

FAQ

Nutzung von Informationstechniken im Bereich

„VS-Nur für den Dienstgebrauch“

Anlage 4 zum GHB (VS-NfD-Merkblatt Teil II)

Grundsatzfragen:

Ich möchte die Administration meiner IT Outsourcen. Geht das?

Eine Beteiligung von IT-Dienstleistern an der Administration der Unternehmens-IT kann nur mit schriftlicher Einwilligung aller amtlichen VS-Auftraggeber erfolgen, deren VS-NfD betroffen sind. Im Teil I 1.1 ist festgelegt, dass VS-NfD nur Personen zugänglich gemacht werden darf, die im Zusammenhang mit der Auftragsdurchführung Kenntnis erhalten müssen (Grundsatz "Kenntnis nur wenn nötig"). Des weiteren darf nach Ziffer 1.3 im Teil I die Weitergabe von VS-NfD nur an Auftragnehmer erfolgen, die am Auftrag beteiligt sind und Zugang zu den Informationen im Zusammenhang mit der Bearbeitung des Auftrags haben müssen. Wer am Auftrag beteiligt ist und wer im Zusammenhang mit der Bearbeitung des Auftrags Zugang zu den Informationen haben muss, entscheidet der jeweilige amtliche VS-Auftraggeber.

Ich möchte bei der Bearbeitung meiner VS-NfD Daten WLAN nutzen, was muss ich beachten?

Der Einsatz von WLAN bei der Bearbeitung von VS-NfD Daten ist nur möglich in Verbindung mit einer BSI zugelassenen VPN (Virtual Private Network) Lösung. Die VPN Systeme mit einer BSI Zulassung finden sich auf der Webseite des BSI unter dem folgenden Link:

https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/Hinweise/Hinweise_html.html.

Besteht die Möglichkeit einer Sicherheitsüberprüfung für Systemadministratoren? Nein.

Grundlage der Sicherheitsüberprüfung(SÜ) ist das Sicherheitsüberprüfungsgesetz (SÜG). Dieses erlaubt eine SÜ erst beim Umgang mit Verschlusssachen ab dem Geheimhaltungsgrad VS-VERTRAULICH.

Kann ich für mein VS-NfD Netz beim BMWi eine Genehmigung bekommen?

Für den Schutz von VS-NfD ist nach dem Geheimschutzhandbuch(GHB) ausschließlich der Sicherheitsbevollmächtigte des Unternehmens zuständig.

Hierbei sind die Vorgaben der Anlage 4 zum GHB (VS-NfD Merkblatt) als Mindestanforderungen umzusetzen. Im Hinblick auf die laufende Neufassung des GHB empfehlen wir die Vorgaben des BSI Grundschutzes zu implementieren.

Weitergehende Anforderungen, z.B. Einsatz von zugelassenen Kryptoprodukten, ergeben sich aus den Einsatz- und Betriebsbedingungen.

Daraus folgt, dass eine Genehmigung oder Prüfung durch das BMWi **NICHT** erfolgt.

Allgemeine Fragen zur HW:

Was ist unter dem Begriff Speichermedium unter Ziff. 1.4 des Merkblattes zu verstehen?

Das Speichermedium eines tragbaren IT-Systems sind die eingebaute Festplatte oder die Wechselfestplatten.

Kann ich auch mein Tablet-PC oder mein Smartphone als mobiles IT-System einsetzen?

Gem. Ziff.II.1.4 des Merkblatts sind tragbare IT-Systeme (also auch Tablet-PC's oder Smartphones) mit einem BSI zugelassenen Kryptosystem zu verschlüsseln. Zugelassene Produkte finden sich auf der Webseite BSI - „Liste der zugelassenen Produkte“ (BSI 7164).

Wie ist das mit denen, „im Einzelfall vom BMWi freigegebenen“ Systemen laut Merkblatt?

Dies gilt nur und ausschließlich für den Fall, dass keinerlei Produkte mit BSI Zulassung verfügbar sind.

Mein Rechner stürzt ab und geht im laufenden Betrieb kaputt. Darauf sind eingestufte Daten gespeichert. Ich kann diese aber vor der Wartung / Reparatur nicht löschen. Was muss ich tun?

Sofern der Rechner eine Wechselfestplatte enthält, ist diese zu entnehmen. Bei fest eingebauten Speicher ist die Wartungsfirma auf das Merkblatt zu verpflichten und durch geeignetes, ermächtigtes Personal zu beaufsichtigen.

An meinem IT-System möchte ich gerne eine Funk Tastatur und eine Funk Maus einsetzen. Ist das möglich?

Funktastaturen und Funk-Netzwerke dürfen nur eingesetzt werden, wenn sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind. Derzeit stehen solche Produkte mit einer Zulassung durch das BSI nicht zur Verfügung. Daher ist eine Verwendung ausgeschlossen.

Allgemeine Fragen zur Software:

In unserem Unternehmen verwenden wir Bitlocker zur Verschlüsselung, kann ich das Produkt nicht auch verwenden?

Nein! Bitlocker ist vom BSI für den Einsatz bei VS als nicht ausreichend bewertet worden.

Ich habe ein Mac OS x als Betriebssystem. Welche Verschlüsselungssoftware gibt es ?

Für Apple Betriebssysteme gibt es aktuell eine BSI Zulassung für das Produkt „SecurePIM“. Ein VS-NfD Konformer Einsatz ergibt sich aus den entsprechenden Einsatz- und Betriebsbedingungen. Diese sind verpflichtend umzusetzen.

Kann ich das Produkt Office 365 in für die Bearbeitung von VS-NfD nutzen?

