Informationstechnische Geheimschutzanweisung ITGA Nr.: *xy*

(Arbeitsanweisung für die Bearbeitung von VS mit IT-Systemen)

BMWi-Firmen-Nr.	VS-Auftragnehmer	Ausgabedatum	Änderungsstand *)
4711-4711	***XYZ GMBH***	*Datum der Ersterstellung*	*Datum der Änderung*
Adresse: ***Musterstraße 1234 Musterdorf*** Abteilung: ***Sicherheit 1***		Genehmigung BMWi *Datum Genehmigungs-schreiben BMWi*	In Kraft gesetzt

Titel VS-Auftrag:	***Musterjet***
VS-Auftragsnummer:	***xyz/111/999-2013***
VS-Einstufung:	***Geheimhaltungsgrad Auftrag***

IT-Systeme / IT-Betriebsräume	***Bemerkungen***
IT-Systeme: ***6 VS PC, 10 VS Laptops***	*Konfiguration lt. Anhang 3*
VS-Kopplung **: ☐ **keine** ☐ **mit ITGA *XYZ***	
VS-Vernetzung ***: ☐ **keine** ☐ **lokales VS-Netz**	
Maßnahmen zum Abstrahlschutz werden vom **VS**-Auftraggeber gefordert: ☐ **ja** ☐ **nein**	
Umsetzung der Maßnahmen: ☐ **nach nat. Zonenmodell** ☐ **Einsatz von Hardware nach SDIP27 Level A** ☐ **HF-Kabine** ☐ **andere Maßnahmen z.B. DfmA**	
Standorte: Kontrollzone ***xy***, Sperrzone ***xy***	

* Datum der letzten Änderung, einzelne Seiten können unterschiedliche Stände haben
** VS-Kopplung mit mind. einer weiteren ITGA (national) bzw. internationalem Standort
*** VS-Vernetzung entspricht einer lokalen Vernetzung des VS-IT-Systems innerhalb der ITGA

_____ Sicherheitsbevollmächtigter(SiBe)

_____ Systemverantwortlicher *

* Sicherheitsbestimmungen zur Kenntnis genommen.

Verteiler:

BMWi
Projektleiter / Systemverantwortlicher
Umlauf VS-Zugriffsberechtigte (falls vorhanden)
SiBe

Inhaltsverzeichnis

Präambel

Grundlage für diese IT-Geheimschutzanweisung (ITGA) ist das Handbuch für den Geheimschutz in der Wirtschaft (GHB), herausgegeben vom Bundesministerium für Wirtschaft und Energie (BMWi) in der Fassung von 2004, einschließlich der nachträglich herausgegebenen Ergänzungen und Nachträge sowie die VS-IT-Richtlinien/U (VSITR/U) des BMWi und die Anweisungen des Sicherheitsbevollmächtigten (SiBe). Jede IT-VS-Be- und Verarbeitung setzt für die einzelne IT-VS-Betriebsstelle eine vom BMWi genehmigte ITGA voraus.

Diese Anweisung regelt die Einzelheiten des Betriebsablaufs für das beschriebene IT-System. Sie beschreibt die erforderlichen Maßnahmen zum Schutz von VS beim Einsatz von Informationstechnik (IT).
Bei internationalen Projekten sind zusätzliche, beispielsweise auf zwischenstaatlicher Ebene vereinbarte Regelungen zu beachten.

1. Geltungsbereich

Diese Anweisung gilt nur für die Bearbeitung von Verschlusssachen (VS), die **VS-VERTRAULICH** oder **GEHEIM** eingestuft sind und im Zusammenhang mit der in Anhang 3 aufgeführten Hardware- und System-/Standardsoftware-Konfiguration, die im Bereich der definierten IT-VS-Betriebsstelle installiert ist.

Sie regelt die Vorgehensweise bei Wartung, Reparatur und Instandsetzung der betroffenen IT-VS-Systeme.

Bei VS mit der Einstufung VS-NUR FÜR DEN DIENSTGEBRAUCH ist nach dem VS-NfD-Mekblatt (GHB, Anlage 4) zu verfahren.

2. IT-VS-Betriebsstelle

Der Raum, in dem sich die Hardware befindet (s. Deckblatt), bildet insgesamt die IT-VS-Betriebsstelle. Die IT-VS Betriebsstelle befindet sich in der Verantwortung der *(Unternehmen*). In der IT-VS-Betriebsstelle erfolgt die IT-VS-Bearbeitung nach den Grundsätzen des persönlichen Gewahrsams (siehe auch Ziffer 6.1). Die IT-Anlage darf nur in der entsprechenden VS-Sperr- bzw. VS-Kontrollzone betrieben werden *(genaue Bezeichnung hier eintragen),* dies gilt auch für offene Bearbeitung.
Die VS-Sperr- bzw. VS-Kontrollzonenanweisung ist zu beachten.

