Richtlinien zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik in Unternehmen (VS-IT-Richtlinien / U - VSITR/U)

Die vorliegenden IT-Richtlinien gelten für Unternehmen und Einzelpersonen, die sich gegenüber dem Bundesministerium für Wirtschaft und Technologie (BMWi) zur Einhaltung der Vorschriften des Handbuchs für den Geheimschutz in der Wirtschaft (GHB) verpflichtet haben. Aufgrund dieser Richtlinien kann es sinnvoll sein, allgemeine IT-spezifische Maßnahmen in einer betriebsinternen Anweisung festzulegen.
Der Begriff Informationstechnik (IT) umfasst im folgenden Geräte und Verfahren, die auf elektronischer Grundlage zur automatischen Erfassung, Darstellung, Speicherung, Verarbeitung oder Übermittlung von Informationen in Form von Texten, Daten, Bildern oder Sprache dienen.

I. Allgemeiner Teil

§ 1 Zweck und Anwendungsbereich

(1) Die Richtlinien regeln, welche Maßnahmen zur Geheimhaltung von VS beim Einsatz von Informationstechnik (IT) ergänzend zu den Regelungen des GHB zu treffen sind.
(2) Die Richtlinien sind anzuwenden, wenn VS-VERTRAULICH oder höher eingestufte VS mit IT verarbeitet oder übertragen werden. Sie richten sich an
- Unternehmen und
- Personen, die selbständig tätig oder in Unternehmen beschäftigt sind und die IT für die Verarbeitung, Speicherung oder Übertragung von VS nutzen oder Tätigkeiten an IT-Systemen ausüben, bei denen sie sich Zugang zu VS verschaffen können oder die für den Geheimschutz beim Einsatz von IT für VS zuständig sind.

§ 2 Begriffsbestimmungen

Im Sinne dieser Richtlinien umfasst
- "VS-Datenträger" ein Speichermedium, das VS enthält,
- "Kryptosystem" alle Mittel, die für eine bestimmte Kryptierung und Dekryptierung benötigt werden (z. B. Kryptogerät und Kryptodaten),
- "Kryptodaten" eine Folge von Zeichen, die als Parameter zum Kryptieren und Dekryptieren benötigt werden,
- "IT-Sicherheitsfunktion" eine mit IT realisierte Sicherheitsvorkehrung, insbesondere zur Kryptierung, Abstrahlsicherheit, Zugriffskontrolle, Beweissicherung, Protokollauswertung, Wiederaufbereitung oder Wahrung der Unverfälschtheit von Software.

II. Zuständigkeiten

§ 3 Verantwortliche/r für IT-Geheimschutzmaßnahmen

Unternehmen mit komplexen IT-Systemen oder vielfältigen IT-Anwendungen für VS bestimmen eine/n IT-VS-Beauftragte/n mit IT-Fachkenntnissen, der/die den/die SiBe bei der Umsetzung dieser Richtlinien unterstützt. Er/sie soll nicht zugleich Aufgaben eines Systemadministrators bei für VS eingesetzten IT-Systemen wahrnehmen und soll in der Durchführung dieser Richtlinien durch BMWi besonders geschult sein. Sofern der/die IT-VS-

Beauftragte Funktionen des/der betrieblichen Datenschutzbeauftragten wahrnimmt, darf er/sie nicht gleichzeitig Aufgaben des/der SiBe ausüben, die sich auf personenbezogene Daten nach dem SÜG beziehen. Wird ein/e IT-VS-Beauftragte/r nicht bestimmt, so verbleiben dessen/deren Aufgaben bei dem/der SiBe.

§ 4 Aufgaben von BMWi bei der Umsetzung dieser Richtlinien

(1) BMWi berät die Unternehmen bei der Umsetzung dieser Richtlinien und führt Schulungen durch. Insbesondere wird die Notwendigkeit von Zulassungen nach § 14 Abs. 2 oder davon abweichenden Maßnahmen durch BMWi festgestellt und, falls erforderlich, durch das BMWi veranlasst. BMWi kann zu seiner Unterstützung andere Stellen, insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI), hinzuziehen.

