

Geheimhaltungsvorschrift



WIEN, 14. April 2011

Genehmigung und Herausgabe

Geheimhaltungsvorschrift

Die Geheimhaltungsvorschrift tritt mit **T.: 1. Jänner 2012** in Kraft.

**Gleichzeitig wird die „Verschlusssachenvorschrift (VSaV)“,
VersNr. 7610-01040-0191, außer Kraft gesetzt.**

Weiters werden außer Kraft gesetzt, die Erlässe vom:

- 5. November 1996 GZ 10.792/7-1.1/96,
- 16. Jänner 1997 GZ 10.792/11-1.1/96,
- 11. April 1997 GZ 10.792/4-1.1/97,
- 11. November 1998 GZ 10.792/7-1.1/98,
- 23. Jänner 2002 GZ 10.792/1-PräsA/2002.

Genehmigt:

WIEN, 14. April 2011

Für den Bundesminister:

KEMPERLE

VORWORT

Die Geheimschutzvorschrift (GehSV) **bezweckt** die Sicherstellung der Amtsverschwiegenheit, des Datenschutzes, des Schutzes von Staatsgeheimnissen und militärischen Geheimnissen sowie die Umsetzung der völkerrechtlichen/internationalen Verpflichtungen Österreichs zur sicheren Verwendung von klassifizierten Informationen im Ressortbereich des Bundesministeriums für Landesverteidigung und Sport (BMLVS).

Sie **beschreibt** den Vorgang der Klassifizierung von Informationen und definiert die einzelnen Klassifizierungsstufen, enthält die Aufgaben und den Verantwortungsbereich des Informationssicherheitspersonals und regelt den Umgang mit klassifizierten Informationen, sowohl für den nationalen als auch den internationalen Bereich.

Problemstellungen, fachliche Unklarheiten sowie unregelmäßige Tätigkeiten oder Maßnahmen, die aufgrund des(r) praktischen Einsatzes/Ausbildung mit der Geheimschutzvorschrift auftreten, sind

- je nach **Dringlichkeit** bzw. **Wichtigkeit der Klärung** **sofort schriftlich auf dem Dienstweg an BMLVS/Präs** heranzutragen,
- zu dokumentieren **und zusätzlich** in Form eines **Erfahrungsberichtes** bis

T.: 31. Dezember 2012

auf dem Dienstweg an BMLVS/Präs vorzulegen.

Mit Vorliegen der Erfahrungsberichte wird die ggstdl. Ausgabe evaluiert und allfällige Änderungen im Einvernehmen mit Präs und AbwA festgelegt.

Sprachliche Gleichbehandlung

Die in dieser Dienstvorschrift verwendeten personenbezogenen Ausdrücke betreffen – soweit dies inhaltlich in Betracht kommt – Frauen und Männer gleichermaßen.

ZUORDNUNG

Eine Zuordnung im herkömmlichen Sinn ist durch die digitale Bereitstellung mit Druckberechtigung nicht erforderlich.

Die Verteilung innerhalb der Kommanden (ab Einheitsebene einschließlich) und Dienststellen obliegt den jeweiligen Kommandanten bzw. Dienststellenleitern.

HINWEIS: Diese GehSV **einschließlich der formatgetreuen Aufbereitung der erforderlichen Formulare** ist im **Intranet** auf der **Homepage/Site**

<http://www.praes.intra.bmlv.at/vsavneu/index.htm>

als **Download** verfügbar.

ERGÄNZUNGS- UND ÄNDERUNGSBLATT

Ifd. Nr.	Ergänzungs- und Änderungserlass	Datum der Durchfüh- rung
1	GZ S90619/10-Präs/2011 (Text eingearbeitet)	1.1.2012

--	--	--

INHALTSVERZEICHNIS

A. Allgemeines	15
I. Rechtsgrundlagen	15
II. Geltungsbereich.....	16
III. Grundsätze	17
B. Klassifizierte Informationen	21
I. Begriff	21
II. Klassifizierung.....	22
III. Klassifizierungsstufen	24
1. EINGESCHRÄNKT (E).....	24
2. VERTRAULICH (V).....	24
3. GEHEIM (Geh).....	24
4. STRENG GEHEIM (StrGeh)	24
IV. Kennzeichnung	25
C. Zugang zu Klassifizierten Informationen	29
I. Voraussetzungen für den Zugang	29
II. Unterweisung.....	30
III. Dokumentation des Zuganges	32
D. Geheimschutzpersonal	33
I. Allgemeines.....	33
II. Verantwortlichkeit der Kommandanten und Leiter.....	34
III. Informationssicherheitsbeauftragter (InfoSihB).....	35
IV. Geheimschutzbeauftragter (GehSchB).....	36
E. Behandlung von Klassifizierten Informationen	39
I. Elektronische Verarbeitung	39
II. Kanzleimäßige Behandlung.....	40
III. Empfangsbestätigung	42
IV. Öffnen klassifizierter Informationen ab Klassifizierungsstufe VERTRAULICH	43
V. Verbuchung und Registrierung.....	44

VI.	Registrierung multilateral klassifizierter Informationen	47
VII.	Überführung von Papier in elektronische Form (Scannen).....	48
VIII.	Überführung elektronischer Informationen in Papierform	49
IX.	Kopieren	50
F.	Übermittlung Klassifizierter Informationen	53
I.	Allgemeines.....	53
II.	Verbringung, Versand, Übermittlung und Mitnahme.....	54
III.	Kuriere.....	56
IV.	Weitergabe innerhalb der Dienststelle.....	57
V.	Mündliche Weitergabe	58
G.	Verwahrung, Vernichtung und Kontrolle	59
I.	Verwahrung	59
II.	Vernichtung	61
III.	Kontrolle.....	64
IV.	Verlust oder Preisgabe.....	65
H.	Sonstige Bestimmungen für klassifizierte Informationen.....	67
I.	Weitergabe an ressortfremde Stellen.....	67
II.	Übergangsbestimmungen	68
III.	Strafbestimmungen.....	69
Beilagen:		
Beilage	I: Nachweis der Unterweisung.....	71
Beilage	II: Empfangschein.....	73
Beilage	III: Bestandverzeichnis für klassifizierte Informationen	75
Beilage	IV: Geschäftsbuch für klassifizierte Informationen	77

Beilage	V: Kurierbescheinigung	79
Beilage	VI: Zustellbuch für klassifizierte Informationen	81
Beilage	VII: Vernichtungsprotokoll.....	83
Beilage	VIII: Muster für Schriftstück mit korrekten Bezeichnungen	85
Beilage	IX: Muster AUT freigegeben für GBR	89
Beilage	X: Muster AUT freigegeben für NATO	91

Stichwortverzeichnis

A. ALLGEMEINES

I. Rechtsgrundlagen

Rechtsgrundlagen für die Geheimschutzvorschrift – in der Folge **1** auch in der Abkürzung GehSchV verwendet – sind **insbesondere:**

- Informationssicherheitsgesetz (InfoSiG),
- Datenschutzgesetz 2000 (DSG 2000),
- Informationssicherheitsverordnung (InfoSiV),
- Art 20 Abs 3 des Bundes-Verfassungsgesetzes (B-VG),
- § 46 des Beamten-Dienstrechtgesetzes (BDG),
- § 5 des Vertragsbedienstetengesetzes (VBG),
- 11 Abs 2 des Wehrgesetzes 2001 (WG 2001),
- §§ 26 bis 28 des Militärstrafgesetzes (MilStG),
- §§ 252 bis 255 und § 310 des Strafgesetzbuches (StGB),
- § 1 Abs 5 des Militärbefugnisgesetzes (MBG),
- § 12 Bundesministeriengesetz. (BMG).

II. Geltungsbereich

- 2 Die **Geheimhaltungsvorschrift** gilt im **gesamten Ressortbereich** des Bundesministeriums für Landesverteidigung und Sport (BMLVS).
- 3 Als **Dienststellen** im Sinne dieser Dienstvorschrift gelten im Bereich der Zentralstelle des BMLVS auch die Organisationseinheiten gemäß Bundesministeriengesetz.
- 4 Die **Leiter des Heeres-Nachrichtenamtes** und des **Abwehramtes** regeln für ihren jeweiligen Wirkungsbereich den Verkehr mit klassifizierten Informationen in Anlehnung an die Bestimmungen dieser Dienstvorschrift nach den besonderen Erfordernissen der militärischen Nachrichtendienste.
- 5 Die Geheimhaltungsvorschrift ist sowohl auf **nationale** als auch **internationale klassifizierte Informationen** anzuwenden.
Sofern aufgrund völkerrechtlicher Vereinbarungen **strengere Geheimhaltungsvorschriften** festgelegt wurden, sind diese für die betreffenden klassifizierten Informationen anzuwenden.
Diese werden im Bedarfsfall durch den **Ltr des Abwehramtes** in seiner Funktion **als Informationssicherheitsbeauftragter** festgelegt.
- 6 Im **Einsatz** und bei **Übungen** obliegt es den **Kommandanten abweichende Regelungen** für den Geheimhaltung zu verfügen.