In diesem Bereich werden VS (Verschlusssachen) bis zum VS-Grad

☐ **VS-VERTRAULICH**

☐ **GEHEIM**

bearbeitet**.**

3. Personelle Zuständigkeiten / Projekte und Aufträge

Die personellen Zuständigkeiten sind im Anhang 2 geregelt.
Alle dort benannten Personen müssen VS-ermächtigt sein, und zwar mindestens bis zu dem Einstufungsgrad der zu bearbeitenden Daten-VS.
Eine Aufstellung über die Zugriffsberechtigten mit dem entsprechenden Zeitraum der Berechtigung ist während der Dauer des Projektes sowie anschließend im Rahmen der Geheimschutzdokumentation (5 Jahre) als Anlage zu der ITGA vorzuhalten.

☐ Projekte und Aufträge die mit dieser ITGA bearbeitet werden, sind auf dem Deckblatt abschließend aufgeführt.

Alternativ:

☐ Eine Übersicht über die VS- Projekte / VS-Aufträge die mit dem IT-System bearbeitet werden ist als Anlage beigefügt und die tagesaktuelle Übersicht über die VS-Projekte die mit dem IT-System bearbeitet werden, wird durch den SiBe / IT-VS-Beauftragten geführt. Die Übersicht ist dem BMWi nach Aufforderung vorzulegen.

4. IT-VS-Verwaltung

4.1 Grundsätzliche Regelungen der VS-Verwaltung

- Datenträger (Disketten, Wechselfestplatten, Flash-Speicher, Tapes, CD-ROM etc.) für die IT-VS-Bearbeitung sind vor dem Beginn der VS-Arbeiten der VS-Registratur zur Registrierung zu übergeben.
- Formatierung und Erstinstallation der entsprechenden Datenträger werden mit der Original-Software durch den Systemverantwortlichen/IT-VS-Beauftragten durchgeführt.
- Datenträger werden nur durch die VS-Registratur gekennzeichnet, registriert und ausgegeben. Nach Fertigstellung der VS-Unterlage sind alle Datenträger an die VS-Registratur zurückzuliefern.
- Unbrauchbar gewordene Datenträger sind an die VS-Registratur zurückzugeben.
- Jede Kopie eines Datenträgers mit Tagebuch-Nr. bedarf eines entsprechenden schriftlichen Vervielfältigungsauftrages (VS-Registratur).
- Für die Erstellung von Sicherungskopien von Datenträgern, die noch VS-Zwischenmaterial sind, wird kein Vervielfältigungsauftrag benötigt.
- Die Verwendung nicht registrierter oder privater Datenträger ist untersagt.

4.2 Registrierung und Kennzeichnung von IT-VS

4.2.1 Ausgabe der IT-VS-Datenträger

Datenträger (Wechselfestplatten, Disketten, Flash-Speicher, Tapes, CD-ROM, Notebooks) für die VS-Bearbeitung sind zur Ersterfassung bei der VS-Registratur anzuliefern und werden dort gem. den Bestimmungen für VS-Material verwaltet.
Befinden sich herausnehmbare Speichermedien in Behältern, Hüllen o.ä., so sind auch diese entsprechend zu kennzeichnen.
Nach Fertigstellung der VS-Unterlage sind alle Datenträger an die VS-Registratur zurückzuliefern.
Unbrauchbar gewordene Datenträger sind ebenfalls an die VS-Registratur zurückzugeben. Die Daten auf nicht mehr benötigten Datenträgern sind nach den entsprechenden BSI-Vorgaben **physikalisch** zu löschen.

Hierüber ist unter Hinzuziehung des SiBe / IT-VS-Beauftragten eine "VS-Vernichtungsverhandlung" zu erstellen.

4.2.2 Drucker- / Plotterausgaben

Alle Rechnerausgaben (z.B.:Drucker, Plotter) der Geheimhaltungsgrade VS-VERTRAULICH oder GEHEIM, die nicht Zwischenmaterial sind, müssen unverzüglich bei der VS-Registratur im VS-Tagebuch erfasst werden.
Druckvorlagen können bis zum Abschluss der redaktionellen Bearbeitung als VS-Zwischenmaterial behandelt werden.

4.3 Vervielfältigung / Sicherungskopien / Auszüge

Jede Kopie eines Datenträgers mit VS-Tagbuch-Nr. bedarf eines Vervielfältigungsauftrages (VS-Registratur). Offene oder VS-NfD-Auszüge der VS-Datenträger dürfen ohne besondere Genehmigung der VS-Registratur angefertigt werden.
VS-Vervielfältigungen sind schriftlich mit dem entsprechenden Formblatt zu beantragen. Solche Aufträge müssen über die VS-Registratur laufen. Mehrfache Ausfertigungen auf dem örtlichen (PC)-Drucker sind in Ausnahmefällen zulässig und vorher mit der VS-Registratur abzustimmen.

4.4 VS-Zwischenmaterial

Die Be- und Verarbeitung sowie die Speicherung von VS-Zwischenmaterial darf nur auf VS-Datenträgern erfolgen, die entsprechend Ziffer 4.2.1 als VS gekennzeichnet und durch die VS-Registratur erfasst sind. Anfallendes VS-Zwischenmaterial ist entsprechend der Anlage 3 zum GHB zu behandeln und bis zur Vernichtung durch die zuständige Stelle vorschriftsmäßig aufzubewahren.
Zum VS-Zwischenmaterial zählen u.a. Fehldrucke von Listen und Plotterausgaben, Farbband-kassetten (insbesondere Einwegfarbbänder) sowie evtl. Zwischenausgaben.