(2) Zur Umsetzung dieser Richtlinien kann BMWi weitere Hinweise herausgeben, die sich insbesondere auf folgendes erstrecken:
- Hinweise zur Erstellung von IT-Geheimschutz-Anweisungen,
- Maßnahmen gegen kompromittierende Abstrahlung,
- Verwendung von Passworten und Personenidentifikationsnummern (PIN),
- Installation von Hardware, die für VS eingesetzt werden soll,
- Sicherung von Leitungen für die unkryptierte Übertragung von VS,
- Schutz von IT-Betriebsräumen und Produkten mit IT-Sicherheitsfunktionen,
- Überprüfung neuer oder geänderter Betriebs- / Anwendungssoftware,
- Überprüfung der Geheimschutzmaßnahmen vor Freigabe von IT für VS,
- Durchführung technischer Prüfungen.

III. IT-Planung

§ 5 IT-Planung und -Beschaffung

(1) Ist geplant, IT für VS einzusetzen, so ist der/die SiBe bzw. der/die IT-VS-Beauftragte bereits zu Planungsbeginn zu beteiligen. Bei komplexen IT-Systemen oder vielfältigen IT-Anwendungen für VS soll BMWi frühzeitig beratend hinzugezogen werden.

(2) Bereits vor der Beschaffung von IT bzw. vor der Modifizierung vorhandener IT, die für VS eingesetzt wird, muss - im Einvernehmen mit BMWi - festgelegt werden, welche IT-Sicherheitsfunktionen das IT-System enthalten muss und welche Sicherheitsleistungen die IT-Hersteller / -Vertreiber zu erbringen haben. Es ist insbesondere zu beachten, dass
- Produkte mit IT-Sicherheitsfunktionen amtlich zugelassen sein müssen,
- Produkte mit IT-Sicherheitsfunktionen, sobald feststeht, dass sie für VS eingesetzt werden sollen, geschützt aufbewahrt und transportiert werden müssen,
- eine sicherheitsgerechte Wartung und Instandsetzung der IT-Systeme erfolgt.

§ 6 IT-Geheimschutz-Anweisung

(1) In einer IT-Geheimschutz-Anweisung (ITGA) ist das Sicherheitskonzept für die eingesetzte IT zu beschreiben. Folgende Unterlagen sind Teil der ITGA:
- Übersicht über die
  -- VS-Projekte, die mit dem IT-System bearbeitet werden (sollen),
  -- VS-Einstufungen der Daten / Programme,

  - -- eingesetzte/vorgesehene IT (z.B. Hardware, Betriebssysteme, Anwendungssoftware, Datenträger) und die darin enthaltenen IT-Sicherheitsfunktionen.
  - Systemspezifische Verfahrensanweisungen für den Betrieb der IT-Systeme, insbesondere Benennung der berechtigten Nutzer, der Systemverwalter und sonstigen Funktionsträger sowie
  - Geheimschutzvorkehrungen für den Notfall, Störungsfall oder Schadensfall.

(2) Die ITGA muss BMWi zur Genehmigung zugeleitet werden. Der VS-Betrieb der IT-Systeme darf erst nach Genehmigung durch BMWi aufgenommen werden. Alle Änderungen in bezug auf Hardware, Software, Organisation, Anwendungsbereich und (räumliche) Umgebung sind in der ITGA zu ergänzen. Sofern diese geheimschutzrelevant sind, ist erneut die Genehmigung von BMWi einzuholen.

IV. IT-Einsatz
§ 7 Zugangs - / Zugriffskontrolle und Zugriffsrechte

(1) IT-Systeme, die für VS eingesetzt werden, müssen über ein Zugangs- und Zugriffskontrollsystem verfügen, das sicherstellt, dass nur Befugte im Rahmen der ihnen erteilten Zugriffsrechte Zugang erhalten und auf VS zugreifen können. Wiederholt abgewiesene Zugangs-/Zugriffsversuche sollen für diesen Nutzer zur Systemsperrung führen, die nur von hierzu besonders beauftragten Personen aufgehoben werden darf.