III. Grundsätze

Zielsetzung dieser Dienstvorschrift ist die **Gleichbehandlung nationaler wie internationaler Informationen** um die Akzeptanz zu erhöhen und die administrativen und formalen Maßnahmen für den Bediensteten im Bereich des Geheimschutzes möglichst einfach zu halten. 7

Durch die **Einführung** einer **vierten Geheimhaltungsstufe** kann der Schutzgrad von klassifizierten Informationen besser in Einklang mit den Aufwendungen zum Schutz gehalten werden und es ist nicht mehr notwendig „zu hoch“ zu klassifizieren. 8

Unbeschadet der Bestimmungen dieser Dienstvorschrift verpflichtet Art. 20 Abs 3 B-VG alle mit Aufgaben der Bundes-, Landes- und Gemeindeverwaltung betrauten Organe, soweit gesetzlich nicht anders bestimmt ist, zur **Verschwiegenheit** über alle Ihnen ausschließlich aus ihrer amtlichen Tätigkeit bekannt gewordenen Tatsachen (**Amtsverschwiegenheit**). 9

Personen darf nur **Zugang zu klassifizierten Informationen** gewährt werden, 10

- wenn und so lange dies für die Erfüllung ihrer dienstlichen Aufgaben erforderlich ist („**need to know**“ **Prinzip**) und
- wenn sie entsprechend unterwiesen und ab der Klassifizierungsstufe VERTRAULICH aufwärts überprüft wurden (s. RdNr. 52 - 58).

Weiters gilt für alle Bediensteten im Ressort die „**Clear Desk Policy**“. Das bedeutet, dass außerhalb der Dienstzeit keine der Amtsverschwiegenheit oder einer Klassifizierungsstufe unterliegenden dienstlichen Schriftstücke, Arbeitsunterlagen, Stempel, Chipkarten, etc. in den Kanzleiräumen frei zugänglich sein dürfen. 11

- 12 Der **Bestand** an klassifizierten Informationen ist möglichst **gering** zu **halten**.
- 13 **Klassifizierte Informationen** sind entsprechend dieser Dienstvorschrift zu **kennzeichnen**.
- 14 Entsprechend dieser Dienstvorschrift sind
- der Bestand,
 - der Zugang,
 - die Übergabe und
 - die Vernichtung
- an klassifizierten Informationen zu dokumentieren.
- 15 Klassifizierte Informationen sind **gesichert zu verwahren** und vor **unbefugtem Zugriff** zu schützen.
- 16 **Informations-** und **Kommunikationstechnik** zur Verarbeitung, Übertragung und Speicherung von klassifizierten Informationen ist vor Verwendung im BMLVS einem **Zulassungsverfahren** zu unterziehen.
- 17 **Internationale klassifizierte Informationen** bezeichnet in dieser Dienstvorschrift alle klassifizierten Informationen, die unter Zugrundelegung völkerrechtlicher Verpflichtungen oder Bestimmungen klassifiziert wurden.
- 18 **Multilateral klassifizierte Informationen** bezeichnet in dieser Dienstvorschrift klassifizierte Informationen die mit Klassifizierungsvermerken nach den Bestimmungen der NATO und der EU versehen sind.
- 19 Im **multilateralen Bereich** nehmen die **Zentralregister EU und NATO** bei **BMLVS/MilPol** die Rechte des Verfassers wahr.

Register bezeichnet in dieser Vorschrift das jeweils zu Anwendung kommende Instrument zur Registrierung und/oder Verbuchung von klassifizierten Informationen. Es können dies sowohl Bestandsverzeichnisse oder Geschäftsbücher als auch Datenbanken in zugelassenen IKT-Systemen sein. **20**

B. KLASSIFIZIERTE INFORMATIONEN

I. Begriff

Klassifizierte Informationen sind Informationen, Tatsachen, Gegenstände und Nachrichten (unabhängig von Darstellungsform und Datenträger), die eines besonderen Schutzes gegen Kenntnisnahme und Zugriff durch Unbefugte bedürfen. **21**

Klassifizierte Informationen **können insbesondere sein:** **22**

- Schriftstücke,
- Zeichnungen,
- Pläne,
- Karten,
- Bildmaterial,
- elektronische Daten und Datenträger,
- Tonträger,
- Amtssiegel,
- technische Geräte,
- technische Systeme und/oder deren Teilkomponenten wenn diese klassifizierte Informationen enthalten oder verarbeiten.

II. Klassifizierung

- 23** Die **Klassifizierung einer Information** ist die Zuordnung einer Klassifizierungsstufe für diese Information.
- 24** Die **Klassifizierungsstufe** ist auf Grund des Schutzbedarfes der Information hinsichtlich des Schutzes vor Zugriff durch Unbefugte unter Berücksichtigung der in RdNr. 34 bis RdNr. 37 bei den einzelnen Klassifizierungsstufen angeführten Kriterien durch den Verfasser der Information festzulegen.
- 25** Die Zuordnung einer Klassifizierungsstufe hat unter **Abwägung** der erforderlichen **administrativen** und **sicherheitsmäßigen Aufwendungen** gegenüber dem im Fall einer Preisgabe zu erwartenden **Schaden** zu erfolgen.
- 26** **Ab** der **Klassifizierungsstufe VERTRAULICH** hat die Festlegung der Klassifizierungsstufe durch den Kommandanten/Dienststellenleiter (Ebene kleiner Verband/Abteilung) zu erfolgen.
- 27** Die **Deklassifizierung** ist die ersatzlose Aufhebung der Klassifizierung einer Information.
- 28** Wenn sich auf Grund einer **Änderung der Sachlage** oder **auf Grund des Zeitablaufes der Schutzbedarf** einer Information ändert, so ist die Klassifizierungsstufe durch jene Stelle welche die Klassifizierungsstufe festgelegt hat entsprechend anzupassen oder aufzuheben.
- 29** Die **Hinaufsetzung oder Herabsetzung** der Klassifizierungsstufe oder die Deklassifizierung ist zu **dokumentieren**. Die **Empfänger** der klassifizierten Information sind davon **in Kenntnis** zu **setzen**.

Die **Änderung** der Klassifizierung von **multilateral klassifizierten Informationen** ist nur auf schriftliche Weisung der Zentralregistratur BMLVS zulässig. **30**

Informationen, die sich auf **klassifizierte Informationen beziehen** (zB Stellungnahmen, Berichtigungen, Ergänzungen, Einladungen zu Besprechungen), sind, sofern sie keinen oder nur einen geminderten Rückschluss auf einen Inhalt zulassen, entweder mit einer herabgesetzten Klassifizierungsstufe zu versehen oder nicht zu klassifizieren. **31**

Haben zusammengefasste/zusammengeführte klassifizierte Informationen **verschiedene Klassifizierungsstufen**, so ist für die zusammengefasste/zusammengeführte klassifizierte Information die **jeweils höchste Klassifizierungsstufe** zu verwenden. Die Teile (zB Beilagen) behalten ihre Klassifizierungsstufe und können für sich alleine nach dieser Klassifizierungsstufe behandelt werden. **32**

Darüber hinaus ist zu prüfen, ob nicht auf Grund des Zusammenschlusses mehrer klassifizierten Informationen die **Schutzwürdigkeit gestiegen ist** und daher eine **höhere Klassifizierungsstufe erforderlich** ist. **33**

III. Klassifizierungsstufen

1. EINGESCHRÄNKT (E)

34 **Eingeschränkt** sind klassifizierte Informationen, deren unbefugte Weitergabe den im Art. 20 Abs. 3 B-VG genannten Interessen (Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, umfassenden Landesverteidigung, auswärtige Beziehungen, wirtschaftliche Interessen einer Körperschaft des öffentlichen Rechts, Vorbereitung einer Entscheidung, überwiegende Interessen der Parteien) zuwiderlaufen würde.

2. VERTRAULICH (V)

35 **Vertraulich** sind klassifizierte Informationen, deren unbefugte Weitergabe den im Art. 20 Abs. 3 B-VG genannten Interessen zuwiderlaufen würde und die zusätzlich nach anderen Bundesgesetzen unter strafrechtlichem Geheimschutz stehen und deren Geheimhaltung im öffentlichen Interesse gelegen ist

3. GEHEIM (Geh)

36 **Geheim** sind klassifizierte Informationen, die vertraulich sind und deren Preisgabe zudem die Gefahr einer erheblichen Schädigung der im Art. 20 Abs. 3 B-VG genannten Interessen schaffen würde.