5. IT-VS-System

5.1 Installation / Wartung / Instandsetzung

Im Störungsfall ist umgehend der SiBe / IT-VS-Beauftragte zu informieren. Dieser veranlasst alle weiteren Maßnahmen.

Während des VS-Betriebs ist jede Form der Installation, Wartung und Instandhaltung durch Fremdfirmen untersagt. Es ist sicher zu stellen, dass Unbefugte keine Kenntnis von VS erhalten.

Für die Systemwartung gilt darüber hinaus, dass VS vor Aufnahme der Wartungsarbeiten aus dem IT-System zu entfernen sind.

Ist dies nicht möglich, ist entsprechend ermächtigtes Wartungs- oder Instandsetzungspersonal einzusetzen oder dieses durch geeignetes, ermächtigtes Fachpersonal zu beaufsichtigen.

Dem Wartungstechniker dürfen während seiner Tätigkeit keine VS zur Kenntnis gelangen. Über Art und Umfang der Arbeiten ist ein Protokoll zu führen.

Eine Auslagerung der VS-IT-Administration in verschiedenen nationalen und / oder internationalen VS-Projekten widerspricht im Kontext “Need to know“ bzw. “Weitergabe an Dritte“ den Regeln und dem Geist des Geheimschutzhandbuches (GHB). Die VS-IT-Administration gehört zu den Kernaufgaben, die ein geheimschutzbetreutes Unternehmen selbst und daher durch firmeneigenes Personal ausführen muss. Diese Aufgabe kann und darf nicht durch eine Fremd- / Tochterfirma ausgeführt werden.

5.2 Zugangs- / Zugriffskontrolle

Zugang-/Zugriff auf das IT-System darf nur durch Befugte, im Rahmen der erteilten Zugriffsrechte erfolgen. Dies ist durch ein geeignetes System oder durch Rollen- / Berechtigungskonzepte sicher zu stellen.

Bei der Vergabe, Änderung und Rücknahme von Rechten muss sicher gestellt sein, dass:

- der Antrag von einer berechtigten Person stammt (z.B. Projektleiter),
- die zu berechtigende Person ausreichend ermächtigt ist,
- der Grundsatz „Kenntnis nur wenn nötig“ beachtet wird und
- keine sicherheitsmäßig unvereinbare Bündelung von Funktionen besteht.

Die Zustimmung des IT-VS-Beauftragten / SiBe ist einzuholen

Die Vergabe, Änderung und Rücknahme von Rechten ist so zu dokumentieren, dass jederzeit nachvollzogen werden kann, wer wann in welchem Umfang berechtigt war.

5.3 Hardwarekonfiguration

Die Komponenten des IT-VS-Systems sind im Anhang 3 abschließend aufgelistet. Bei Veränderungen der Hardware ist der Anhang 3 anzupassen und dem BMWi umgehend zuzuleiten.

☐ Es handelt sich um ein „Stand-Alone-System“
☐ Es handelt sich um ein vernetztes System (siehe Anlage 6 – Netzbeschreibung, Netzwerkschema)

Netzwerk **innerhalb einer Sperrzone**
☐ Das System befindet sich innerhalb der Sperrzone X – eine kryptierte Übertragung ist nicht erforderlich.

*Wenn **nicht innerhalb einer Sperrzone jedoch innerhalb der Liegenschaft** dann sind:*

☐ die Übertragungseinrichtungen sind so geschützt, dass ein Zugriff Unbefugter unverzüglich erkannt und abgewehrt wird (Approved Circuits).

☐ die Übertragung erfolgt kryptiert.

☐ Aufgrund der Besonderheiten des Systems (z.B. Einsatz in mobiler Umgebung) wurden die folgenden Maßnahmen zum Schutz des Systems vereinbart:
(hier bitte eine detaillierte Beschreibung des Systems und der getroffenen Schutzmaßnahmen)

Sofern Hardwarekomponenten mit Festspeicher (z.B.: Multifunktionsdrucker, Plotter, usw.) betrieben werden, müssen diese in Sperrzonen aufgestellt werden. Die entsprechende HW-Komponente ist in der Hardwareliste aufzuführen.

☐ Eine Hardwarekomponenten mit Festspeicher wird innerhalb einer **Sperrzone** betrieben.
Eine genauer Hardwarebeschreibung findet sich im Anhang 3.

5.4 Versiegelung

Der SiBe / IT-VS-Beauftragte schützt die Systemeinheit mit Siegeln vor mechanischem Zugriff. Arbeitstäglich **muss** sich der jeweilige VS-Zugriffsberechtigte **vor dem Beginn der IT-VS-Bearbeitung** von der äußeren Unversehrtheit der Hardware überzeugen (Prüfen der Versiegelung auf Unversehrtheit).

Sofern die ITGA innerhalb einer Sperrzone betrieben wird, kann von einer Versiegelung abgesehen werden.