(2) Bei der Vergabe, Änderung und Rücknahme von Zugriffsrechten muss gewährleistet sein, dass
  - der Antrag dazu von einer berechtigten Stelle stammt (z.B. Projektleiter),
  - die zu berechtigende Person ausreichend VS-ermächtigt ist,
  - der Grundsatz "Kenntnis nur, wenn nötig" beachtet wird und
  - keine sicherheitsmäßig unvereinbare Bündelung von Funktionen entsteht.

  Die Übertragung der Befugnis zur Vergabe und Änderung von Zugriffsrechten bedarf der Zustimmung des/der IT-VS-Beauftragten.

(3) Die Vergabe, Änderung und Rücknahme von Zugriffsrechten ist so zu dokumentieren, dass jederzeit feststellbar ist, wer zu welchen Zeiten
  - zur Vergabe, Änderung oder Rücknahme von Rechten in welchem Umfang berechtigt war und
  - welche für den Geheimschutz relevanten Rechte ausüben konnte.

  Die Dokumentation ist mindestens fünf Jahre aufzubewahren.

(4) Zur Identifizierung/Authentisierung eingesetzte Mittel eines Rechteinhabers in Form von
  - Besitz (z.B. Chipkarten) sind wie Schlüssel zu VS-Verwahrgelassen und
  - Wissen (z.B. PIN oder Passwort) sind wie Zahlenkombinationen zu VS-Verwahrgelassen

  zu behandeln. Besitzmittel können anstelle der Aufbewahrung in einem VS-Schlüsselbehälter auch in persönlichem Gewahrsam gehalten werden. Einzelheiten über die Auswahl, Vergabe, Kontrolle und den Wechsel von Passworten/PIN sind in der ITGA festzulegen.

(5) Anstelle der in Absatz 1 bis 4 genannten Maßnahmen können auch andere Schutzvorkehrungen getroffen werden (z. B. Betrieb in einem VS-Aktensicherungsraum), soweit damit ein vergleichbarer Schutz erreicht wird.

§ 8 Beweissicherung und Protokollauswertung

(1) Für VS eingesetzte IT-Systeme sollen, über eine automatische Beweissicherung
- abgewiesene Zugangs-/Zugriffsversuche,
- Ausdrucke, Ausgaben von VS auf Datenträger und Übermittlungen von VS sowie
- Zugriffe auf VS-Daten

aufzeichnen.
Es soll möglich sein, sicherheitserhebliche Ereignisse bezogen auf einzelne Benutzer, Benutzergruppen und zugriffsgeschützte Objekte zuverlässig und nachvollziehbar aufzubereiten.

(2) Abgewiesene Zugangs-/Zugriffsversuche sollen vom IT-System unmittelbar dem/der IT-VS-Beauftragten oder einem/einer von ihm/ihr Beauftragten angezeigt oder revisionssicher protokolliert werden. Ausdrucke und Ausgaben von VS auf Datenträger, die zur Weitergabe an Dritte oder zur Archivierung bestimmt sind, sowie Übermittlungen von VS sind vom IT-System oder auf andere Weise der VS-Registratur anzuzeigen.

(3) Der Zugriff auf die Aufzeichnungen nach Absatz 1 sowie ihre Löschung darf nur durch den/die IT-VS-Beauftragte/n oder eine/n von ihm/ihr Beauftragte/n durchgeführt werden. Die Aufzeichnungen sind, soweit keine zwingenden Gründe entgegenstehen, nach Überprüfung durch den/die IT-VS-Beauftragte/n oder eine/n von ihm/ihr Beauftragte/n zu löschen.

(4) Falls keine automatische Beweissicherung möglich ist, sind manuelle Protokolle zumindest über
- die VS-Bearbeitungszeiten der berechtigten Nutzer bzw. Zeiten, zu denen an VS-IT-Systemen gearbeitet wurde und
- Ausdrucke und sonstige Ausgaben (z.B. auf Datenträger) oder Übermittlungen von VS (gilt nicht für VS-Zwischenmaterial)

zu erstellen. Im Einzelfall können weitere Aufzeichnungen gefordert werden.

