Richtlinien
zum Geheimschutz von Verschlusssachen
beim Einsatz von Informationstechnik
(VS-IT-Richtlinien – VSITR)

Inhaltsverzeichnis

Nach § 64 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen für das Land Schleswig-Holstein (VS-Anweisung – VSA SH) werden mit Wirkung vom 01.03.2004 die nachstehenden Richtlinien erlassen. Die VS-Datenrichtlinien vom 10.12.1980 und die VS-Fernmelderichtlinien vom 01.03.1986 werden gleichzeitig außer Kraft gesetzt.

I.
Allgemeiner Teil

§ 1
Zweck und Anwendungsbereich

(1) Die Richtlinien regeln, welche Maßnahmen zur Geheimhaltung von VS beim Einsatz von Informationstechnik (IT) ergänzend zur oder abweichend von der VS-Anweisung zu treffen sind. Von diesen Richtlinien kann im Einzelfall im Einvernehmen mit der Verfassungsschutzbehörde des Landes abgewichen werden, wenn der beabsichtigte Zweck durch andere Sicherheitsvorkehrungen erreicht wird.

(2) Die Richtlinien sind anzuwenden, wenn VS-VERTRAULICH oder höher[1] eingestufte VS mit IT verarbeitet[2] oder übertragen[3] werden.

§ 2
Eingeschränkte Geheimschutzmaßnahmen

Werden in einer Dienststelle nur ausnahmsweise VS-VERTRAULICH eingestufte VS mit IT verarbeitet oder in einem lokalen Kommunikationsnetz übertragen, so brauchen diese Richtlinien bis auf folgende Maßnahmen nicht angewandt zu werden:

---

1 Zu VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS siehe Anlage 7 zur VSA SH. Die Anlage ist auch im Behördenbereich anzuwenden.

2 Dies schließt das Speichern von Daten ein.

3 Darunter fällt neben der Übermittlung von Daten an Dritte auch die Übertragung von Daten zwischen technischen Komponenten im eigenen Bereich.

1. Die IT-Nutzerinnen oder -Nutzer müssen bei der

   a) Verarbeitung von VS sicherstellen, dass Unbefugte keine Kenntnis von den VS erhalten und

   b) Übertragung von VS sicherstellen (z. B. durch Telefonanruf), dass die Nachricht die berechtigte Empfängerin oder den Empfänger unverzüglich erreicht.

2. Die VS-Datenträger sind nach der VS-Anweisung zu behandeln.

3. Durch organisatorische Maßnahmen (z. B. persönliche Zuordnung und gesonderte Verwahrung von VS-Datenträgern) ist sicherzustellen, dass der Grundsatz „Kenntnis nur, wenn nötig" beachtet wird.

4. VS-Daten, die nicht mehr benötigt werden, sind vollständig mit nicht eingestuften Daten zu überschreiben.

§ 3
Kommunikation im inter-/supranationalen Bereich

Bei der Kommunikation mit Partnern im inter-/supranationalen Bereich (z. B. NATO, WEU) gehen die jeweiligen inter-/supranationalen Bestimmungen und Abkommen vor.

§ 4
Begriffsbestimmungen

Im Sinne dieser Richtlinien umfasst

1. „VS-Datenträger“ ein Speichermedium, das VS enthält, soweit diese nicht nur in flüchtiger Form vorliegen,

2. „Kryptosystem" alle Mittel, die für eine bestimmte Kryptierung und Dekryptierung benötigt werden (z. B. Kryptogerät und Kryptodaten),

3. „Kryptodaten" eine Folge von Zeichen, die als Parameter zum Kryptieren und Dekryptieren benötigt werden,

4. „IT-Sicherheitsfunktion" eine mit IT realisierte Sicherheitsvorkehrung, insbesondere zur Kryptierung, Abstrahlsicherheit, Zugangs-/Zugriffskontrolle, Beweissicherung, Protokollauswertung, Wiederaufbereitung oder Wahrung der Unverfälschtheit von Software.