Ein Einsatz von Office 365 im Zusammenhang mit VS-NfD ist **NICHT ZULÄSSIG!** Einzelheiten hierzu finden Sie in der Mail Info 2018-4.

Allgemeines zur Kryptierung:

Was verschlüsseln?

Verschlüsselt werden muss entweder die Hardware (Ziff. II.1.4, II.1.5) selbst oder die elektronische Übermittlung von Daten (Ziff. II.2).

Womit muss ich verschlüsseln?

Es müssen grundsätzlich BSI zugelassene Produkte sein. Diese finden sich auf der Webseite des BSI unter

https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/zugelasseneProdukte_html.html

Wo finde ich die zugelassenen Kryptosysteme?

Eine abschließende Auflistung aller Kryptosysteme mit BSI Zulassung finden sich auf der Webseite des BSI unter

https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/zugelasseneProdukte_html.html

Die entsprechenden Einsatz- und Betriebsbedingungen zu den Produkten können vom Geheimschutzserver des BMWI (geschützter Bereich) herunter geladen werden.

Wo kann ich CHIASMUS bekommen?

CHIASMUS kann über das BSI, Referat Z3 bezogen werden.

Hinweise und detaillierte Bezugsadresse finden sich auf der Seite des BSI unter:

<https://www.bsi.bund.de/DE/Themen/ProdukteTools/Chiasmus/Chiasmus.html>

Ansprechpartner für fachliche Fragen: Chiasmus@bsi.bund.de

Bestellung und Lizenzbedingungen: service-center@bsi.bund.de

ACHTUNG – Die Zulassung für das Produkt endet am 31.12.2021. Ein Einsatz ist darüber hinaus nicht mehr zulässig.

Warum brauche ich eine Festplattenverschlüsselung und warum reicht es nicht aus, das auf meinem Notebook die Dateien oder Ordner mit CHIASMUS verschlüsselt abgelegt sind?

Es reicht nicht aus, weil Ordner oder Dateien keine Speichermedien sind. Darüber hinaus verfügen die geforderten, zugelassenen Festplattenverschlüsselungsprogramme noch über eine Zugangskontrolle.

Kryptierung von Hardware:

Welche IT-Systeme sind zu verschlüsseln?

Lt. Ziff. II 1.4 der Anlage 4 sind alle tragbaren IT-Systeme wie z.B. Notebook, Netbook, Laptop zu verschlüsseln.

Muss ich meine CD's, USB-Sticks, Wechselplatten auch verschlüsseln?

Nein, nicht zwingend. Aber - wenn sie eingestufte Daten unverschlüsselt enthalten, sind sie entsprechend den Vorschriften zu kennzeichnen und im persönlichen Gewahrsam zu führen oder in verschlossenen Räumen / Behältnissen aufzubewahren.

Kryptierte Übertragung von Daten:

Was bedeutet Übertragung von Daten i.S.d. Merkblatts?

Sobald auf die eingestufteten Daten in einem anderen lokalen Standort zugegriffen wird /
Sobald ich mit dem Zugriff auf die Daten den eigenen Standort verlasse.

Ich greife auf den Fileserver in einem anderen Ort zu. Ist das Übertragung?

Ja!

Was ist bei Übertragung zu beachten?

Die Daten sind mit einem BSI zugelassenen Produkt zu verschlüsseln.

Gibt es Ausnahmen von der kryptierten Übermittlung?

Ja, aber nur wenn es sich um ein örtlich zusammenhängendes, firmeneigenes Gelände handelt **und** die Übertragungseinrichtungen vor dem Zugriff Unbefugter geschützt sind.

Was ist die Alternative wenn ich nicht kryptieren möchte?

Dann bleibt nur ein lokales Netz oder ggf. lokale Netze in jedem Standort – also eine dezentrale Datenhaltung für eingestufte Daten.

Falls erforderlich kann dann eine Übermittlung als Mailanhang mit Chiasmus verschlüsselt erfolgen.

Ich möchte VS-NfD als Anlage zu einer Mail versenden. Was muss ich beachten?

Mailversand von NfD ist nur kryptiert erlaubt. Zum kryptieren sind BSI zugelassene Produkte zu verwenden.

Eine abschließende Auflistung aller Produkte mit BSI Zulassung findet sich auf der Webseite des BSI.

Anmerkungen zum Thema „getrennte Netze“

Mit zunehmender Vernetzung werden unsere IT-Systeme immer anfälliger für Cyberangriffe. Angesichts der zunehmenden Bedrohungen aus dem Netz rückt die Sicherheit von IT-Systemen immer stärker in den Focus. Dazu zählt z.B. der weltweite Einsatz gleicher Hard- und Softwaresysteme, was zu einer erhöhten Bedrohungslage für die Kompromittierung von Daten durch Schadsoftware führt.

In diesem Zusammenhang weisen wir darauf hin, dass bereits bisher die VS-NfD Daten separat in speziell geschützten Datenbereichen zu halten sind.

Darüber hinaus empfiehlt das BMWi, Referat RS 3, über die im VS-NfD-Merkblatt geforderten Maßnahmen hinaus, eine Trennung der VS-NfD Daten von den Unternehmensnetzwerken als weitergehende Sicherheit zu realisieren.

Dies erhöht nicht nur den Schutz der VS-NfD Daten, sondern kann auch zu Kostenreduzierung (BSI zugelassene Produkte müssen nur für das separierte VS-NfD-Netzwerk eingesetzt werden) und weniger Administrationsaufwand aufgrund des kleineren Nutzerkreises beitragen.