§ 9 Wiederaufbereiten, Löschen und Vernichten von VS-Datenträgern

(1) VS-Datenträger mit unkryptierten VS sind vor einer Wiederverwendung durch IT-Nutzer ohne Zugriffsberechtigung zu allen gespeicherten Daten so aufzubereiten, dass eine Kenntnisnahme des früheren Inhalts nicht möglich ist. Beim Wiederanlauf von IT-Systemen sowie bei Wartungs- und Instandsetzungsarbeiten muss sichergestellt sein, dass Unbefugte keine Kenntnis von VS erhalten.

(2) Nicht mehr benötigte VS-Datenträger, die eingestufte VS unkryptiert enthalten haben, sind physikalisch zu löschen oder zu vernichten.

§ 10 Schutz der Software und Testläufe

(1) Für VS eingesetzte Betriebs- / Anwendungssoftware soll so geschützt sein, dass Veränderungen durch Unbefugte erkennbar werden (Gewährleistung der Unverfälschtheit).

(2) Der Einsatz neuer oder geänderter Betriebs- / Anwendungssoftware sowie Testläufe sind dem/der IT-VS-Beauftragten rechtzeitig vorher anzuzeigen, der/die
- bei neuer oder geänderter Betriebs- / Anwendungssoftware feststellt, ob eine Überprüfung erforderlich ist und im Bedarfsfall entscheidet, wie diese zu erfolgen hat, und
- bei Testläufen sicherstellt, dass diese nicht während der VS-Verarbeitung / Übertra-

gung durchgeführt werden, grundsätzlich nicht mit VS erfolgen und dass Geheimschutzvorkehrungen nicht beeinträchtigt werden.

Soweit wesentliche Beeinträchtigungen des Geheimschutzes möglich sind, ist der Einsatz von Betriebs-/Anwendungssoftware bis zur Vorlage eines positiven Prüfergebnisses und die Durchführung von Testläufen untersagt.

§ 11 Systemwartung

(1) Vor Wartungs- oder Instandsetzungsarbeiten sollen die VS aus dem IT-System entfernt werden. Ist dies nicht möglich, ist entsprechend ermächtigtes Wartungs- oder Instandsetzungspersonal einzusetzen oder dieses durch geeignetes Fachpersonal zu beaufsichtigen. Während der VS-Verarbeitung / -Übertragung ist eine Wartung oder Instandsetzung des IT-Systems grundsätzlich nicht zulässig.

(2) Eine Fernwartung durch eigenes Personal ist zulässig, wenn
- für die Übertragungen im Rahmen der Fernwartung für VS zugelassene Kryptosysteme eingesetzt werden und
- eine zuverlässige Zugriffskontrolle, Beweissicherung und Überprüfung der Aufzeichnungen erfolgt.

Die Fernwartung soll grundsätzlich nicht während der VS-Verarbeitung / -Übertragung durchgeführt werden. Dabei müssen alle im IT-System zugänglichen VS-Daten kryptiert oder entfernt werden.

(3) Sofern die Fernwartung durch ein anderes Unternehmen durchgeführt werden soll, muss zusätzlich zu den unter (2) genannten Bedingungen
- BMWi für das (die) jeweilige(n) Projekt(e) zustimmen,
- ein Sicherheitsbescheid von BMWi über dieses Unternehmen vorliegen,
- jeder Fernwartungsvorgang durch das eigene Unternehmen gesondert freigeschaltet und beendet werden.

§ 12 Abstrahlsicherheit

(1) IT-Hardware, die VS unkryptiert führt, ist unter Beachtung der Hinweise von BMWi zu installieren.

(2) Durch den amtlichen VS-Auftraggeber ist festzustellen, ob kompromittierende Abstrahlung zu einem untragbaren Sicherheitsrisiko führt. Die abschließende Entscheidung über die Erforderlichkeit von Maßnahmen gegen kompromittierende Abstrahlung obliegt BMWi. Sofern Maßnahmen erforderlich sind, muss die IT-Hardware
- in amtlich zugelassenen abstrahlsicheren Räumen oder Behältern betrieben werden,
- eine amtliche Zulassung für den Betrieb innerhalb einer bestimmten Sicherheitszone aufweisen und innerhalb einer solchen betrieben werden, oder
- vom BSI als abstrahlsicher zugelassen sein.