4. STRENG GEHEIM (StrGeh)

37 **Streng Geheim** sind klassifizierte Informationen, die geheim sind und deren Bekanntwerden überdies eine schwere Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen wahrscheinlich machen würde.

IV. Kennzeichnung

Klassifizierte Informationen sind eindeutig und gut erkennbar durch Anbringen der Klassifizierungsstufe in Großbuchstaben und ausgeschriebenen kenntlich zu machen (Klassifizierungsvermerk) (s. Beilage VIII). 38

Bei **schriftlichen Informationen** ist auf jeder Seite in der **Kopf- und der Fußzeile** der Klassifizierungsvermerk anzubringen. 39

In der **Kopfzeile** ist überdies folgende **Seitennummerierung** anzubringen: Seite x von y (x = aktuelle Seitennummer, y = Gesamtzahl aller Seiten des Dokuments).

Bei den **Klassifizierungsstufen GEHEIM und STRENG** **GEHEIM** ist überdies in der **Kopfzeile jeder Seite** 40

- die Geschäftszahl,
 - das Datum der Genehmigung und
 - die Nummer der Ausfertigung
- anzubringen.

Im Geschäftsstück ist die **Zuordnung der Ausfertigungen** anzugeben.

Schriftliche Informationen, die **automatisiert mit zugelassenen IKT-Systemen erstellt** wurden, können aus zwingenden technischen Gründen bis zu einer Anpassung im nationalen Bereich davon **abweichende Kennzeichnungen** aufweisen. 41

Auf der ersten Seite von Dokumenten der **Klassifizierungsstufe VERTRAULICH** oder höher sind alle Beilagen (Anhänge und Beilagen) konkret aufzulisten. 42

Die **Beilagen** sind wie das Dokument selbst zu kennzeichnen, darüber hinaus sind sie **durchzunummerieren** und in der **Kopfzeile** jeder Seite ist der **Vermerk „ Beilage xxx zu GZ ...“** anzubringen. 43

44 **Beilagen**, die automatisiert mit zugelassenen IKT-Systemen erstellt wurden können aus zwingenden technischen Gründen bis zu einer Anpassung im nationalen Bereich, davon **abweichende Kennzeichnungen** aufweisen.

45 Auf **national klassifizierten Informationen** sind Klassifizierungsvermerke **ausschließlich** in **deutscher Sprache** anzubringen.

46 Bei **klassifizierten Informationen** im **internationalen Bereich** ist die Kennzeichnung **zweizeilig** wie folgt vorzunehmen:

- **die erste Zeile** enthält die **deutschen Begriffe** und setzt sich aus folgenden Elementen zusammen:
 - Länderbezeichnung: AUT,
 - Klassifizierungsgrad,
 - Formulierung „FREIGEGERBEN FÜR“,
 - Angabe des Empfängers (Organisation, Länderbezeichnung oder Koalition, zB EU, DEU, NATO,);
- unmittelbar unter diese deutsche Kennzeichnung ist die entsprechende **englische Kennzeichnung** zu setzen (**zweite Zeile**):

AUT GEHEIM FREIGEGERBEN für GBR
AUT SECRET RELEASABLE TO GBR

(s. Beilage IX)

- wird **in AUT eine EU-klassifizierte Information** erstellt ist die Kennzeichnung **einzeilig**, unter Verwendung der entsprechenden französischen Klassifizierungsvermerke zu setzen wie zB:

SECRET UE

Im **Geschäftsverkehr mit der NATO/PfP** – in weiterem Gebrauch in dieser Dienstvorschrift nur mehr als NATO bezeichnet – sind die Klassifizierungsvermerke in englischer Sprache, mit der EU jene in französischer Sprache zu verwenden (s. RdNr. 48). **47**

Die **Zuordnung** der englischen und französischen Klassifizierungsvermerke zu den jeweiligen deutschen Klassifizierungsvermerken ist der nachstehenden Tabelle zu entnehmen: **48**

Deutsch	Englisch	Französisch
EINGESCHRÄNKT	RESTRICTED	RESTREINT
VERTRAULICH	CONFIDENTIAL	CONFIDENTIEL
GEHEIM	SECRET	SECRET
STRENG GEHEIM	TOP SECRET	TRÈS SECRET

Bei von **internationalen Organisationen erhaltenen klassifizierten Informationen**, ist die jeweilige **Kennzeichnung beizubehalten**. **49**

Sollten **klassifizierte NATO oder EU Beilagen** einem (nationalen) **Geschäftsstück beigefügt** werden, so ist für dieses Geschäftsstück zumindest die jeweils höchste Klassifizierungsstufe zu verwenden. **50**

Sollte dies aus Gründen des nationalen Geheimschutzes nicht zweckmäßig sein, sind die **Beilagen gesondert** zu verteilen.

C. ZUGANG ZU KLASSIFIZIERTEN INFORMATIONEN

I. Voraussetzungen für den Zugang

Der **Zugang zu klassifizierten Informationen** ist nur unter den nachstehenden **Voraussetzungen** zulässig: 51

- Erfordernis für die Erfüllung der dienstlichen Aufgaben („**need to know**“ Prinzip),
- nachweisliche **Unterweisung** über den Umgang mit klassifizierten Informationen,
- ab der Klassifizierungsstufe VERTRAULICH eine der Klassifizierungsstufe entsprechende **Verlässlichkeitsprüfung** bzw. **Sicherheitsüberprüfung**:

Klassifizierungsstufe	Anforderungen
EINGESCHRÄNKT	need to know Geheimhaltungunterweisung
VERTRAULICH	need to know Geheimhaltungunterweisung einfache Verlässlichkeitsprüfung
GEHEIM	need to know Geheimhaltungunterweisung erweiterte Verlässlichkeitsprüfung
STRENG GEHEIM	need to know Geheimhaltungunterweisung erweiterte Verlässlichkeitsprüfung durch AbwA

II. Unterweisung

- 52** Personen, denen Zugang zu klassifizierten Informationen gewährt werden soll, sind **vor dem ersten Zugang einer Unterweisung** über den Umgang mit klassifizierten Informationen durch den Geheimschutzbeauftragten zu unterziehen.
- 53** Diese **Unterweisung** hat jedenfalls Informationen über nachstehende **Themen zu umfassen**:
- die Bestimmungen dieser Dienstvorschrift,
 - notwendige technische/organisatorische/personelle Absicherungsmaßnahmen gem. den nationalen und völkerrechtlichen Dienstvorschriften,
 - Gefährdung der Sicherheit durch indiskrete Gespräche,
 - Vorsichtsmaßnahmen beim Umgang mit den Medien,
 - Bedrohung durch nachrichtendienstliche Tätigkeiten,
 - Verpflichtung zur unverzüglichen Meldung von:
 - Annäherungsversuchen/Handlungsweisen, die auf Spionage hindeuten,
 - allen ungewöhnlichen Umständen mit Bezug zur mil. Sicherheit,
 - strafrechtliche bzw. disziplinare Folgen von Verstößen gegen die Geheimhaltungspflicht;
 - den Hinweis auf die Informationsblätter und das Informationsportal des Abwehramtes,
 - weitere gesetzliche oder erlassmäßige Bestimmungen abhängig von der Aufgabenstellung und der Art der zur Verfügung gestellten klassifizierten Informationen (s. Beilage I).
- 54** Bedienstete der Militärvertretung BRÜSSEL, Mitglieder nationaler Delegationen in multilateralen Gremien und sonstige Bedienstete, die mit EU und/oder NATO-Informationen befasst sind, sind **darüber hinaus nachweislich** über die gültigen Sicherheitsvorschriften des Rates der EU und/oder der NATO zu informieren.

Die Unterweisung ist jährlich zu wiederholen.	55
Der Nachweis der durchgeführten Unterweisung ist schriftlich festzuhalten (s. Beilage I). Der Nachweis ist vom Geheimschutzbeauftragten zu verwahren.	56
Die Unterweisung für die Geheimschutzbeauftragten (GehSchB) erfolgt jeweils durch die J2/ S2/Sicherheitsbeauftragten.	57
Die Unterweisung der Geheimschutzbeauftragten der Zentralstelle des BMLVS sowie unmittelbar Nachgeordneter erfolgt durch das Abwehramt.	58

III. Dokumentation des Zuganges

- 59** Der **tatsächliche Zugang** zu Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM, im Fall von NATO- klassifizierten Informationen bereits ab der Klassifizierungsstufe NATO- RESTRICTED, ist im jeweiligen **Register zu dokumentieren**.
- 60** Die **Dokumentation** hat
- den Namen der Person der Zugang gewährt wurde,
 - den Zeitpunkt des Zuganges sowie
 - die Bezeichnung der Information zu welcher der Zugang gewährt wurde
- zu enthalten.
- 61** Sofern für die **Dokumentation des Zuganges ein IKT-System** gem. RdNr. 75 verwendet wird, ist sicherzustellen, dass alle Zugriffe auf diese Informationen im System unveränderbar dokumentiert werden.
- Eine **schriftliche Dokumentation** des Zuganges im Register **entfällt** in diesem Fall.