II.
Zuständigkeiten

§ 5
Verantwortliche(r) für IT-Geheimschutzmaßnahmen

Behörden mit komplexen IT-Systemen oder vielfältigen IT-Anwendungen für VS bestimmen eine Verantwortliche oder einen Verantwortlichen mit IT-Fachkenntnissen, der die Geheimschutzbeauftragte oder den Geheimschutzbeauftragten bei der Umsetzung dieser Richtlinien unterstützt oder auf Weisung der Behördenleiterin oder des Behördenleiters eigenverantwortlich für die Durchführung dieser Richtlinien sorgt. Sie oder er soll möglichst nicht zugleich Aufgaben der Systemadministration bei für VS eingesetzten IT-Systemen wahrnehmen und in der Durchführung dieser Richtlinien besonders geschult sein. Wird eine/ein Verantwortliche(r) für IT-Geheimschutzmaßnahmen nicht bestimmt, so verbleiben deren/dessen Aufgaben bei der oder dem Geheimschutzbeauftragten.

§ 6
Mitwirkung der Verfassungsschutzbehörde des Landes und des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[1]

(1) Die Verfassungsschutzbehörde des Landes bzw. auf deren Veranlassung hin das BSI wirkt nach § 60 VSA SH bei der Durchführung dieser Richtlinien mit. Die Mitwirkung umfasst insbesondere Beratung, Schulung und technische Prüfungen.

---

[1] Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 183, 53133 Bonn, Telefon: (02 28) 95 82-0, Telefax:-4 00

(2) Das BSI gibt zur Umsetzung dieser Richtlinien Hinweise heraus. Sie sollen sich insbesondere auf Folgendes erstrecken:

1. Verwendung von Passwörtern und Personenidentifikationsnummern (PIN),
2. Installation von Hardware, die für VS eingesetzt werden soll,
3. Beurteilung der Gefahr der kompromittierenden Abstrahlung und deren Nutzung durch Dritte,
4. Sicherung von Leitungen für die unkryptierte Übertragung von VS,
5. Schutz von IT-Betriebsräumen und Produkten mit IT-Sicherheitsfunktionen,
6. Überprüfung neuer oder geänderter Betriebs-/Anwendungs-Software,
7. Überprüfung der Geheimschutzmaßnahmen vor Freigabe von IT für VS,
8. Freigabe nicht zugelassener Produkte mit IT-Sicherheitsfunktionen für VS,
9. Tätigkeiten, bei denen nach § 15 Abs. 2 Nr. 7 VSA SH die Möglichkeit besteht, sich Zugang zu VS zu verschaffen.

III.
IT-Planung

§ 7
IT-Planung und -Beschaffung

(1) Ist geplant, IT für VS einzusetzen, so ist die oder der für IT-Geheimschutzmaßnahmen Verantwortliche bereits zu Planungsbeginn zu beteiligen. Bei komplexen IT-Systemen oder vielfältigen IT-Anwendungen für VS soll die Verfassungsschutzbehörde des Landes beratend hinzugezogen werden.

(2) Vor der Beschaffung von IT, die für VS eingesetzt werden soll, muss ein IT-Geheimschutzkonzept vorliegen. Darauf basierend ist in die Beschaffungsaufträge aufzunehmen, welche IT-Sicherheitsfunktionen das IT-System enthalten muss und welche Sicherheitsleistungen die IT-Hersteller/-Vertreiber zu erbringen haben. Es ist insbesondere sicherzustellen, dass

1. Produkte mit IT-Sicherheitsfunktionen die nach § 17 erforderliche Zulassung aufweisen und sicherheitsgerecht implementiert werden,

2. Produkte mit IT-Sicherheitsfunktionen ab dem Zeitpunkt, zu dem feststeht, dass sie für VS eingesetzt werden sollen, geschützt aufbewahrt und transportiert werden (siehe § 18 Abs. 2),

3. eine sicherheitsgerechte Wartung und Instandsetzung (siehe § 14) erfolgt.

§ 8
IT-Geheimschutzkonzept und Dienstanweisungen

(1) Es soll ein IT-Geheimschutzkonzept erstellt werden, das Folgendes enthalten muss:

1. Eine Übersicht über

   a) die Aufgaben, bei denen VS anfallen und die unter Einsatz von IT erledigt werden oder erledigt werden sollen und die für die Aufgaben zuständigen Organisationseinheiten,

   b) die VS-Einstufungen der Daten/Programme und die voraussichtliche Häufigkeit des IT-Einsatzes für VS,

   c) die eingesetzte/vorgesehene IT (z. B. Hardware, Betriebssysteme, Anwendungs-Software, Datenträger) und die darin enthaltenen IT-Sicherheitsfunktionen.

