuwenden.

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