D. GEHEIMSCHUTZPERSONAL

I. Allgemeines

Zum **Geheimsschutzpersonal** zählen

62

- der Informationssicherheitsbeauftragte (InfoSihB) und sein Stellvertreter,
- die Geheimsschutzbeauftragten (GehSchB) und deren Stellvertreter sowie
- die J2/S2/Sicherheitsbeauftragte und deren Stellvertreter.

Das Geheimsschutzpersonal muss über eine **gültige Prüfbescheinigung** verfügen (s. RdNr. 51).

63

II. Verantwortlichkeit der Kommandanten und Leiter

64 Die **Kommandanten (Dienststellenleiter)** sind **verantwortlich**, dass in ihrem Zuständigkeitsbereich die Bestimmungen über den Umgang mit klassifizierten Informationen bekannt sind und eingehalten werden.

Sie haben dafür zu sorgen, dass der Zugang zu klassifizierten Informationen nur nach den Bestimmungen dieser Dienstvorschrift erfolgt.

65 Die Kommandanten (Dienststellenleiter) **legen fest**, welche **Funktionen ihrer Dienststelle** Zugang zu klassifizierten Informationen welcher Klassifizierungsstufe benötigen (s. RdNr. 51 ff).

III. Informationssicherheitsbeauftragter (InfoSihB)

Der **Informationssicherheitsbeauftragte** (§ 4 Abs. 1 InfoSiV) des BMLVS ist der Leiter des Abwehramtes. **66**

Seine Aufgaben sind im § 4 Abs. 2 InfoSiV geregelt.

Sein Stellvertreter ist der stellvertretende Leiter des Abwehramtes.

Die **Organe des Abwehramtes** sind berechtigt, im Auftrag des InfoSihB in der Zentralstelle des BMLVS und bei allen nachgeordneten Dienststellen die Maßnahmen des Geheimschutzes und der Informationssicherheit jederzeit zu überprüfen. **67**

IV. Geheimschutzbeauftragter (GehSchB)

68 Der Kommandant (Dienststellenleiter) bestimmt den **GehSchB und dessen Stellvertreter** für seinen Bereich. Wird für eine Dienststelle kein GehSchB bestimmt, so hat der Kommandant (Dienststellenleiter) diese Funktion selbst auszuüben.

69 Im Bereich der **Zentralstelle des BMLVS** sind grundsätzlich bis Abteilungsebene (oder für gleichzuhaltende Organisationseinheiten) ein GehSchB und ein Stellvertreter zu bestimmen.

70 Fällt in einem Organisationsbereich nur eine **geringe Anzahl** von klassifizierten Informationen an, so braucht kein GehSchB bestimmt werden.

In diesem Fall sind die Aufgaben durch den Kommandanten (Dienststellenleiter) wahrzunehmen (s. RdNr. 68). Als Stellvertreter kann auch der GehSchB der übergeordneten Organisationsebene eingeteilt werden.

71 Wenn bei Dienststellen klassifizierte Informationen in **erheblichem Ausmaß** anfallen, können für einzelne Organisationselemente dieser Dienststellen oder für bestimmte Kategorien von klassifizierten Informationen eigene GehSchB bestellt werden.

72 Der **Stellvertreter** vertritt den GehSchB in dessen Abwesenheit, **ohne dass zwingend eine Übergabe** der klassifizierten Informationen zu erfolgen hat.

Der Name des Vertreters und der Zeitraum der Vertretung ist in den **Registern** auf geeignete Weise zu **vermerken**.

Der Geheimschutzbeauftragte hat in Bezug auf zu registrierende klassifizierte Informationen in Papierform insbesondere folgende **Aufgaben** wahrzunehmen: **73**

- Entgegennehmen klassifizierter Informationen,
- Führen der Register für klassifizierte Informationen,
- Verteilen der klassifizierten Informationen mittels Zustellnachweis zur Bearbeitung,
- Abfertigen und Versenden von klassifizierten Informationen,
- Verwahren und Vernichten von klassifizierten Informationen,
- Durchführen der Unterweisung gemäß RdNr. 52,
- Kontrollieren des Bestandes innerhalb der Organisationseinheit.

Als **J2/S2/Sicherheitsbeauftragte** eingeteilte Funktionsträger dürfen nicht als GehSchB oder Stellvertreter eingeteilt werden, sie unterstützen jedoch die GehSchB bei der Unterweisung gem. RdNr. 52. **74**

E. BEHANDLUNG VON KLASSIFIZIERTEN INFORMATIONEN

I. Elektronische Verarbeitung

Klassifizierte Informationen dürfen nur mit für die jeweiligen Klassifizierungsstufen zugelassenen IKT-Systemen (Hardware und Software) unter Einhaltung der entsprechenden Vorgaben verarbeitet, bearbeitet, übermittelt und gespeichert werden. 75

Klassifizierte Informationen sind bei Verfügbarkeit über entsprechend zugelassene elektronische Systeme zu **übermitteln**. 76

Die Weitergabe bzw. Vernichtung von Ausfertigungen in **Papierform** ist gem. RdNr. 179 zu dokumentieren. 77

In IKT-Systemen gem. RdNr. 75 ist sicherzustellen, dass auch alle **Lesezugriffe** auf verarbeitete klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH und höher bzw. der entsprechenden internationalen Klassifizierung **protokolliert** werden. 78

Bei **NATO klassifizierten Informationen** ist diese Protokollierung bereits ab der Klassifizierungsstufe NATO RESTRICTED erforderlich. 79

In diesen Systemen ist eine sinngemäße Abbildung der Bestimmungen der Kapitel II. bis VIII. sicherzustellen. 80

II. Kanzleimäßige Behandlung

- 81** Bei klassifizierten Informationen der **Klassifizierungsstufe GEHEIM oder höher** ist anstelle eines Verteilers eine Empfängerliste zu verwenden, in welcher die Empfänger oder Funktionen konkret angeführt werden.
- 82** **Ausfertigungen** von klassifizierten Informationen der **Klassifizierungsstufe GEHEIM oder höher** sind so durch eine fortlaufende Nummer (Ausfertigungsnummer) zu kennzeichnen, dass jede Ausfertigung einem bestimmten Empfänger zugeordnet werden kann. Die Zuordnung der Ausfertigungsnummern zu den Empfängern muss aus der Empfängerliste ersichtlich sein.
- 83** Als **Ausfertigungen** gelten die an die Empfänger ergehenden Erledigungen und die vom Originalakt oder den Ausfertigungen angefertigten Kopien.
- 84** Für **multilateral klassifizierte Informationen** erfolgt die Verteilung durch die Zentralregister des BMLVS.
- 85** Klassifizierte Informationen mit der Klassifizierungsstufe STRENG GEHEIM sind immer mit einem **Öffnungsvermerk** zu versehen.
- 86** Bei den **anderen klassifizierten Informationen** sind **Öffnungsvermerke** nur im Bedarfsfall auf Grund inhaltlicher Besonderheiten zu verwenden.
- 87** Der **Öffnungsvermerk** hat den **Wortlaut**
„Nur zu öffnen durch ...“
und die Funktion zu enthalten. Der Öffnungsberechtigte ist grundsätzlich durch seine Funktion (zB S2) zu bezeichnen. Nur in begründeten **Ausnahmefällen** darf im Öffnungsvermerk auch der Name des Öffnungsberechtigten angeführt werden.

Sofern ein System gem. RdNr. 75 bis 78 verwendet wird, ist **88**
anstelle des Öffnungsvermerks die Information funktionsbezogen so zu
adressieren, dass nur die in Frage kommenden Personen Zugriff
erhalten (keine Adressierung an Organisationseinheiten).

III. Empfangsbestätigung

- 89** Der **Empfang** klassifizierter Informationen in Papierform
- ab der Klassifizierungsstufe VERTRAULICH,
 - bei NATO-Informationen ab der Stufe EINGESCHRÄNKT und höher bzw. der entsprechenden internationalen Klassifizierung,
- ist vom Empfänger mittels einer der klassifizierten Information beigelegten Empfangsbestätigung (s. Beilage II) zu bestätigen.
- 90** Die Empfangsbestätigung ist an den Absender innerhalb von zehn Tagen zu retournieren.
- 91** Bei **Übermittlung von klassifizierten Informationen** durch Systeme gem. RdNr. 75 bis 78 entfällt die Bestätigung des Empfanges, wenn durch das System die Zustellung dokumentiert wird und dem Absender diese Dokumentation zugänglich ist.