Sofern nur in sehr geringem Umfang - maximal 20 Std. pro Monat zu unregelmäßigen Zeiten - mit kompromittierender Abstrahlung zu rechnen ist, kann im Einvernehmen mit BMWi auf weitergehende Maßnahmen verzichtet werden.

§ 13 Speicherung, Übertragung und Netzanbindung

(1) VS sind bei Speicherung und Übertragung zu kryptieren. Bei der Speicherung von VS

auf Rechnern ohne Anbindung an oder Zugang zu einem anderen Kommunikationsnetz ist eine Kryptierung nicht erforderlich, wenn die VS materiell gemäß GHB gesichert sind. Bei der Übertragung von VS kann die Kryptierung außerdem unterbleiben,

- innerhalb eines zutrittsgeschützten IT-Betriebsraumes, oder
- wenn die Übertragungseinrichtungen so geschützt sind, dass ein Zugriff Unbefugter unverzüglich erkannt wird (approved circuits), oder
- wenn in einem lokalen Netz maximal GEHEIM eingestufte VS übertragen werden und
  - -- ein Zugriffskontrollsystem nach **§ 7** Abs. 1 eingesetzt ist,
  - -- die Übertragungseinrichtungen sich vollständig in einem Bereich mit zuverlässiger Zutrittskontrolle befinden oder außerhalb nach Nummer 2 geschützt sind.

Bei Verbindung mit einem anderen Kommunikationsnetz muss dieses und die Verbindung zu diesem mindestens wie ein lokales Netz geschützt sein.

(2) Soweit die für den Betrieb eines Kryptosystems benötigten Kryptodaten nicht automatisch bereitgestellt werden, dürfen diese nur von amtlichen Stellen oder in deren Auftrag hergestellt werden. BMWi teilt den Unternehmen im Bedarfsfall die jeweils zuständige Stelle mit. Für die Verwaltung von auf dem Kurier-/Postweg bereitgestellten Kryptodaten ist ein/eine Kryptoverwalter/in und Vertreter/in zu bestellen. Der/die Kryptoverwalter/in gibt die Kryptodaten in die Kryptosysteme ein oder bei Bedarf an die befugten IT-Nutzer aus. Namen und Anschrift des/der Kryptoverwalters/in und Vertreters/in sowie Änderungen sind BMWi mitzuteilen. BMWi leitet die Angaben - sofern erforderlich - an die für die Herstellung und Verteilung von Kryptodaten zuständige Stelle weiter.

§ 14 Zulassung von Produkten mit IT-Sicherheitsfunktionen

(1) Produkte mit Funktionen zur Kryptierung, Abstrahlsicherheit, Löschung oder Vernichtung von VS-Datenträgern oder Sicherung von Übertragungsleitungen (approved circuits) müssen vom BSI zugelassen sein. Die in der Zulassung angegebenen Einsatz- und Betriebsbedingungen sind zu beachten.

(2) Produkte mit Funktionen zur Zugriffskontrolle, Beweissicherung und Protokollauswertung oder Wiederaufbereitung oder Unverfälschtheit von Software sollen vom BSI zugelassen sein. BMWi kann die Verwendung anderer Produkte erlauben, wenn keine geeigneten zugelassenen oder geprüften Produkte verfügbar sind und eine Zulassung oder Prüfung nicht oder nicht zeitgerecht veranlasst werden kann. In diesem Fall sind Produkte zu bevorzugen, die ein amtlich anerkanntes Prüfzertifikat aufweisen.

(3) Die Zulassungen/Prüfungen erfolgen abgestuft nach der Schutzbedürftigkeit von IT-Anwendungen für VS auf der Grundlage allgemein anerkannter Sicherheitskriterien und Verfahren, die bei Bedarf um besondere Prüfungen zum Schutz vor nachrichtendienstlichen Angriffen zu ergänzen sind.

§ 15 Schutz von IT-Betriebsräumen und Produkten mit IT-Sicherheitsfunktionen

(1) Räume, in denen VS unkryptiert verarbeitet oder übertragen werden, sind gegen unbemerkten Zutritt Unbefugter zu schützen.