☐ Die Hardware befindet sich innerhalb einer Kontrollzone und ist versiegelt.

☐ Die Hardware befindet sich innerhalb einer Sperrzone, eine Versiegelung ist nicht erforderlich.

5.5 System-/Standardsoftware

Die Systemkonfiguration ist im Anhang 3 insbesondere in Bezug auf sicherheitsrelevante Aspekte zu beschreiben*. (Virenschutzsoftware, Verschlüsselungssoftware sind aufzulisten)*

☐ Einbringung von Software in das System wird zuvor über einen aktuellen VS - Virenschleusen-PC geprüft.

☐ Auf dem System befindet sich ständig aktuelle Virenschutzsoftware (siehe Anhang 3). Die Virenschutzsoftware wird _____ aktualisiert*.(Häufigkeit angeben !!!)*
Die Aktualisierung wird wie folgt durchgeführt: *(kurze Verfahrensbeschreibung !!!)*

Hinweis: bitte verwenden Sie zur Übertragung der aktuellen Virenpatterns ausschließlich nicht wiederbeschreibbare Datenträger (CD / DVD). Die Übertragung mittels USB-Sticks o.ä. ist im Kontext „need-to-know“ nicht zulässig.

5.6 Schutz gegen kompromittierende Abstrahlung

In diesem Kapitel sind Angaben zur kompromittierenden Abstrahlung gefordert. Es gibt dabei verschiedene Möglichkeiten (s.u.) die dafür in Betracht kommen. Wählen Sie die für Sie zutreffende Maßnahme aus.

☐ Maßnahmen zur Abstrahlsicherheit werden vom Auftraggeber nicht gefordert (siehe VS-Einstufungsliste, Ziffer 31). *(weiter ab Ziff. 5.7)*

☐ Schutzmaßnahmen sind zur Zeit erforderlich für:

- Rechner
- Monitor
- Tastatur
- Drucker
- Verbindungsleitungen
- Alle permanent speichernden Datenträger

☐ weitere Komponenten für die Schutzmaßnahmen erforderlich sind:
(Bitte ggf. hier auflisten)

Schutzmaßnahmen werden im Rahmen dieser ITGA erfüllt durch:

☐ Tempestierte Hardware nach SDIP 27 Level A

☐ DfmA: Vermessungsprotokoll vom: *(Datum angeben)*

☐ HF-Kabine gem. Vermessungsprotokoll vom: *(Datum angeben)*

☐ Zonenmodell:

Hinweis: Die Zonenfestlegung erfolgt durch das BSI nach erfolgter Vermessung / Beauftragung durch das BMWi.
Sämtliche Prüfberichte der im Anhang 3 aufgeführten Hardware sind mit dieser ITGA gemeinsam einzureichen. Es können nur ITGAen genehmigt werden, mit vollständig vorliegenden Prüfberichten.

Bitte beachten Sie, dass jedes IT-System inkl. **aller verwendeten Datenträger sowie der kompletten Peripherie** vermessen werden muss. Bei jeder Zulassung (Neuvermessung) seit dem 01.01.2014 ist eine sogenannte Konstruktionsstandsfestschreibung erforderlich, die Massenspeicher ungeachtet ihrer Form ausdrücklich einschließt.

- Vermessung und Zulassung für den Betrieb in der Zone X gem. Vermessungsprotokoll vom: (Datum angeben)

☐ es wurden weitergehende Überwachungsmaßnahmen vereinbart. Dies sind im einzelnen:
Beschreiben Sie hier die vereinbarten, weitere Überwachungsmaßnahmen. (z.B. Auflagen des BSI) Wie werden die Vereinbarungen umgesetzt?

5.7 Konfigurationsänderung / Nutzungsänderung

Jede geplante Änderung der Hardware- und System-Standardsoftware-Konfiguration, hierzu gehören auch Versionswechsel und die Einrichtung von neuen oder zusätzlichen Netzanschlüssen, muss neben dem zuständigen PC-Verantwortlichen/Systemverantwortlichen auch dem SiBe/IT-VS-Beauftragten durch den Projektleiter mitgeteilt werden. Der SiBe / IT-VS-Beauftragte muss vor der Beschaffung / Realisierung die Genehmigung des BMWi einholen. Damit können Änderungsauflagen verbunden sein. Der Anhang 3 muss deshalb regelmäßig, bei wesentlichen Veränderungen (z.B. räumlichen Änderungen, zusätzlicher neuer Hardware und Software) **sofort**, den tatsächlichen Verhältnissen angepasst werden.
Unterbleibt die vorherige Unterrichtung, so erlischt die für diese Anweisung erteilte Genehmigung.

5.8 VS-Datenfernübertragung (DFÜ) / Vernetzung

Während der VS-Bearbeitung darf das IT-VS-System an **kein** lokales oder betriebsinternes (offenes) LAN oder externes Datennetz (WAN) angeschlossen sein. Ebenso darf keine Fernwartung stattfinden (s.a. Pkt. 5.1).
Eine Wireless LAN Funktionalität (hier stellvertretend für alle möglichen Funkvernetzungen), ist nicht zulässig. Entsprechende Komponenten sind zu deaktivieren.