IV. Öffnen klassifizierter Informationen ab Klassifizierungsstufe VERTRAULICH

Der **innere Umschlag** (s. RdNr. 130), welcher die klassifizierten Informationen enthält, darf nur vom Kommandanten (Dienststellenleiter), GehSchB oder angeführten Empfänger geöffnet werden. **92**

Der **Öffnungsberechtigte** hat die unverzügliche Registrierung der klassifizierten Information zu veranlassen.

Unterlagen im Zusammenhang mit **Verlässlichkeitsprüfungen** dürfen nur von Organen der nachrichtendienstlichen Abwehr geöffnet werden (§ 20 Abs. 3 MBG). **93**

Der Öffnungsberechtigte hat die **Umhüllung auf Unversehrtheit** und die **Sendung auf Vollzähligkeit** zu prüfen. **94**

Fehlende Stücke sind dem Absender unverzüglich anzuzeigen und bei der Übernahme in der Empfangsbestätigung zu vermerken.

Bei **Verdacht der unbefugten Öffnung** von klassifizierten Informationen sind durch den GehSchB unverzüglich die Maßnahmen gemäß RdNr. 191 bis 198 einzuleiten.

Bei **Übermittlung** von klassifizierten Informationen **durch IKT-Systeme** ist durch die Systemkonfiguration und durch die Aufstellung der Endgeräte sicher zu stellen, dass nur Berechtigte Zugang zu den übermittelten klassifizierten Informationen haben. **95**

V. Verbuchung und Registrierung

- 96** Die **Klassifizierungsstufe von Geschäftsbüchern** für die Verbuchung von Geschäftsstücken bis zur Klassifizierungsstufe **GEHEIM** ist **EINGESCHRÄNKT**, für jene der Klassifizierungsstufe **STRENG GEHEIM** ist das Geschäftsbuch **GEHEIM** zu klassifizieren.
- 97** Als **EINGESCHRÄNKT** klassifizierte Informationen sind gemäß den Bestimmungen der Büroordnung (Kanzleiordnung)
- in zugelassenen Systemen gem. RdNr. 75 bis 78 oder
 - in den allgemeinen Geschäftsbüchern (Kartei)
- zu verbuchen.
- Bei der **Verbuchung** ist der Klassifizierungsvermerk „**EINGESCHRÄNKT**“ ersichtlich zu machen.
- 98** Als **VERTRAULICH** klassifizierte Informationen sind in der Zentralstelle des BMLVS und den diesen unmittelbar nachgeordneten Ämtern im allgemeinen Geschäftsbuch (Kartei) gemäß den Bestimmungen der Büroordnung (Kanzleiordnung) zu verbuchen.
- Im Geschäftsbuch (Kartei) ist der Klassifizierungsvermerk „**VERTRAULICH**“ ersichtlich zu machen und der Vermerk über die Vernichtung anzubringen.
- Multilateral klassifizierte Informationen werden durch die Zentralregister BMLVS verwaltet und vernichtet.
- 99** Bei sonstigen nachgeordneten Dienststellen sind für klassifizierte Informationen mit der Klassifizierungsstufe **VERTRAULICH** eigene getrennte Geschäftsbücher zu führen, in welchen diese mit eigener Geschäftszahl zu verbuchen sind.
- 100** Als **GEHEIM** oder **STRENG GEHEIM** klassifizierte Informationen sind getrennt in eigenen Geschäftsbüchern gemäß Beilage IV oder mit zugelassenen IT-Systemen gem. RdNr. 75 bis 78 mit eigenen Geschäftszahlen zu verbuchen.

Klassifizierte Informationen der Klassifizierungsstufe VERTRAULICH oder höher, die im **Einsichtverkehr** vorgeschrieben werden, sind ebenso in **fortlaufender Reihenfolge des Einlangens – getrennt nach ihrer Klassifizierungsstufe ohne Vergabe einer eigenen Geschäftszahl** – in den Registern bzw. Geschäftsbüchern zu registrieren (s. Beilage IV). Nach **Weitergabe** des Geschäftsstückes ist die Eintragung zu **streichen**. **101**

Diese Registrierung entfällt bei Übermittlung in einem zugelassenen System gem. RdNr. 75 bis 78.

Die **Geschäftszahl** (Beispiel: 515-G/SI/2006) für jene klassifizierten Informationen in Papierform, die in eigenen Registern zu verbuchen sind, besteht aus: **102**

- der fortlaufenden Zahl innerhalb des laufenden Kalenderjahres (zu Jahresbeginn jeweils mit 1 beginnend),
- dem durch einen Bindestrich getrennten Klassifizierungsvermerk in abgekürzter Form (G bzw. SG),
- der durch einen Schrägstrich getrennten Kurzbezeichnung der Organisationseinrichtung gemäß Geschäftseinteilung der Zentralstelle bzw. gemäß aktuellem Abkürzungsverzeichnis,
- der durch einen Schrägstrich getrennten Jahreszahl (vierstellig).

In **Systemen gem. RdNr. 75 bis 78** dürfen Informationen verschiedener Klassifizierungsstufen gemeinsam behandelt werden, sofern das System den Anforderungen der höchsten zu verarbeitenden Klassifizierungsstufe entspricht. **103**

Dienststellen, die **keine Geschäftsbücher** führen, aber klassifizierte Informationen ständig oder vorübergehend verwahren, haben nach Klassifizierungsstufen und Herkunft (national / EU / NATO) **getrennte Register (Bestandsverzeichnisse)** zu führen (s. Beilage III). **104**

Sollte darüber hinaus aus Gründen der Übersichtlichkeit ein Nachweis über klassifizierte Geschäftsstücke notwendig werden, ist das Führen zusätzlicher Register anzuordnen.

105 Sofern ein System gem. RdNr. 75 bis 78 verwendet wird, ist der **Vorgang des Einbringens** der klassifizierten Information in das System einer **Registrierung gleichzuhalten**.

In diesem Fall sind auch klassifizierte Informationen in Papierform oder anderen Medien bis zur jeweils höchsten zugelassenen Stufe **in diesem System zu verbuchen**.

106 Bei den Registern und Geschäftsbüchern sind die **Buchseiten** zu **nummerieren**. Die **Seitenanzahl** ist am inneren, vorderen Umschlag zu vermerken und vom GehSchB zu bestätigen.

107 Die Register und Geschäftsbücher sind am **Jahresende** abzuschließen und dem Kommandanten (Dienststellenleiter) vorzulegen. Von diesem ist nach Überprüfung die **ordnungsgemäße Führung durch Abzeichnung zu bestätigen**.

VI. Registrierung multilateral klassifizierter Informationen

Alle multilateral klassifizierten Informationen (NATO, EU), die dem BMLVS zugehen, sind an die in der Zentralstelle des BMLVS eingerichteten Zentralregister weiterzuleiten. 108

Die **Verbuchung** von multilateralen Informationen 109

- mit den Klassifizierungsstufen VERTRAULICH,
- bei NATO ab der Stufe EINGESCHRÄNKT
- und höher

erfolgt **ausschließlich bei den Zentralregistern BMLVS** in eigenen **Geschäftsbüchern.**

Andere Dienststellen die international klassifizierte Informationen 110

- mit den Klassifizierungsstufen VERTRAULICH,
- bei NATO/PfP ab der Stufe EINGESCHRÄNKT
- und höher

ständig oder vorübergehend verwahren, haben **Register (Bestandsverzeichnisse)** zu führen.

Geschäftsbücher und Register sind getrennt nach multilateraler Organisation und Klassifizierungsstufe zu führen. 111

Multilateral klassifizierte Informationen bleiben stets im **Eigentum** der jeweiligen **multilateralen Organisation.** 112

Daher dürfen die Originaldokumente nicht als Beilagen zum Akt in den Kanzleien und Archiven hinterlegt werden sondern sind bei den dafür vorgesehenen Registern des BMLVS zu verwahren.