2. Systemspezifische Dienstanweisungen mit Angabe des Anwendungsbereichs und

3. eine Übersicht über die Vorkehrungen der IT-Notfallvorsorge und die diesbezüglichen Geheimschutzmaßnahmen.

Die Angaben können in einem IT-Sicherheitskonzept enthalten sein, soweit keine Geheimhaltungsgründe entgegenstehen.

(2) Das IT-Geheimschutzkonzept ist bei geheimschutzrelevanten Änderungen, spätestens jedoch im jährlichen Abstand, auf notwendige Anpassungen zu überprüfen.

§ 9

Vergabe des IT-Einsatzes an Dritte

(1) Bei Vergabe des IT-Einsatzes an eine andere Behörde ist sicherzustellen, dass diese die erforderlichen Geheimschutzmaßnahmen trifft.

(2) Die Vergabe des IT-Einsatzes an ein Unternehmen ist zulässig, wenn die Behördenleiterin oder der Behördenleiter nach Abwägung der Wirtschaftlichkeits- und Sicherheitsinteressen zugestimmt hat und bei dem Unternehmen die erforderlichen Geheimschutzmaßnahmen getroffen sind (siehe § 49 Abs. 3 VSA SH).

IV.
IT-Einsatz

§ 10

Zugangs-/Zugriffskontrolle und Zugriffsrechte

(1) IT-Systeme, die für VS eingesetzt werden, müssen über ein zuverlässiges Zu gangs-/Zugriffskontrollsystem verfügen, so dass nur Befugte im Rahmen der ihnen erteilten Rechte Zugang erhalten und auf VS zugreifen können. Wiederholte abgewiesene Zugangs-/Zugriffsversuche sollen für diese Personen zur Systemsperrung führen. Diese darf nur von der für IT-Geheimschutzmaßnahmen verantwortlichen Person aufzuheben sein.

(2) Bei der Vergabe, Änderung und Rücknahme von Rechten muss gewährleistet sein, dass

1. ein dazu erforderlicher Antrag von einer berechtigten Stelle stammt,
2. die zu berechtigende Person eine ausreichende VS-Ermächtigung besitzt,
3. der Grundsatz „Kenntnis nur, wenn nötig" beachtet wird und
4. keine sicherheitsmäßig unvereinbare Bündelung von Funktionen entsteht.

Die Übertragung der Befugnis zur Vergabe und Änderung von Rechten bedarf der Zustimmung der oder des nach § 5 Verantwortlichen.

(3) Die Vergabe, Änderung und Rücknahme von Rechten ist so zu dokumentieren, dass jederzeit feststellbar ist, wer zu welchen Zeiten

1. zur Vergabe, Änderung oder Rücknahme von Rechten in welchem Umfang berechtigt war und
2. welche für den Geheimschutz relevanten Rechte ausüben konnte.

Die Dokumentation ist mindestens zehn Jahre aufzubewahren.

(4) Zur Identifizierung/Authentisierung eingesetzte Mittel eines Rechteinhabers sind wie folgt zu behandeln:

1. Mittel in Form von Besitz (z. B. Chipkarten) wie Schlüssel zu VS-Verwahrgelassen und
2. Mittel in Form von Wissen (z. B. PIN oder Passwort) wie Zahlenkombinationen zu VS-Verwahrgelassen.

Die in Nummer 1 genannten Mittel können anstelle einer Aufbewahrung in einem VS-Schlüsselbehälter auch in persönlichem Gewahrsam gehalten werden. Einzelheiten über die Auswahl, Vergabe, Kontrolle und den Wechsel von Passworten/PIN sollen in einer Dienstanweisung festgelegt sein.

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

§ 11
Beweissicherung und Protokollauswertung

(1) Für VS eingesetzte IT-Systeme sollen über eine automatische Beweissicherung Folgendes aufzeichnen:

1. Zugangs-/Zugriffsversuche durch Unbefugte,

2. versuchte Rechteüberschreitungen,
3. Ausdrucke, Ausgaben von VS auf Datenträger sowie Übermittlungen von VS sowie
4. Zugriffe auf VS-Daten (wer hat zu welchem Zeitpunkt welche Rechte ausgeübt).