Die Nichtbeachtung dieser Vorschriften stellt einen schweren Sicherheitsverstoß dar, der zum Entzug der Zugriffsberechtigung führen kann, sowie ggf. strafrechtlich geahndet werden kann.

Für eine Anbindung an ein weiteres VS-Netz sind besondere Anforderungen zu erbringen und es Bedarf einer ausdrücklichen Genehmigung durch BMWi. Es sind BSI zugelassene Kryptosysteme – entsprechend dem Geheimhaltungsgrad dieser ITGA - für die Datenübermittlung einzusetzen.

☐ die kryptierte Anbindung an ein weiteres VS-Netz wird mit dieser ITGA beschrieben. Ein Netzwerkplan findet sich in der Anlage, die entsprechende Kryptobox ist in der Hardwareliste aufgeführt.

Beschreiben Sie hier bitte kurz den Aufbau des Netzes und gehen sie insbesondere auch darauf ein ob. eine Anbindung an ein weiteres Netz über eine „Drehstuhlschnittstelle" oder ein „Rot-Schwarz-Gateway" existiert.
Vergessen Sie dabei nicht, ggf. eine Virenschleuse einzusetzen und beschreiben Sie das Verfahren mit seinen Abläufen..

6. Schutz der IT-VS-Daten

6.1 Sicherung der IT-VS-Betriebsstelle

Bei der IT-VS-Bearbeitung, solange sich VS im System befindet, muss der jeweilige Zugriffsberechtigte in eigener Verantwortung den persönlichen Gewahrsam über die dort befindlichen VS halten oder die ständige Besetzung der IT-VS-Betriebsstelle durch andere VS-Ermächtigte, die z.B. am gleichen Projekt arbeiten, nach dem Grundsatz **"Kenntnis, nur wenn nötig"** sicherstellen.

Um die IT-VS-Anlage vor unbefugtem Zugriff und Manipulation zu schützen, befindet sich die IT-VS-Betriebsstelle in einer VS-Kontroll- bzw. VS-Sperrzone. Die Handhabung wird in der entsprechenden Kontroll- bzw. Sperrzonenanweisung beschrieben.
Befinden sich mehrere IT-VS-Anlagen im gleichen Raum, auf denen unterschiedliche Projekte bearbeitet werden, ist der Sichtschutz gemäß des Grundsatzes **"Kenntnis, nur wenn nötig"** durch zusätzliche Maßnahmen zu realisieren. *(individuelle Maßnahmen erläutern, z.B. Einsatz von Stellwänden, zeitlich versetztes arbeiten)*
Die Bildschirme sind so aufzustellen, dass sie von Außen nicht einsehbar sind. Ggf. sind während des Betriebes die Fenster durch geeignete Maßnahmen (Vorhänge, Jalousien) blickdicht zu machen.

Zur Einhaltung des Grundsatzes *"***Kenntnis, nur wenn nötig"** ist es erforderlich, den Bildschirm dunkel zu schalten oder abzudecken, wenn sich Unbefugte im Raum aufhalten. Ist die ständige Besetzung nicht zu realisieren, so sind die VS- sowie alle IT-VS-Datenträger in einem zugelassenen VS-Verwahrgelass zu deponieren.

6.2 Datenhaltung

Die Datenhaltung hat grundsätzlich **nur auf auswechselbaren** VS-Datenträgern (Wechselfestplatten, Flash-Speicher, Disketten, Tapes, CD-ROM etc.) oder auf VS-Notebooks zu erfolgen. Auf einem Datenträger darf nur ein VS-Projekt gespeichert werden (Einhaltung des „Need to Know"). Die Wechselfestplatten / Notebooks sind so einzustufen, wie der höchste VS-Einstufungsgrad der darin enthaltenen Verschlusssache. Sie sind mit einer entsprechenden VS-Tagebuch-Nr. zu versehen. Bei dem Einsatz in einer Kontrollzone, sind die VS-Datenträger oder das VS-Notebook nach Arbeitsende im zugelassenen VS-Verwahrgelass zu hinterlegen.

6.3 Datensicherung und Wiederanlauf

Im Rahmen der Datensicherung erstellte VS-Daten (einschließlich VS-eingestufter Programme) sind gemäß den VS-Vorschriften zu behandeln. Die Speichermedien sind entsprechend des höchsten Geheimhaltungsgrades im Tagebuch zu erfassen und zu kennzeichnen.
Im übrigen gelten die Regeln analog Ziff.4.2 der ITGA.
Bei den erforderliche Maßnahmen zum Wiederanlauf sind die Erfordernisse des Geheimschutzes zu berücksichtigen.

6.4 Passwort.

Bei Beginn der VS-Bearbeitung muss ein Passwort nach folgenden Regeln vergeben werden:

- Die Zeitdauer bis zum erzwungenen Wechsel der Passworte darf 3 Monate nicht überschreiten.
- Die Länge des Passwortes muss mindestens zehn Zeichen betragen.
- Trivialpassworte oder persönliche Daten dürfen nicht benutzt werden.
- Das Passwort soll auch Sonderzeichen enthalten.
- Im BIOS implementiert (falls keine Softwareentwicklung betrieben werden muss).
- Bildschirmschoner Passwort muss aktiviert sein.