VII. Überführung von Papier in elektronische Form (Scannen)

- 113** Für das **Überführen** von klassifizierten Informationen, die in Papierform vorliegen, in elektronische Form (zB durch Einscannen) dürfen **nur Systeme** verwendet werden, die **gem. RdNr. 75 bis 78** dafür zugelassenen wurden.
- 114** In Papierform vorliegende klassifizierte Informationen
- der **Klassifizierungsstufe STRENG GEHEIM und GEHEIM** dürfen nur vom **Verfasser**,
 - der **Klassifizierungsstufe VERTRAULICH** nur mit **Genehmigung des Kommandanten (Dienststellenleiters)** gescannt werden.
- 115** Bei der Überführung **multilateral klassifizierter Informationen** in elektronische Systeme übernehmen die **jeweiligen Zentralregister BMLVS** die **Aufgaben des Verfassers**.

VIII. Überführung elektronischer Informationen in Papierform

Die **Überführung** von klassifizierten Informationen, die in elektronischer Form vorliegen, in Papierform (zB durch Ausdrucken) hat unter Verwendung der **gem. RdNr. 75 bis 78 angeführten Systeme** und Verfahren zu erfolgen. **116**

Die **verwendeten Systeme** haben die der jeweiligen Klassifizierungsstufe **entsprechende Dokumentation sicherzustellen.**

Mit den **Ausdrucken** ist nach den Bestimmungen dieser Dienstvorschrift für klassifizierte Informationen in Papierform vorzugehen **117**

IX. Kopieren

- 118** Unter „**Kopieren**“ ist in dieser Dienstvorschrift die Übertragung von klassifizierten Informationen von einem Medium oder System auf ein anderes zu verstehen, wobei die Originalinformation erhalten bleibt, wie zB:
- **Kopie** im herkömmlichen Sinn – von Papier auf Papier,
 - **Scannen** – von Papier zu IKT-System,
 - **Ausdrucken** – von IKT-System zu Papier.
- 119** **Nicht** unter „**Kopieren**“ fällt das Weitergeben oder Weiterleiten von Informationen (zB Die Belastung oder die Erteilung einer Leseberechtigung in einem ELAK- System).
- 120** **Kopien** von in **Papierform** vorliegenden klassifizierten Informationen der **Stufe EINGESCHRÄNKT** dürfen von dem **zum Empfang und zur Bearbeitung berechtigten Personenkreis** in dem für die Bearbeitung unmittelbar erforderlichen Ausmaß angefertigt werden.
- Bei der **Weitergabe** sind die Kriterien für den Zugang zu klassifizierten Informationen (s. RdNr. 51) zu berücksichtigen.
- Diese Kopien sind **unmittelbar nach Zweckerfüllung zu vernichten**.
- 121** In Papierform vorliegende klassifizierte Informationen der **Klassifizierungsstufe VERTRAULICH** dürfen nur mit Genehmigung des **Kommandanten (Dienststellenleiters)** kopiert werden.
- Die erteilte **Genehmigung** und die **Anzahl** der Kopien sind auf dem Original das kopiert wird durch den Genehmigenden mit Datum und Unterschrift zu vermerken.
- Die **Anzahl** der hergestellten Kopien sowie die **Empfänger** sind gemäß den Bestimmungen der RdNr. 97 ff zu verbuchen.

In Papierform vorliegende klassifizierte Informationen der Stufen **GEHEIM** und **STRENG GEHEIM** dürfen **durch die Empfänger NICHT KOPIERT** werden. Es ist beim **Ersteller** eine zusätzliche Ausfertigung anzufordern. **122**

Das Kopieren von **multilateralen klassifizierten Informationen** der Klassifizierungsstufe CONFIDENTIEL UE, bei NATO RESTRICTED und höher, ist nur mit schriftlicher Genehmigung der Zentralregister des BMLVS (s. RdNr. 108) zulässig, diese Kopien sind zu verbuchen und nach Zweckerfüllung dem Vernichtungsprozedere zuzuführen. **123**

Die **Herstellung von Auszügen** aus Geschäftsstücken der Klassifizierungsstufen **GEHEIM** und **STRENG GEHEIM**, sofern diese zur Erstellung eigener Geschäftsstücke dienen, ist mit **Genehmigung des Kommandanten (Dienststellenleiters)** zulässig. **124**

Dabei ist eine Neubeurteilung der Klassifizierungsstufe vorzunehmen.

Elektronisch vorliegende klassifizierte Informationen dürfen nur auf zugelassenen Systemen RdNr. 75 bis 78 und unter sinngemäßer Anwendung der Bestimmungen in den RdNr. 118 ff kopiert werden. **125**

Die **Protokollierung/Dokumentation** ist gemäß den für das jeweilige System verfügbaren Regelungen durchzuführen.

F. ÜBERMITTLUNG KLASSIFIZIERTER INFORMATIONEN

I. Allgemeines

Sofern **zugelassene elektronische Systeme** zur Verfügung stehen, sind diese zur Übermittlung zu verwenden. **126**

Die **Abfertigung** von klassifizierten Informationen der **Klassifizierungsstufe EINGESCHRÄNKT** ist – sofern sie nicht elektronisch erfolgt – vom zuständigen Kanzleileiter oder einem hiezu Beauftragten zu veranlassen. **127**

Die **Abfertigung** von klassifizierten Informationen der **Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM** ist – sofern diese nicht auf elektronischem Wege erfolgt – vom zuständigen GehSchB zu veranlassen. **128**

Dokumente der **Klassifizierungsstufe EINGESCHRÄNKT** sind im verschlossenen Kuvert zu übermitteln. **129**

Dokumente der **Klassifizierungsstufe VERTRAULICH** oder höher sind in einem doppelten undurchsichtigen verschlossenen Kuvert zu übermitteln, wobei nur am inneren Kuvert die Klassifizierungsstufe anzugeben und eine Empfangsbestätigung beizulegen ist (s. Beilage II). **130**

Am **äußeren Kuvert** sind lediglich der Empfänger und der Absender anzugeben. **131**

Das innere Kuvert ist mit einem geeigneten Sicherheitsklebeband so zu verschließen, dass eine Öffnung oder Öffnungsversuche während des Transportes zum Empfänger erkennbar sind. **132**

II. Verbringung, Versand, Übermittlung und Mitnahme

- 133 Die **Verbringung** von klassifizierten Informationen der **Klassifizierungsstufe EINGESCHRÄNKT** darf sowohl **innerhalb des Bundesgebietes** als auch **in das Ausland** auf dem **Postweg oder persönlich** erfolgen.
- 134 Klassifizierte Informationen der **Klassifizierungsstufe VERTRAULICH und GEHEIM** dürfen **innerhalb des Bundesgebietes** durch **Post oder Zustelldienst** versendet werden.
Dabei ist ein **Rückschein (RSa)** oder eine gleichwertige nachweisliche Zustellart zu verwenden die eine Zustellung an Ersatzempfänger ausschließt.
Eine Verbringung in das **Ausland** hat durch **Kurier** zu erfolgen, wobei **multilateral klassifizierte Informationen** nur in und über die jeweiligen Mitgliedsländer verbracht werden dürfen.
- 135 In **Ausnahmefällen** kann der **persönliche Transport** (das Mitführen) klassifizierter Informationen **bis zur Klassifizierungsstufe GEHEIM in das Ausland** genehmigt werden.
Die **Genehmigung** für national klassifizierte Informationen erteilt der Kommandant/Dienststellenleiter, für multilateral klassifizierte Informationen der InfoSihB/BMLVS (Ltr AbwA).
- 136 Klassifizierte Informationen der **Klassifizierungsstufe STRENG GEHEIM** sind **grundsätzlich** durch die **Militärstreife** sonst durch **zwei Kuriere** zu transportieren.
- 137 Die elektronische Übermittlung von klassifizierten Informationen hat auf **sicheren Übertragungswegen** auf dafür **zugelassenen Systemen** nach den vorgegebenen Methoden und Verfahren zu erfolgen.