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

(2) Abgewiesene Zugangs-/Zugriffsversuche sollen vom IT-System unmittelbar der oder dem für IT-Geheimschutzmaßnahmen Verantwortlichen oder einer von ihr oder ihm beauftragten Person angezeigt oder revisionssicher protokolliert werden. Ausdrucke und Ausgaben von VS auf Datenträger, die zur Weitergabe 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 sollen nur der oder dem für IT-Geheimschutzmaßnahmen Verantwortlichen oder einer von ihr oder ihm beauftragten Person erlaubt sein. Die Aufzeichnungen sind, soweit keine zwingenden Gründe entgegenstehen, nach Überprüfung durch die oder den für IT-Geheimschutzmaßnahmen Verantwortlichen oder eine von ihr oder ihm beauftragte Person zu löschen.

§ 12
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 mehr 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 STRENG GEHEIM oder GEHEIM eingestufte VS unkryptiert enthalten haben, sind zusätzlich physikalisch zu löschen oder zu

vernichten. Dies gilt auch für VS-Datenträger mit VS-VERTRAULICH eingestuften VS, wenn eine Wiederaufbereitung nicht möglich ist.

§ 13
Schutz der Software und Testläufe

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

(2) Der Einsatz neuer oder geänderter Betriebs-/Anwendungs-Software sowie Testläufe sind der oder dem für IT-Geheimschutzmaßnahmen Verantwortlichen rechtzeitig vorher anzuzeigen, der bei

1. neuer oder geänderter Betriebs-/Anwendungs-Software feststellt, ob eine Überprüfung erforderlich ist und im Bedarfsfalle entscheidet, wie diese zu erfolgen hat,

2. Testläufen sicherstellt, dass diese nicht während der VS-Verarbeitung/-Übertragung durchgeführt werden, grundsätzlich nicht mit VS erfolgen und dass Geheimschutzvorkehrungen nicht beeinträchtigt werden.

Soweit wesentliche Beeinträchtigungen des Geheimschutzes möglich sind, kann die oder der für IT-Geheimschutzmaßnahmen Verantwortliche den Einsatz von Betriebs-/Anwendungs-Software bis zur Vorlage eines positiven Prüfergebnisses sowie die Durchführung von Testläufen untersagen.

§ 14
Systemwartung

(1) Vor Wartungs- oder Instandsetzungsarbeiten sollen die VS aus dem IT-System entfernt werden. Ist dies nicht möglich, ist entsprechend sicherheitsüberprüftes 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 ist nur zulässig, wenn

1. die Fernwartung durch eigenes, sicherheitsüberprüftes und nach Bedarf zum Zugang zu VS ermächtigtes Personal erfolgt,

2. für die Übertragungen im Rahmen der Fernwartung zugelassene Kryptosysteme eingesetzt sind und

3. eine zuverlässige Zugriffskontrolle, Beweissicherung und Überprüfung der Aufzeichnungen erfolgt.

Die Fernwartung soll nur zu Zeiten erfolgen, zu denen keine VS-Verarbeitung/-Übertragung stattfindet und wenn alle im IT-System zugänglichen VS-Daten kryptiert oder gelöscht sind.

(3) Die Behördenleiterin oder der Behördenleiter kann abweichend von Absatz 2 zulassen, dass ein Unternehmen die Fernwartung durchführt, wenn

1. ihr oder ihm ein Sicherheitsbescheid des Bundesministeriums für Wirtschaft und Arbeit über das Unternehmen vorliegt oder eine andere oberste Bundes- oder Landesbehörde für die erforderlichen Geheimschutzmaßnahmen bei dem Unternehmen gesorgt hat (siehe § 49 VSA SH),

2. eine gesonderte Freischaltung und Beendigung jedes Fernwartungsvorganges durch die Dienststelle erfolgt und

3. nach Absatz 2 Satz 1 Nr. 2 bis 3 und Satz 2 verfahren wird.

§ 15
Abstrahlsicherheit

(1) IT-Hardware, die VS unkryptiert führt, soll unter Beachtung der Hinweise des BSI (siehe § 6 Abs. 2 Nr. 2) installiert sein.