Weiterhin dürfen **maximal drei Login-Fehlversuche** zugelassen werden.

Nach dem dritten Fehlversuch ist die User-ID zu sperren. Eine erneute Freigabe darf erst nach Klärung des Sachverhaltes durch den SiBe / IT-VS-Beauftragten erfolgen.

6.5 Pausenregelung

Bei Arbeitsunterbrechungen von maximal 30 Minuten dürfen die Wechselfestplatte in dem IT-System innerhalb der **ständig aktivierten und technisch überwachten Kontrollzone** verbleiben, wenn die VS-Einstufung VS-VERTRAULICH nicht übersteigt. Der Bildschirm ist zu sperren, die Sperre darf nur mittels Passwort aufzuheben sein. Beim Verlassen des Raumes durch den letzten Mitarbeiter ist die Gefahrenmeldeanlage (GMA) scharf zu schalten.
VS der Einstufung **GEHEIM müssen** in das Verwahrgelass verbracht werden.

6.6 Tägliche Beendigung der IT-VS-Bearbeitung

Nach der Beendigung der IT-VS-Bearbeitung bzw. bei Arbeitsende sind vom VS-Zugriffsberechtigten die folgenden Sicherheitsmaßnahmen durchzuführen:

- Die internen Speicher (Arbeits-/Hauptspeicher), die beim Ausschalten nicht automatisch gelöscht werden (ohne Spannung), sind gezielt zu löschen oder zu überschreiben.
- Ausgabegeräte (Drucker / Plotter) sind auszuschalten bzw. ihre flüchtigen Speicher zu leeren / zu löschen, eventuell vorhandene Einwegfarbbänder sind zu entnehmen.
  Drucker mit einem internen Speicher sind nur innerhalb einer Sperrzone zu betreiben.
- Alle auswechselbaren VS-Datenträger (USB-Festplatten, Wechselfestplatten, Disketten, Tapes, CD-ROM, Flash-Speicher usw.) oder Notebooks und andere im Raum befindliche VS müssen vorschriftsmäßig in einem zugelassenem und genehmigten VS- Behältnis aufbewahrt werden.
- Die IT-VS-Anlage ist abzuschalten und abzuschließen.
- Die Kontroll- oder Sperrzonenanweisung ist strikt einzuhalten.

7. Anwendersoftware

Wird vom Zugriffsberechtigten im Zusammenhang mit dem VS-Auftrag auf dem IT-VS-System Software erstellt, geändert oder ergänzt, ist diese so zu dokumentieren, dass ein fachkundiger Dritter in der Lage ist, den Inhalt nachzuvollziehen und alle VS-relevanten Maßnahmen zu überprüfen.
Beinhaltet die Anwendersoftware nach der VS-Einstufungsliste des Auftrages eingestufte Informationen, so ist sie entsprechend einzustufen.

Die Unversehrtheit **der installierten, nicht handelsüblichen Software** ist regelmäßig zu überprüfen. Die Überprüfung (z.B. Checksummenverfahren) muss protokolliert werden.

Vom Auftraggeber beigestellte oder vorgeschriebene Software muss im vorgegebenen Zustand eingesetzt werden.

8. Protokollierung

Bitte löschen Sie die nicht zum verwendete Variante (i.d.R. die Variante 2!!) sowie die nicht in Anspruch genommene Möglichkeit (i.d.R. Möglichkeit 1!!!)

Variante1 (automatische Protokollierung – Regelfall !!)
Bei Betriebssystemen mit Rechnerprotokolliermöglichkeit **ist diese zu nutzen**.
Die Protokollierung soll, folgende Angaben enthalten:

- Beginn der VS-Bearbeitung
- Ende der VS-Bearbeitung
- Name des berechtigten Benutzers
- Angaben zu erstellten Ausdrucken / Datenträgern
- Angaben zu übermittelten VS
- auf welche Dateien wurde zugegriffen
- unberechtigte Login Versuche

- Abgewiesene Zugriffsversuche werden ebenfalls protokolliert
  Sie werden vom IT-System:
  - ☐ unmittelbar dem IT-VS-Beauftragten angezeigt
  - ☐ revisionssicher protokolliert.