- Eine **offene fernmündliche Weitergabe** von klassifizierten Informationen ist nur in Ausnahmefällen bei Gefahr in Verzug zulässig und nach Identifikation des Empfängers so zu halten, dass der Sachverhalt gegenüber Dritten verschleiert wird. **138**
- Für die **Mitnahme von multilateral klassifizierten Dokumenten** in das Ausland, einschließlich der Durchreisestaaten, ist **vor Reiseantritt die Zustimmung der Zentralregister BMLVS** einzuholen. Die Verbringung in das Ausland ist im jeweiligen Register zu vermerken. **139**
- Bedienstete, die **multilateral klassifizierte Informationen** auf Auslandsdienstreisen mitführen, sollen über einen **gültigen Dienst- oder Diplomatenpass** verfügen, jedenfalls ist eine **Kurierbescheinigung** (s. Beilage V) mitzuführen. **140**
- Klassifizierte Informationen dürfen **nicht an öffentlichen Orten gelesen und keinesfalls unbeaufsichtigt gelagert** werden. Sie sind in entsprechenden **Behältnissen österreichischer Vertretungen** zu verwahren. Ist dies nicht möglich, so sind sie **ständig persönlich mitzuführen** und während der **Ruhezeit in versperrbaren Behältnissen** (zB Hotelzimmersafe) zu lagern. **141**
- Nach **Beendigung der Dienstreise** ist den Zentralregistern BMLVS fernmündlich die ordnungsgemäße Wiederverwahrung zu melden. **142**
- Die **Mitnahme von IKT-Geräten und Systemen** gem. RdNr. 75 bis 78 in das Ausland ist im ADR-Auftrag bzw. in der Entsendeweisung anzuordnen. **143**
- Der Transport und die Lagerung von klassifiziertem Gerät ist in den fachdienstlichen Vorschriften zu regeln. **144**

III. Kuriere

- 145** Als **Kuriere** sind militärische Organe (§ 1 Abs. 1 MBG) einzuteilen.
Diesen ist vom zuständigen Vorgesetzten ein **schriftlicher Wachauftrag** zu erteilen.
In **Ausnahmefällen** können auch **Zivilbedienstete** der Zentralstelle als Kurier eingeteilt werden, denen jedoch **keine Befugnisse nach MBG** zustehen.
- 146** Als **Kuriere** für klassifizierte Informationen sind nur Personen einzuteilen, die über eine **gültige Prüfbescheinigung** verfügen.
- 147** Den Kurieren ist von der Dienststelle eine **Kurierbescheinigung** (s. Beilage V) auszustellen, die sie in Verbindung mit ihrem Dienstausweis oder Wehrdienstausweis zur Übernahme sowie Übergabe von klassifizierten Informationen berechtigt.
- 148** Zur Durchführung des Kurierauftrages kann auch das Tragen von **Zivilkleidung** angeordnet werden.
- 149** Kuriere sind, sofern sie klassifizierte Informationen der **Klassifizierungsstufen GEHEIM oder STRENG GEHEIM** befördern zu **bewaffnen**. Die Art der Bewaffnung ist der Bedrohung anzupassen. Kuriere die klassifizierte Informationen **in das Ausland** befördern sind **nicht zu bewaffnen**, außer das Mitführen von Waffen ist durch internationale Abkommen oder im Rahmen von Auslandseinsätzen ausdrücklich gestattet.
- 150** Für **Personen**, die gem. RdNr. 135 klassifizierte Informationen der Klassifizierungsstufen **GEHEIM oder STRENG GEHEIM** aus anderen Gründen **außerhalb militärischer Liegenschaften mit sich führen** (zB bei Besprechungen, Übungen), gelten die gleichen **Bestimmungen wie für Kuriere**.

IV. Weitergabe innerhalb der Dienststelle

Innerhalb der Dienststelle erfolgt die auch nur vorübergehende Weitergabe der klassifizierten Informationen der **Klassifizierungsstufe VERTRAULICH und höher** mit **Zustellbuch** (s. Beilage VI) oder mittels Empfangsschein (s. Beilage II). **151**

Zustellbücher sind mit der Bezeichnung der Dienststelle zu kennzeichnen. Zustellbücher enthalten keinen Hinweis auf den Inhalt der klassifizierten Information und unterliegen daher keiner Klassifizierung. **152**

Bei **Übermittlung und Bearbeitung** von klassifizierten Informationen **auf zugelassenen IKT-Systemen** entfällt die Bestätigung des Empfanges, wenn durch das System die Zustellung dokumentiert wird. **153**

V. Mündliche Weitergabe

- 154** Haben **Besprechungen** klassifizierte Informationen der **Klassifizierungsstufe VERTRAULICH oder höher zum Inhalt**, so ist dies in der Einberufung zur Besprechung unter Angabe der höchsten Klassifizierungsstufe bekannt zu geben.
- Es dürfen nur **Personen** an o.a. Besprechungen **teilnehmen**, welche die Ermächtigung zum Zugang zu klassifizierten Informationen der entsprechenden Klassifizierungsstufe besitzen (s. RdNr. 51).
- 155** Genehmigte Aufzeichnungen sind entsprechend zu klassifizieren. Die Mitnahme von nicht genehmigten **Kommunikationsmitteln** oder **Aufzeichnungsgeräten** ist verboten (zB Mobiltelefone).
- 156** Bei der **mündlichen Darlegung** von Informationen der **Klassifizierungsstufen GEHEIM oder STRENG GEHEIM** sind, wenn vom AbwA zugelassene **abhörgeschützte oder abhörsichere Räume** nicht zur Verfügung stehen, entsprechende Maßnahmen (u.a. Ortswahl, Abgabe von Mobiltelefonen und ähnlichen Geräten, Bewachung/Sicherung des Raumes) für die **Abhörsicherheit** zu treffen.

G. VERWAHRUNG, VERNICHTUNG UND KONTROLLE

I. Verwahrung

Klassifizierte Informationen sind der jeweiligen Klassifizierungsstufe entsprechend **in den Diensträumen gesichert zu verwahren** und dürfen nur bei unabdingbaren dienstlichen Notwendigkeiten aus diesen verbracht werden. **157**

Für die **Klassifizierungsstufe EINGESCHRÄNKT** sind **versperrbare Büromöbel** zu verwenden. **158**

Klassifizierte Informationen der **Klassifizierungsstufen VERTRAULICH oder höher** müssen in für diesichere Verwahrung von klassifizierten Informationen der entsprechenden Klassifizierungsstufe **zugelassenen Behältnissen** verwahrt werden. **159**

Eine Verwahrung in einem gemeinsamen Behältnis, welches für die jeweils höchste in Betracht kommende Klassifizierungsstufe zugelassen wurde, ist möglich (s.RdNr. 167). **160**

Den **Erstschlüssel** hat jene Person, die für die Benützung des Behältnisses verantwortlich ist so zu verwahren, dass ein Zugriff durch Unbefugte ausgeschlossen ist. **161**

Zweit- bzw. Reserveschlüssel (ggf. Codes für elektronische Schlösser) verwahren **162**

- in der Zentralstelle die Sicherheitsbeauftragten,
- sonst
 - der Kommandant,
 - Chef des Stabes oder
 - Dienststellenleiter

in einem verklebten Umschlag mit der Unterschrift des Erstschlüsselverwahrers in ihrem Behältnis für klassifizierte Informationen.

- 163 Im Umschlag ist eine **Schlüsselausgabeliste** zu verwahren.
- 164 Das **Öffnen** des Behälters mit dem Zweitschlüssel hat **im Beisein einer zweiten Person**, die in der Schlüsselausgabeliste einzutragen ist, zu erfolgen.
- 165 Bei **Verlust eines Schlüssels** ist dies dem Vorgesetzten unverzüglich zu melden und sind bis zur Änderung / Erneuerung des Schlosses geeignete Maßnahmen zur Verhinderung unbefugter Zugriffe zu setzen.
- 166 Allenfalls in **Papierform** oder auf **Datenträgern** vorliegende national und/oder multilateral klassifizierte Informationen sind **getrennt für die jeweilige Organisation** und **getrennt nach Klassifizierungsstufen** zu verwahren.

BEACHTEN: National klassifizierte Informationen sind getrennt von multilateral klassifizierten Informationen zu verwahren.

- 167 Allenfalls in **Papierform** oder auf **Datenträgern** vorliegende **national und/oder multilateral klassifizierte Informationen** können in einem **gemeinsamen Behältnis verwahrt** werden. In diesem Fall müssen die **Behältnisse** den Anforderungen für die **höchste Klassifizierungsstufe** der gemeinsam verwahrten klassifizierten Informationen **entsprechen**. Dabei ist jedoch eine **organisatorische Trennung** (zB in getrennten Ordnern) nach Klassifizierungsstufen und Organisationen einzuhalten.
- 168 Im **Einsatz** und **bei Übungen** können klassifizierte Informationen entsprechend den Bedingungen im Einsatz- oder Übungsraum in einfachen versperrbaren Behältnissen verwahrt werden, sofern eine **durchgehende Bewachung** sichergestellt ist.

II. Vernichtung

Die **verfassende Stelle** hat auf den **Ausfertigungen** zu vermerken **169**
ob die klassifizierte Information zu einem bestimmten Zeitpunkt, nach
Zweckerfüllung oder auf Weisung zu vernichten ist.

Ist **kein Vermerk** angebracht so hat der **Kommandant (Dienststellenleiter)** der aufbewahrenden Stelle festzulegen wann die klassifizierte Information zu vernichten ist.

MERKE: Wurde **keinerlei Festlegung** getroffen, so ist die klassifizierte Information **nach 10 Jahren** zu vernichten.