(2) Es ist durch die oder den für IT-Geheimschutzmaßnahmen Verantwortlichen unter Beachtung der Hinweise des BSI (siehe § 6 Abs. 2 Nr. 3) zu prüfen und durch die Behördenleiterin oder den Behördenleiter zu entscheiden, inwieweit mit einer erheblichen Gefährdung der Geheimhaltung der VS durch Nutzung von kompromittierender Abstrahlung durch Unbefugte zu rechnen ist. Ist mit einer erheblichen Gefährdung zu rechnen, so muss die IT-Hardware

1. in vom BSI zugelassenen abstrahlsicheren Räumen betrieben werden oder
2. eine Zulassung des BSI für den Betrieb innerhalb einer bestimmten Sicherheitszone aufweisen und innerhalb einer solchen betrieben werden oder
3. vom BSI als abstrahlsicher zugelassen sein.

§ 16
Speicherung, Übertragung und Netzanbindung

(1) VS sind bei Speicherung und Übertragung zu kryptieren. Bei der Speicherung von VS ist eine Kryptierung nicht erforderlich, wenn die VS materiell nach der VS-Anweisung gesichert sind und die Rechner nicht oder nur über ein Kryptosystem oder nach Satz 3 an ein Kommunikationsnetz angeschlossen sind. Bei der Übertragung von VS kann, über die bestehenden Ausnahmen nach § 47 Abs. 2 VSA SH hinaus, eine Kryptierung unterbleiben

1. innerhalb eines zutrittsgeschützten IT-Betriebsraumes (siehe § 18),

2. wenn die Übertragungseinrichtungen so geschützt sind, dass ein Zugriff Unbefugter unverzüglich erkannt wird (approved circuits) oder

3. wenn in einem lokalen Netz

   a) nur VS-VERTRAULICH oder ausnahmsweise GEHEIM eingestufte VS übertragen werden,

b) ein Zugriffskontrollsystem nach § 10 Abs. 1 eingesetzt ist und

c) die Übertragungseinrichtungen sich vollständig in einem Bereich mit zuverlässiger Zutrittskontrolle befinden oder außerhalb gegen unmittelbaren Zugriff Unbefugter geschützt sind;

bei Verbindung mit einem anderen Kommunikationsnetz müssen dieses und die Verbindung zu diesem mindestens nach Buchstabe b und c geschützt sein.

(2) Soweit die für den Betrieb eines Kryptosystems benötigten Kryptodaten nicht automatisch bereitgestellt werden, dürfen diese nur vom BSI oder einer vom BSI anerkannten Stelle hergestellt werden. Für die Verwaltung von auf dem Kurier-/Postweg bereitgestellten Kryptodaten ist eine Kryptoverwalterin/-Vertreterin oder ein Kryptoverwalter/-Vertreter zu bestellen. Sie oder er gibt die Kryptodaten in die Kryptosysteme ein oder bei Bedarf an die befugten IT-Nutzerinnen oder -Nutzer aus. Namen und Behördenanschrift der Kryptoverwalterin/-Vertreterin oder des Kryptoverwalters/-Vertreters sowie Änderungen sind dem BSI oder der vom BSI anerkannten Stelle mitzuteilen.

§ 17
Zulassung von Produkten mit IT-Sicherheitsfunktionen

(1) Produkte mit Funktionen zur

1. Kryptierung,
2. Abstrahlsicherheit,
3. Löschung oder Vernichtung von VS-Datenträgern oder
4. Sicherung von Übertragungsleitungen (approved circuits)

müssen vom BSI zugelassen sein. Die Zulassung hat auch die erforderlichen Angaben zu den Einsatz- und Betriebsbedingungen zu enthalten.

(2) Produkte mit Funktionen zur

1. Zugangs-/Zugriffskontrolle,

2. Beweissicherung und Protokollauswertung,
3. Wiederaufbereitung von VS-Datenträgern oder
4. Unverfälschtheit von Software

sollen vom BSI zugelassen sein. Die Behördenleiterin oder der Behördenleiter kann die Verwendung anderer Produkte freigeben, insbesondere wenn sich Produkte zum Zeitpunkt des Inkrafttretens dieser Richtlinien bereits im Einsatz oder in der Beschaffung befinden oder im Einzelfall keine geeigneten zugelassenen Produkte verfügbar sind und eine Zulassung nicht oder nicht zeitgerecht veranlasst werden kann.