(2) Produkte mit IT-Sicherheitsfunktionen sind ab dem Zeitpunkt, zu dem feststeht, dass sie für VS eingesetzt werden sollen,

- in Räumen nach Absatz 1 oder entsprechend geschützten Räumen aufzubewahren,
- unter ständiger Kontrolle von VS-ermächtigtem Personal zu transportieren oder so

zu verpacken, dass ein Zugriff Unbefugter erkennbar wird,
- durch VS-ermächtigtes Personal zu installieren, zu warten und instand zu setzen, soweit nicht durch organisatorische Maßnahmen (z.B. keine Verarbeitung/Übertragung von VS in Anwesenheit von Personen und Beaufsichtigung dieser) ein Zugang zu VS auszuschließen ist, und
- in einem gesonderten Verzeichnis nachzuweisen (z. B. in der ITGA).

§ 16 Kennzeichnung von VS

(1) Bei der Darstellung von VS - z. B. Schriftgut - auf Sichtgeräten soll sich, soweit möglich, der Geheimhaltungsgrad auf jeder Seite oder Darstellung deutlich vom dargestellten Inhalt abheben (z.B. durch größere Schrift und Fettdruck); einer farblichen Unterscheidung bedarf es nicht.
(2) VS-Ausdrucke müssen gemäß 6.4 GHB gekennzeichnet sein. Davon abweichend braucht sich der Geheimhaltungsgrad farblich nicht vom ausgedruckten Inhalt zu unterscheiden. Bei STRENG GEHEIM oder GEHEIM eingestuften VS ist der Geheimhaltungsgrad jedoch auf der ersten Seite in roter Farbe anzubringen; ausgenommen VS-Zwischenmaterial, das nicht an Dritte weitergegeben wird.
(3) Datenträger mit unkryptierten VS sind mit dem höchsten Geheimhaltungsgrad der darauf gespeicherten VS gemäß GHB zu kennzeichnen. Bei fest installierten Datenträgern kann hierauf verzichtet werden. Die Kennzeichnung ist für kryptierte VS nicht erforderlich.

§ 17 Nachweis von VS

(1) Gespeicherte VS brauchen nicht einzeln nachgewiesen zu werden, ausgenommen die Fälle nach **§ 8** Abs. 2 Satz 2. Bei Übertragung von VS an Dritte genügt eine elektronische Empfangsbestätigung.
(2) Ausdrucke von VS sind unverzüglich der VS-Registratur zuzuleiten und im VS-Bestandsverzeichnis zu registrieren, ausgenommen VS-Zwischenmaterial, das nicht an Dritte weitergegeben wird.
(3) VS-Datenträger, ihr Verbleib und ihre Vernichtung sind in einem VS-Bestandsverzeichnis nachzuweisen. Zur Erfassung genügt die Angabe eines Ordnungskriteriums (z.B. fortlaufende Nummer) sowie des Einsatzbereichs (Organisationseinheit, IT-Nutzer) und eine Kurzangabe des Aufgabengebiets. VS-Datenträger sind grundsätzlich nur gegen Quittung weiterzugeben.

§ 18 Datensicherung und Wiederanlauf

(1) Im Rahmen der Datensicherung hinterlegte VS-Daten (einschließlich VS-eingestufter Programme) sind gemäß den VS-Vorschriften zu behandeln. Sind die VS-Daten kryptiert, sind die zum Dekryptieren benötigten Kryptodaten gesondert und entsprechend ihrer VS-Einstufung aufzubewahren.
(2) Bei Wiederanlauf-Vorkehrungen sind die erforderlichen Geheimschutzmaßnahmen einzubeziehen.

§ 19 Überprüfung der Maßnahmen und Freigabe von IT für VS

(1) Bevor ein IT-System erstmals für VS eingesetzt wird, hat der/die IT-VS-Beauftragte zu prüfen, ob die erforderlichen Geheimschutzmaßnahmen getroffen sind.
(2) Der/die IT-VS-Beauftragte entscheidet über die Freigabe des IT-Systems für VS. Grundsätzlich darf die Freigabe erst nach Genehmigung der entsprechenden ITGA durch BMWi erfolgen. Die Freigabe ist zu dokumentieren.
(3) Alle geheimschutzrelevanten Änderungen bei freigegebenen IT-Systemen bedürfen der vorherigen Zustimmung des/der IT-VS-Beauftragten. Die Änderungen sind in der ITGA zu dokumentieren. Bei wesentlichen Änderungen muss erneut die Genehmigung von BMWi eingeholt werden.