Variante2 (manuelle Erfassung – N U R sofern eine Rechnerprotokollierung nicht möglich ist !!)
Da der Nachweis der reinen IT-VS-Bearbeitung nicht automatisch erfasst wird, muss für jedes IT-VS-System eine manuelle Erfassung dieser Zeiten im Betriebsbuch erfolgen.
Die Protokolle müssen folgende Daten beinhalten:

- Beginn der VS-Bearbeitung
- Ende der VS-Bearbeitung
- Name des berechtigten Benutzers
- Angaben zu erstellten Ausdrucken / Datenträgern wie folgt:
- zu Ausdrucken von VS mit Angabe der VS-Tagebuchnummer
- zu Ausdrucken von VS-Zwischenmaterial mit Angabe der Nr. des Quittungsbuches für VS-Zwischenmaterial
- zum Abspeichern von VS-Dateien auf VS-Datenträgern mit Angabe der VS-Tagebuchnummer
- Angaben zu übermittelten VS
- auf welche Datei bzw. auf welches Projekt wurde zugegriffen

Der folgende Absatz gilt bei beiden Varianten !
Es soll möglich sein, sicherheitserhebliche Ereignisse bezogen auf einzelne Benutzer, Benutzergruppen und zugriffsgeschützte Objekte zuverlässig und nachvollziehbar aufzubereiten. Zweck der Dokumentation ist es, auch zu einem späteren Zeitpunkt bekannt werdende Sicherheitsvorkommnisse in der Vergangenheit lückenlos nachverfolgen zu können. Dazu sind unterschiedliche Dokumentationen zu erstellen, die einer längeren Aufbewahrungsfrist unterliegen.

9. Aufbewahrungsfristen

Für die Aufbewahrung der Dokumentation gelten folgende Fristen:

GHB Anlage 37	Art der Doku	Inhalt	Kapitel	Aufbewahrungsfrist
§ 23	Geheimschutz-dokumentation	ITGA,Freigabebestätigung, zugrunde liegende Prüfergebnisse (Zonen- / Abstrahlmessungen)	5.6	5 Jahre **nach** Abmeldung der ITGA
§ 22	SiVoKo	Sicherheitsvorkommnis		
§ 7(3)	Zugangs- / Zugriffskontrolle	Wer, Wann zur Vergabe / Änderung / Rücknahme berechtigt war („Rechteverteiler“) Wer, Welche Rechte, Wann ausüben konnte („Rechteinhaber“)	5.2	
§ 8	Rechnerprotokollierung	Systemlogdateien oder Bericht nach Möglichkeit 1	8	
§ 10	Anwendersoftware nicht handelsübliche Software Vom Auftraggeber beigestellte oder vorgeschriebene Software	Was wurde wann verändert? Überprüfung des Zustandes wird die Software im vorgegebenen Zustand eingesetzt?	7	
§ 11	Instandsetzungs- / Wartungsprotkolle	Art und Umfang der Arbeiten	5.1	
§ 8	Bericht des Systemverantwortlichen	Halbjährliche Kontrolle des VS IT-Systems auf Unversehrtheit. Techn. Prüfung des Systems	8	

Hinsichtlich der Dokumentation über die einzelnen Datenzugriffe (Rechnerprotokollierung oder manuelle Erfassung) gibt es im Rahmen der Beweissicherung zwei Möglichkeiten:

☐ 1.Möglichkeit:

Vor Löschung der Systemlogdateien durch den IT-VS-Beauftragten ist ein **aussagekräftiger** Bericht über die durchgeführten Kontrollen zu fertigen Dieser ist erforderlich um auch später aufkommende, sicherheitsrelevante Manipulationen verfolgen und aufklären zu können.
Aus dem Bericht **muss** mindestens hervorgehen

- Anzahl der abgewiesenen Zugriffe.
- Welche Benutzer wurden wann vom System abgewiesen und warum.
- Welche Benutzer wurden mehrfach / wiederholt vom System abgewiesen.
- Anzahl der berechtigten Zugriffe in dem beobachteten Zeitraum.
- Sind Zugriffe zu außergewöhnlichen Zeiten erfolgt (Wochenende, Nacht) durch welche Benutzer und wie oft.
- Auf welche Dateien wurde in diesen Fällen (außergewöhnlichen Zeiten) zugegriffen.
- Wurden Ausdrucke erstellt, welche Dateien, wann und durch welchen Benutzer.
- Wurden Kopien auf Datenträgern erstellt, welche Dateien, wann und durch welchen Benutzer.
- Wurden Daten übermittelt, welche Dateien, wann und durch welchen Benutzer und wohin.

☐ 2.Möglichkeit:

Die Systemlogdateien / die Protokollierungsunterlagen werden 5 Jahre aufbewahrt (z.B.: auf Datenträger), dann ist ein kurzer Bericht des IT-VS-Beauftragten / SiBe ausreichend der die regelmäßige Kontrolle bestätigt.

10. Kontrollen und Technische Prüfungen

Durch den SiBe/IT-VS-Beauftragten sind folgende Prüfungen durchzuführen

Kontrollen des IT-Systems

- ob Komponenten sicherheitsgerecht eingesetzt, gewartet und Instand gesetzt werden
- Zugriffsrechte erforderlich und korrekt zugewiesen sind
- Mittel zur Identifizierung / Authentifizierung korrekt aufbewahrt werden

Technische Prüfungen

- sind IT-Sicherheitsfunktionen richtig implementiert
- sind Manipulationen am IT-System erkennbar
- ist die Versiegelung an Geräten in Kontrollzonen in Ordnung
- gibt es Anhaltspunkte für techn. Mängel des Abstrahlschutzes

In diesem Zusammenhang ist vom System-Verantwortlichen halbjährlich jeweils zum 31.03 und 30.09.des Jahres ein schriftlicher Bericht zu erstellen, in dem

- die Unversehrtheit des Systems,
- sonstige Vorkommnisse und
- der Nachweis der VS- Bearbeitungszeiten auf dem IT-System

aufgeführt werden. Der Bericht ist an den SiBe/IT-VS-Beauftragten zu senden.