(3) Die Zulassungen 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. Die näheren Einzelheiten legt das BSI in einem Zulassungskonzept fest.

§ 18
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; § 21 und § 52 VSA SH bleiben unberührt.

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

1. in Räumen nach Absatz 1 oder entsprechend geschützten Räumen aufzubewahren,

2. unter ständiger Kontrolle von sicherheitsüberprüftem Personal zu transportieren oder so zu verpacken, dass ein Zugriff Unbefugter erkennbar wird,

3. durch sicherheitsüberprüftes Personal (siehe § 15 Abs. 2 VSA SH) zu installieren, zu warten und instand zu setzen, soweit nicht durch organisatorische Maßnahmen (z. B. keine Verarbeitung/Übertragung von VS in Anwesenheit der Personen und

Beaufsichtigung dieser) ein Zugang zu VS auszuschließen ist, und

4. in einem Bestandsverzeichnis nachzuweisen.

§ 19
Kennzeichnung von VS

(1) Bei der Darstellung von VS auf Sichtgeräten soll sich 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 nach der VS-Anweisung gekennzeichnet sein. Abweichend von der VS-Anweisung 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) Für VS-Datenträger gilt Folgendes:

1. Datenträger mit unkryptierten VS sind mit dem höchsten Geheimhaltungsgrad der darauf gespeicherten VS nach der VS-Anweisung zu kennzeichnen.[1]

2. Dieser Kennzeichnung bedarf es nicht, wenn die VS kryptiert sind.

§ 20
Nachweis von VS

(1) Gespeicherte VS brauchen nicht einzeln nachgewiesen zu werden, ausgenommen die Fälle nach § 11 Abs. 2 Satz 2. Bei Übermittlung von VS genügt abweichend von der VS-Anweisung eine elektronische Empfangsbestätigung.

[1] Bei fest installierten Datenträgern kann darauf verzichtet werden.

(2) Ausdrucke 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 gesonderten 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.

§ 21
Notfallvorsorge (Datensicherung und Wiederanlauf)

(1) Im Rahmen der Datensicherung hinterlegte VS-Daten (einschließlich VS eingestufter Programme) sind nach den VS-Vorschriften zu behandeln. Sind die VS-Daten kryptiert, sind die zum Dekryptieren benötigten Kryptodaten gesondert und entsprechend ihrer VS-Einstufung aufzubewahren.

(2) In Wiederanlauf-Vorkehrungen sind die erforderlichen Geheimschutzmaßnahmen einzubeziehen.

§ 22
Überprüfung der Maßnahmen und Freigabe von IT für VS

(1) Bevor ein IT-System erstmals für VS eingesetzt wird, hat die oder der für IT-Geheimschutzmaßnahmen Verantwortliche eine Überprüfung zu veranlassen, ob die erforderlichen Geheimschutzmaßnahmen getroffen sind. Bei komplexen IT-Systemen oder vielfältigen IT-Anwendungen soll die Verfassungsschutzbehörde des Landes beratend hinzugezogen werden.

(2) Die Behördenleiterin oder der Behördenleiter entscheidet über die Freigabe des IT-Systems für VS. Die Freigabe ist zu dokumentieren.

(3) Geheimschutzrelevante Änderungen bei freigegebenen IT-Systemen, insbesondere der Einsatz für höher eingestufte VS, bedürfen der vorherigen Zustimmung der oder des für IT-Geheimschutzmaßnahmen Verantwortlichen, die oder der vor wesentlichen Änderungen nach Absatz 1 und 2 verfährt.

§ 23
Kontrollen

(1) Die oder der für IT-Geheimschutzmaßnahmen Verantwortliche veranlasst in angemessenen zeitlichen Abständen schwerpunktmäßige Kontrollen. Es ist insbesondere zu kontrollieren, ob

1. IT-Sicherheitskomponenten sicherheitsgerecht eingesetzt, gewartet und instand gesetzt werden,
2. Zugriffsrechte in der erteilten Form erforderlich sind,
3. Zugriffsrechte im IT-System korrekt zugewiesen sind und
4. die Mittel zur Identifizierung/Authentisierung vorschriftsmäßig geschützt sind.

