Ausfüllhilfe für die ITGA

Vorbemerkung:
Diese Ausfüllhilfe soll eine Hilfestellung bieten. Sie soll Sie in die Lage versetzen, die ITGA für Ihr IT-System mit Hilfe der ITGA-Vorlage zu erstellen. Die ITGA-Vorlage enthält alle geforderten Maßnahmen nach den Anlagen 37 und 69 des Geheimschutzhandbuches. Bei der Vielzahl der verwendeten IT-Systemen auf denen eingestufte Daten bearbeitet werden, ist die ITGA immer auf die individuellen Verhältnisse des IT-Systems und des Unternehmens anzupassen.

!! Beim Erstellen der ITGA nutzen Sie bitte für nicht benötigte Passagen die Funktion „Durchstreichen“ und kommentieren darunter, weshalb diese nicht zutreffen. Im Falle das Felder der ITGA durch Ankreuzen auszufüllen sind, ist dies nicht erforderlich. Kursiv geschriebene Texte sind vor Abgabe der ITGA zu löschen!!

Grundsätzliches:
Eine IT-Geheimschutzanweisung (ITGA) regelt die Einzelheiten des Betriebsablaufs für ein beschriebenes IT-System bei nationalen Projekten. Sie beschreibt die erforderlichen Maßnahmen zum Schutz von VS beim Einsatz von Informationstechnik (IT).
Bei internationalen Projekten sind zusätzlich die auf zwischenstaatlicher Ebene vereinbarten Regelungen zu beachten.

Deckblatt:
Auf dem Deckblatt tragen Sie bitte zunächst die Firmennummer ein, unter der Sie beim BMWi geführt werden sowie unter VS-Auftragnehmer Ihren Firmennamen. Darunter bitte die Firmenadresse und die Abteilung eintragen, unter der Sie als Sicherheitsbevollmächtigter (SiBe) im Unternehmen geführt werden.
Das ***Ausgabedatum*** ist das Datum an dem Sie die ITGA zur Genehmigung vorlegen. Für spätere Änderungen gibt es das ***Änderungsdatum***. Hier ist das jeweils aktuelle Datum der letzten Änderung einzutragen.

Den ***Titel des VS-Auftrages***, ***Auftragsnummer*** und ***VS-Einstufung*** entnehmen Sie bitte der VS-Einstufungsliste.

Unter ***IT-System*** führen Sie die Gesamtzahl der Hardware an. Also z.B.: 1 VS-Laptop oder 4 VS-PC und 3 Server oder 6 ThinClient und 1 Server und 2 Drucker

Bei dem Punkt ***Kompr.Abstr***. geben Sie bitte an, was Sie gemäß Punkt 31 der VS-Einstufungsliste erfüllen müssen.

Falls Abstrahlschutz gefordert wird, wählen Sie durch ankreuzen aus, wie dieser umgesetzt wird.

Angaben zum Punkt ***Standorte*** sind die entsprechenden, genehmigten Kontroll-/Sperrzonen in denen die Bearbeitung stattfindet, also in denen das IT-System steht. Neben der Kontroll-/Sperrzonennummer geben Sie bitte noch Gebäude- und Raumnummern an, sofern vorhanden.

Vor dem Einreichen der ITGA ist diese vom SiBe und dem systemverantwortlichen Mitarbeiter zu unterschreiben.

Ziff 1. Geltungsbereich:
Eine ITGA ist immer zu erstellen, wenn Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH oder GEHEIM auf IT-Systemen bearbeitet werden. Zur Bearbeitung gehören Lesen, Bearbeiten, Drucken, Speichern von eingestuften Daten.
Eine ITGA ist *vor Aufnahme der Bearbeitung* beim BMWK zu beantragen.

Achtung:
Dies kann z.B. bereits das Lesen von eingestuften Daten auf einer CD im Rahmen einer Angebotsabgabe sein!

Für Verschlusssachen des Geheimhaltungsgrades
VS-NUR FÜR DEN DIENSTGEBRAUCH gelten die Regelungen der Anlage 4 zum GHB (VS-NfD Merkblatt)

Ziff 2. IT-VS-Betriebsstelle:
Dabei handelt es sich um den Raum oder die Räume in denen das IT-System steht. Geben Sie hier bitte noch einmal die ***genehmigten Kontroll-/Sperrzonen*** an, in denen eine Bearbeitung stattfindet.
Bei einem räumlichen Umzug der ITGA ist diese Ziffer natürlich entsprechend anzupassen.