Die Nachweise über die IT-VS-Aktivitäten müssen im Rahmen einer Kontrolle auf Unregelmäßigkeiten vom System-Verantwortlichen regelmäßig ausgewertet werden.

In unregelmäßigen Abständen ist der Nachweis durch den SiBe / IT-VS-Beauftragten zu kontrollieren. Bei festgestellten Auffälligkeiten ist das BMWi unverzüglich zu informieren.

11. Beendigung der IT-VS-Bearbeitung

Die Beendigung der IT-VS-Bearbeitung im Geltungsbereich dieser Anweisung ist dem SiBe / IT-VS-Beauftragten anzuzeigen. Dabei ist mitzuteilen, ob weitere IT-VS-Bearbeitungen für andere VS-Aufträge konkret erwartet werden. Wenn keine weitere IT-VS-Bearbeitung durchgeführt werden soll, ist die ITGA dem BMWi gegenüber abzumelden.

12. Zur besonderen Beachtung!

Änderungen bedürfen der Benachrichtigung des SiBe / IT-VS-Beauftragten. Jede VS-Wechselfestplatte / Notebook ist einem Mitarbeiter bzw. einer / Gruppe / einem Projekt zugeordnet. Bei IT-VS-Bearbeitung dürfen sich nur VS-Datenträger im System befinden.

*!! Ab hier -- Raum für Besonderheiten des Einzelfalls. -- im folgenden **3 Beispiele** !!*

*Für den Fall, dass ein **Drucker innerhalb** einer **Kontrollzone** betrieben wird:*
Der in der Kontrollzone betriebene Drucker verfügt nicht über einen Festspeicher. Ein entsprechender Hinweis findet sich im Anhang 3 (Hardwareliste)

*Für den Fall das es sich bei der genutzten HW um ein Notebook handelt, **sonst** bitte aus der ITGA **entfernen**:*
Während des Transportes zur und von der Kontrollzone müssen sich die VS-NfD eingestuften Datenträger (Wechselfestplatten, bzw. die Laptops) im ständigen persönlichen Gewahrsam von berechtigten Mitarbeitern befinden. Die Festplatten von mobilen Geräten (z.B. Notebooks), die das Unternehmen verlassen, sind mit einer vom BSI zugelassenen Software zu verschlüsseln.
Dies ist durch den Systemverantwortlichen sicherzustellen.

Anhang 1 – Angaben zur IT-VS-Betriebsstelle

Angaben zur IT-VS-Betriebsstelle

Standort (Gebäude-/Raumnummer):
Nummer der Kontroll-/Sperrzone:

(Lageplan der IT-VS-Betriebsstelle)

Anhang 2 - Personelle Zuständigkeiten

Sicherheitsbevollmächtigter(SiBe)	Hr./Fr.
Ständiger Vertreter des Sicherheitsbevollmächtigten vor Ort	Hr./Fr.
IT-VS-Beauftragter	Hr./Fr.
Daten-VS-Verwalter	Hr./Fr.
Vertreter	Hr./Fr.
Projektleiter	Hr./Fr.
Systemverantwortlicher	Hr./Fr.
Systemadministrator	Hr./Fr.

VS-Zugriffsberechtigte			
Name	**Vorname**	**Abteilung**	**Anmerkung**

Anhang 3 – Geräte- und Softwarekonfiguration (Beispieldaten)

Gerätekonfiguration

Pos	Anz	Bezeichnung	Typ	Rechner am Netz	Bemerkungen (TgBNr.)	Kontroll-/Sperrzone
1.	6	PC MTOS/PACTOS	AMD 64 X2, 2GB	ja	**2021-01**	
2.	6	Wechselfestplatte	320GB Samsung HD320KJ		**2021-02**	
3.	6	DVD-R, CD-RW Laufwerk	TSST SH-D162D			
4.	6	Farbmonitor	Benq FP222WH			
5.	0	Disketten Laufwerk	nein			
6.	0	Drucker	nein			
7.	10	Laptop MTOS/PACTOS	DELL Latitude D830, 2GB	Ja		
8.	10	Festplatte	120GB Toshiba MK1237 GSX		**)**	
9.	10	DVD-R, CD-RW	TSST TS2462D			
10.	0	Disketten Laufwerk	nein			
11.	1	Drucker	HP XYZ23	Ja	**Enthält keinen Festspeicher**	**KZ 2**

Softwarekonfiguration

Pos.	Bezeichnung	Version	Hersteller
1.	Betriebssystem	Windows 7 64bit	Microsoft
2.	Software	OfficeProf SP2	Microsoft
3.	Firewall	Produkt bitte angeben	
4.	Kryptosoftware	Produkt bitte angeben	
5.	Virenscanner	Produkt bitte angeben	

Anhang 4 - Netzwerkschema „xyz“