(2) Die protokollierten Daten im Rahmen der Beweissicherung sind regelmäßig daraufhin zu überprüfen, ob

1. Zugangs-/Zugriffsversuche abgewiesen wurden und
2. Zugriffe auf VS-Daten offensichtlich ungerechtfertigt erfolgten.

§ 24
Technische Prüfungen

(1) Die oder der für IT-Geheimschutzmaßnahmen Verantwortliche hat bei IT-Systemen, die für STRENG GEHEIM oder nicht nur ausnahmsweise für GEHEIM eingestufte VS eingesetzt werden, vor dem erstmaligen Einsatz für VS und danach schwerpunktmäßig in angemessenen zeitlichen Abständen folgende technischen Prüfungen durch das BSI oder eine vom BSI anerkannte Stelle zu veranlassen:

1. Eine Prüfung des IT-Systems unter den spezifischen Einsatzbedingungen, ob die erforderlichen IT-Sicherheitsfunktionen

   a) 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

   b) auch bei einem Verbund mit anderen IT-Systemen diese Sicherheit aufweisen.

2. Abstrahlsicherheits- und Manipulationsprüfungen bei abstrahlsicheren Räumen/ Behältern, bei zonenvermessenen Räumen (siehe § 15 Abs. 2 Nr. 2) und bei für VS eingesetzter Hardware und

3. eine Überprüfung von Sicherheitszonen nach § 15 Abs. 2 Nr. 2 auf mögliche Einrichtungen zur Erfassung/Übertragung kompromittierender Nahbereichsabstrahlung.

(2) Bei IT-Systemen, die über den Fall des § 2 hinaus für VS-VERTRAULICH eingestufte VS eingesetzt werden, sollen stichprobenweise entsprechende technische Prüfungen erfolgen. Das BSI und die von ihm anerkannten Stellen sind bei den Prüfungen im erforderlichen Umfange zu unterstützen.

(3) Das BSI und die von ihm anerkannten Stellen teilen die Ergebnisse der Prüfungen (was wurde mit welchem Ergebnis geprüft und wie ist dies sicherheitsmäßig zu bewerten) der oder dem für IT-Geheimschutzmaßnahmen Verantwortlichen in Form von Prüfberichten mit.

V.
Schlussbestimmungen

§ 25
Sicherheitsvorkommnisse

(1) Wenn beim IT-Einsatz für VS oder im Zusammenhang damit bekannt wird oder der Verdacht entsteht, dass

1. Unbefugte Zugriff auf VS erhalten haben oder ihn sich verschaffen wollten,
2. IT-Systeme/-Komponenten sicherheitserhebliche Mängel aufweisen, manipuliert oder entwendet wurden oder
3. die Geheimhaltung von VS in anderer Weise verletzt wurde oder gefährdet ist,

so ist unverzüglich die oder der für IT-Geheimschutzmaßnahmen Verantwortliche zu benachrichtigen.

(2) Die oder der für IT-Geheimschutzmaßnahmen Verantwortliche veranlasst bei Gefahr im Verzuge die ersten notwendigen Maßnahmen. Er kann bei Feststellung schwerwiegender Mängel bis zu deren Beseitigung den IT-Einsatz für VS einschränken oder untersagen. Im Übrigen unterrichtet sie oder er die Geheimschutzbeauftragte oder den Geheimschutzbeauftragten, die oder der nach § 57 VSA SH verfährt.

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

§ 26
IT-Geheimschutzdokumentation

(1) Es soll eine IT-Geheimschutzdokumentation geführt werden, die mindestens Folgendes enthält:

1. Die Vorschriften/Dienstanweisungen zum Zwecke des IT-Geheimschutzes,
2. das IT-Geheimschutzkonzept,

3. Freigabebestätigungen für IT-Systeme und die zugrunde liegenden Prüfungsergebnisse,
4. die Dokumentation der Vergabe, Änderung und Rücknahme von Zugriffsrechten,
5. Kontroll-/Prüfberichte und
6. Berichte über Sicherheitsvorkommnisse.

(2) Die Dokumentation muss aktuell sein und soll die Unterlagen nach

1. Nummer 1 bis 3 für die letzten fünf Jahre und
2. Nummer 4 bis 6 für die letzten zehn Jahre

enthalten.