Ziff 3. Personelle Zuständigkeiten / Projekte und Aufträge
Der ***Personenkreis*** sollte unter Berücksichtigung des „Need to know“ so klein wie möglich gehalten werden. Alle Personen die im Rahmen der ITGA Zugang zu VS haben, müssen entsprechend dem Geheimhaltungsgrad ermächtigt sein.
Alle Personen sind abschließend im ***Anhang 2*** aufzulisten.

Alle ***VS-Projekte*** die mit der ITGA bearbeitet werden sind aufzulisten. Sie können dies entweder auf dem Deckblatt machen oder Sie fügen einen entsprechenden Anhang bei. Bitte beachten Sie das bei der Bearbeitung mehrerer Projekte das „Need to know“ unbedingt gewährleistet sein muss. Dies kann beispielsweise durch unterschiedliche Datenspeicher (z.B. verschiedene Wechselfestplatten) realisiert werden.
- Wollen Sie mehrere Projekte mit dem IT-System bearbeiten, nehmen Sie bitte zuvor Kontakt mit Ihrer VS-IT-Berater*in auf!

Ziff 5.3 Hardwarekonfiguration
Bei der ersten Auswahl legen Sie fest, ob es sich um ein Stand-Alone-System oder ein vernetztes System handelt.
Ein „***Stand-Alone-System“*** meint entweder einen einzelnen PC oder auch ein einzelnes Laptop.
- Bitte ändern Sie das Muster entsprechend um, wenn es sich um einen Laptop handelt.

Ein ***Netzwerk innerhalb einer Sperrzone*** liegt dann vor, wenn alle Hardwarekomponenten eines vernetzten Systems innerhalb einer genehmigten Sperrzone liegen. Eine genehmigte Sperrzone kann dabei durchaus aus mehreren Räumen bestehen.
Entscheidend ist hier die von Ihrem Firmenberater zuvor genehmigte Sperrzone!

Sobald sich das ***Netz nicht*** mehr ***innerhalb einer Sperrzone*** befindet, sind hier verschiedene Fälle denkbar.
Im ersten Fall befindet sich das „rote VS-Netz“ innerhalb einer Liegenschaft aber beispielsweise in verschiedenen Räumen oder Etagen. Hier sind die verschiedenen

Sperrzonen unterbrochen. In diesem Fall muss eine Übertragung entweder kryptiert (mit einem BSI zugelassenem Produkt) erfolgen oder die Übertragungseinrichtungen müssen entsprechend geschützt sein.

t In solchen Fällen nehmen Sie bitte Kontakt mit Ihrer zuständigen VS-IT-Beraterin auf.

Im zweiten denkbaren Fall ist das „rote VS-Netz“ an ein anderes Netz, beispielsweise an einem anderen Standort angeschlossen. Hierbei ist ausschließlich eine kryptierte Übertragung mit einem BSI zugelassenem Produkt möglich.

t In solchen Fällen nehmen Sie bitte Kontakt mit Ihrer zuständigen VS-IT-Beraterin auf.

Sofern Sie in Ihrem Netzwerk einen sog. ***Multifunktionsdrucker / VS-Netzwerkdrucker*** mit Festspeicher betreiben, darf dieser nur innerhalb einer

 Sperrzone betrieben werden. Ein Betrieb innerhalb einer Kontrollzone ist grundsätzlich nicht zulässig.

 Sollten Sie keinen solchen Drucker betreiben, streichenSie bitte diesen Absatz aus dem Muster.

Ziff 5.4 Versiegelung

Verbleibt ***Hardware in einer Kontrollzone***, ist die Hardware zu versiegeln. Dies ist z.B. der Fall, wenn ein Desktop-PC mit einer Wechselfestplatte betrieben wird. In diesem Fall muss die Wechselfestplatte in das zugelassene VS-Verwahrgelass (Kategorie B3) gebracht werden, das Gehäuse sowie Maus und Monitor sind mit Siegelmarken (mind. Sicherheitsstufe 1) zu versehen. Damit wird sichergestellt, dass das Einbringen von unerlaubter „Schadhardware“ nicht möglich ist.
Vor jeder Bearbeitung muss die Versiegelung auf mögliche Öffnungsversuche hin überprüft werden.