§ 20 Kontrollen/Auswertungen

(1) Der/die IT-VS-Beauftragte veranlasst in angemessenen zeitlichen Abständen schwerpunktmäßige Kontrollen. Es ist insbesondere zu kontrollieren, ob
- IT-Sicherheitskomponenten sicherheitsgerecht eingesetzt, gewartet und instandgesetzt werden,
- Zugriffsrechte in der erteilten Form erforderlich sind,
- Zugriffsrechte im IT-System korrekt zugewiesen sind und
- die Mittel zur Identifizierung / Authentisierung vorschriftsgemäß geschützt sind.

(2) Die protokollierten Daten im Rahmen der Beweissicherung sind regelmäßig daraufhin zu überprüfen, ob
- Zugangs-/Zugriffsversuche durch Unbefugte oder versuchte Rechteüberschreitungen vorgekommen sind und
- Zugriffe auf VS-Daten offensichtlich ungerechtfertigt erfolgten.

(3) Die Ergebnisse der Kontrollen sind zu dokumentieren.

§ 21 Technische Prüfungen

(1) Der/die IT-VS-Beauftragte hat bei IT-Systemen, die für VS eingesetzt werden in angemessenen zeitlichen Abständen folgende technischen Prüfungen zu veranlassen:
- Prüfung des IT-Systems unter den spezifischen Einsatzbedingungen, ob die erforderlichen IT-Sicherheitsfunktionen
  -- sachgerecht implementiert sind, keine erkennbaren Manipulationen aufweisen und auch nach Implementierung in das jeweilige IT-System wirksam greifen und nicht über einen Systemweg manipuliert oder umgangen werden können und
  -- auch bei einem Verbund mit anderen IT-Systemen diese Sicherheit aufweisen,
- Abstrahlsicherheits- und Manipulationsprüfungen bei abstrahlsicheren Räumen / Behältern, bei zonenvermessenen Räumen und bei für VS eingesetzter Hardware. Sofern sich Anhaltspunkte für technische Mängel ergeben, sind diese unverzüglich BMWi anzuzeigen.

(2) Für die Verarbeitung von STRENG GEHEIM eingestufte VS kann BMWi im Einzelfall besondere Regelungen für technische Prüfungen festlegen.

V. Schlussbestimmungen
§ 22 Sicherheitsvorkommnisse

(1) Wenn beim IT-Einsatz für VS oder im Zusammenhang damit bekannt wird oder der Verdacht entsteht, dass
- Unbefugte Zugriff auf VS erhalten haben oder ihn sich verschaffen wollten,
- IT-Systeme / -Komponenten sicherheitserhebliche Mängel aufweisen, manipuliert oder entwendet wurden oder
- die Geheimhaltung von VS in anderer Weise verletzt wurde oder gefährdet ist,

ist unverzüglich der/die IT-VS-Beauftragte zu benachrichtigen.

(2) Der/die IT-VS-Beauftragte veranlasst bei Gefahr im Verzuge die unmittelbar erforderlichen Maßnahmen. Er/sie hat bei Feststellung schwerwiegender Mängel bis zu deren Beseitigung den IT-Einsatz für VS einzuschränken oder zu untersagen. Der/die SiBe ist unverzüglich zu unterrichten.

(3) Sicherheitsvorkommnisse und daraufhin veranlasste Maßnahmen sind zu dokumentieren. Die Dokumentation ist mindestens fünf Jahre aufzubewahren.

§ 23 IT-Geheimschutzdokumentation

Es ist eine IT-Geheimschutzdokumentation zu führen, die
- IT-Geheimschutz-Anweisungen (ITGA's) und Freigabebestätigungen für IT-Systeme und zugrundeliegende Prüfungsergebnisse, für jeweils fünf Jahre sowie
- Dokumentationen der Vergabe, Änderung und Rücknahme von Zugriffsrechten, Kontroll-/Prüfberichte und Berichte über Sicherheitsvorkommnisse für jeweils fünf Jahre

enthält.