Achtung: ***Sicherheitsetiketten sind nicht über das BSI zu beziehen!!!***

Sicherheitsetiketten sollen:

- bei Ablöseversuchen zerstört werden oder zumindest nicht ohne offensichtliche Spuren am Etikett vom zu sichernden Objekt abgelöst und wieder aufgeklebt werden können (Manipulationssicherheit) und
- Sicherheitsmerkmale besitzen, die nicht mit einfachen Mitteln (z.B. Farbkopierer) gefälscht werden können (Fälschungssicherheit).

Ziff 5.5 System-/Standardsoftware

Auf dem IT-System installierte System und Standardsoftware ist im ***Anhang 3*** aufzulisten. Dabei sind mindestens anzugeben:

- Betriebssystem
- Virenschutzsoftware
- Verschlüsselungssoftware (sofern vorhanden)
- Anwendungssoftware

Wie realisieren Sie den geforderten ***Virenschutz***? Haben Sie die Virenschutzsoftware auf dem VS-PC oder arbeiten Sie mit einem Virenschleusen-PC oder praktizieren Sie noch eine weitere Lösung?
Wie häufig aktualisieren Sie den Virenschutz?
Wie läuft das Verfahren der Aktualisierung?
Erläutern Sie den Ablauf des Aktualisierungsverfahrens.

Ziff 5.6 Schutz gegen kompromittierende Abstrahlung
Hier ist Ihre ***VS-Einstufungsliste***, Ziffer 31 maßgeblich.

Ist dort ein „Nein“ angekreuzt, können Sie alles Weitere unter dieser Ziffer durchstreichen.

Nur wenn in der VS-Einstufungsliste ***Maßnahmen zum Abstrahlschutz*** gefordert werden, dann kommt es darauf an, wie Sie diese Maßnahmen erfüllen.

- Wenn Sie eine Bearbeitung nach dem ***Zonenmodell*** realisieren wollen, dann wenden Sie sich zwecks weiterer Maßnahmen an Ihre zuständige VS-IT-Berater*in.

Ziff 5.8 VS-Datenfernübertragung / Vernetzung
Eine VS-Bearbeitung auf IT-Systemen hat grundsätzlich nur auf Stand-Alone-Systemen zu erfolgen.
Unter bestimmten Voraussetzungen kann eine ***VS-Datenfernübertragung*** erforderlich sein. Ebenso kann eine Bearbeitung in einem reinen ***VS-Netz*** erfolgen.
In diesen Fällen ist hier eine detaillierte Beschreibung einzufügen.

Einzelheiten hierzu klären Sie bitte mit Ihrer zuständigen VS-IT-Berater*in.

Ziff 8. Protokollierung / Nachweis über IT-VS-Bearbeitung
Sofern die Möglichkeit einer ***automatischen Protokollierung*** besteht, ist diese zu nutzen.
Davon ist bei heutigen Betriebssystemen i.d.R. auszugehen. Dabei können die betriebssystemabhängigen Protokollierungstools/Systemlogtools genutzt werden.
Darüber hinaus ist der Einsatz von entsprechenden Log-/Protokollierungstools, die die geforderten Daten protokollieren, angeraten.
Ein wesentlicher Aspekt zur Sicherung des IT-Systems sind hier auch sog. Intrusion-Detection oder Data-Loss-Prevention Systeme.

Die Wahl dieser Tools steht Ihnen frei. Sie sind hierbei nicht an BSI-zugelassene Produkte gebunden.
Entscheidend ist, dass die unter Ziff.8, Variante1 geforderten Angaben protokolliert werden.
Es muss nachvollziehbar protokolliert sein:

- **Wer** hat **wann**, **was** mit der eingestuften Datei gemacht?
- **Wer** hat **wann** versucht sich **unberechtigt anzumelden** und wurde abgewiesen?

Abgewiesene Zugriffsversuche **sind zu protokollieren**.

Die ***manuelle Protokollierung*** kommt nur dann in Betracht, wenn aufgrund der Eigenheit des IT-Systems eine automatische Protokollierung nicht möglich ist.
Sie stellt die absolute Ausnahme dar.

Die Logdateien sind aufzubewahren (2.Möglichkeit). Die Aufbewahrungsfrist beträgt 5 Jahre.
Entscheiden Sie sich für die 1.Möglichkeit der Ziff 8. ist ein entsprechender Bericht zu fertigen und vorzuhalten. Auf Anforderung ist dieser dem BMWK zu übersenden.

Bitte streichenSie die von Ihnen nicht genutzte Variante und Möglichkeit in der Ziff 8.