Das **beim Verfasser abgelegte Original** der klassifizierten Information ist nach den Bestimmungen der Büroordnung bzw. der Kanzleiordnung zu skartieren. **170**

Eine Anmietung oder Abgabe von klassifiziertem Schriftgut ab der Klassifizierungsstufe **VERTRAULICH** an das Österreichische Staatsarchiv kommt erst nach erfolgter Deklassifizierung in Betracht.

Register, Bestandsverzeichnisse und Zustellbücher sind **unbegrenzt** aufzubewahren. **171**

Originale von klassifizierten Informationen der Klassifizierungsstufen **VERTRAULICH, GEHEIM und STRENG GEHEIM** sowie **nicht mehr benötigte Register** für klassifizierte Informationen dieser Klassifizierungsstufen der Zentralstelle des BMLVS und der dem BMLVS unmittelbar nachgeordneten Kommanden und Dienststellen, die gemäß RdNr. 170 zu skartieren wären, sind nicht zu vernichten sondern dem bei der **Präsidialabteilung eingerichteten Zwischenarchiv** für klassifizierte Informationen zuzuführen. **172**

Dies gilt nicht für klassifizierte Informationen die beim **AbwA oder HNaA** anfallen. **173**

- 174** Die **Vernichtung** von klassifizierten Informationen gem. RdNr. 22 hat mit einem für die jeweilige Klassifizierungsstufe freigegeben Verfahren so zu erfolgen, dass keine auswertbaren Reste der klassifizierten Information übrig bleiben.
- 175** Die **Vernichtung** von klassifizierten Informationen der **Klassifizierungsstufen VERTRAULICH und GEHEIM** hat durch den **GehSchB** unter **Anwesenheit eines Zeugen** zu erfolgen.
- 176** Die **Vernichtung** von klassifizierten Informationen der **Klassifizierungsstufe STRENG GEHEIM** hat durch den **GehSchB** unter **Anwesenheit von 2 Zeugen** zu erfolgen.
Die **Zeugen** müssen über die Zugangsberechtigung zu klassifizierten Informationen der entsprechenden Klassifizierungsstufe verfügen.
- 177** **Multilateral klassifizierte Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM** werden ausschließlich durch **die Zentralregister BMLVS** vernichtet.
- 178** **Klassifizierte Informationen der Klassifizierungsstufe NATO RESTRICTED** sind durch den **GehSchB** der verwahrenden Stelle zu vernichten.
Eine **Kopie** des Vernichtungsprotokolls ist dem **Zentralregister BMLVS** zu übermitteln.
- 179** Bei der **Vernichtung** von klassifizierten Informationen **ab** der Klassifizierungsstufe **VERTRAULICH** ist ein **Vernichtungsprotokoll** (s. Beilage VII) anzulegen, welches **10 Jahre aufzubewahren** ist.
- 180** Bei **Verwendung eines IKT-Systems** gem. RdNr. 75 bis 78 entfällt die Verpflichtung zur Führung eines Vernichtungsprotokolls dann, wenn für die Vernichtung freigegebene Verfahren verwendet werden, die eine ausreichende Dokumentation sicherstellen.

Eintragungen über klassifizierte Informationen, die vernichtet wurden, sind in den in Papierform vorliegenden **Registern in roter Farbe zu streichen**; die Vernichtung ist mit Bezug auf das Vernichtungsprotokoll anzumerken. **181**

Besteht die **unmittelbar drohende Gefahr**, dass klassifizierte Informationen **durch Unbefugte in Besitz genommen werden** oder eine **Preisgabe** erfolgen könnte, ist der unverzügliche Abtransport oder falls dies nicht möglich ist die unverzügliche Vernichtung sicherzustellen. **182**

Grundsätzlich darf die Vernichtung von klassifizierten Informationen in diesem Fall **nur auf Weisung des Vorgesetzten** erfolgen. Kann die Weisung hiezu nicht rechtzeitig eingeholt werden, ist die Vernichtung selbständig durchzuführen. **183**

Die Vernichtung ist **schriftlich zu dokumentieren**. Entsprechende Vorkehrungen zur **raschen Vernichtung** sind vorzusehen.

Kommandotagebücher und Einsatzjournale sind nicht zu vernichten. **184**

III. Kontrolle

- 185** Das **System** des Geheimschutzes ist durch den J2/S2/Sicherheitsbeauftragten in seinem Wirkungsbereich mindestens **1x jährlich** nachweislich zu **überprüfen**.
- 186** Dabei sind insbesondere
- die Vollständigkeit der Aufzeichnungen,
 - die Sicherheit der Behältnisse und
 - das Schlüsselsystem (Schlüsselordnung)
- zu überprüfen.
- 187** Sind klassifizierte Informationen der **Klassifizierungsstufen GEHEIM oder STRENG GEHEIM** vorhanden, so ist eine **vollständige Überprüfung** der Vorgänge vorzunehmen.
- 188** Bei klassifizierten Informationen der **Klassifizierungsstufen VERTRAULICH** ist eine **stichprobenartige Überprüfung** vorzunehmen.
- 189** Das **Überprüfungsergebnis**, ab Ebene großer Verband aufwärts, ausgenommen HNaA, ist auf dem Dienstweg dem AbwA vorzulegen.
Die durchgeführte Überprüfung ist in **den Registern zu vermerken**.
- 190** Davon unberührt bleiben zusätzliche Überprüfungen durch vorgesetzte Dienststellen.

IV. Verlust oder Preisgabe

Der **Verlust** oder die **Preisgabe** von klassifizierten Informationen **bzw. ein entsprechender Verdacht** sind unverzüglich dem Kommandanten (Dienststellenleiter) sowie mittels BV-Meldung zu melden. **191**

Der **Kommandant/Dienststellenleiter** hat alle erforderlichen Maßnahmen zur Wiederauffindung, Untersuchung des Vorfalles und Verhinderung von (weiteren) Schäden zu treffen. **192**

Das **Untersuchungsergebnis** und die getroffenen Maßnahmen sind schriftlich zu dokumentieren und auf dem Dienstweg dem AbwA zu melden. **193**

Beim **Verdacht einer gerichtlich strafbaren Handlung** ist überdies vom Disziplinarvorgesetzten Anzeige bei der zuständigen Staatsanwaltschaft zu erstatten. **194**

Der Verlust oder die Preisgabe ist auch jener Stelle zu melden die die klassifizierte Information ausgegeben hat (**Verfasser**). Diese hat zur Verhütung von (weiteren) Schäden alle nach dem Inhalt der klassifizierten Information zur **Schadensbegrenzung** erforderlichen Maßnahmen zu treffen. **195**

Werden in Verlust geratene klassifizierte Informationen **innerhalb von 4 Wochen** nicht wiederaufgefunden, so ist unter Vorlage eines Berichtes über den Stand der Ermittlungen die Entscheidung über Fortführung oder Einstellung der Untersuchung bei der vorgesetzten Dienststelle einzuholen. Die getroffene Entscheidung ist dem AbwA zu melden. **196**

197 Das **Auffinden** einer in Verlust geratenen klassifizierten Information ist ebenfalls dem Kommandanten/Dienststellenleiter zu melden. Dieser hat die Zustandebringung dem AbwA und dem Verfasser zu melden.

Dabei ist anzugeben **wann und wo** die klassifizierte Information gefunden wurde und ob **Unbefugte** dazu **Zugang** hatten.

198 Der Verlust, die Preisgabe und das Wiederauffinden von internationalen, aufgrund völkerrechtlicher Vereinbarungen klassifizierten Informationen ist unverzüglich dem Informationssicherheitsbeauftragten zu melden. **Die Untersuchung obliegt dem AbwA.**

H. SONSTIGE BESTIMMUNGEN FÜR KLASSIFIZIERTE INFORMATIONEN

I. Weitergabe an ressortfremde Stellen

Vor der Übermittlung von klassifizierten Informationen ist durch Prüfung im Einzelfall sicherzustellen, dass beim Empfänger die Voraussetzungen für einen adäquaten Schutz gegeben sind. **199**

Von der **Auskunftspflicht** nach dem Auskunftspflichtgesetz, und Informationsweiterverwendungsgesetz sind klassifizierte Informationen **ausgenommen**. **200**

II. Übergangsbestimmungen

- 201** Die bisher im **BMLVS-ELAK** eingerichtete Klassifizierungsstufe „**VERSCHLUSS**“ wird mit Inkrafttreten dieser Dienstvorschrift deaktiviert und für die Neuanlage von Dokumenten gesperrt. Es ist vorgesehen, "**DATENSCHUTZ**" im BMLVS-ELAK als eigenständiges Merkmal zu realisieren. Es wird darauf hingewiesen, dass das Merkmal "**DATENSCHUTZ**" bereits bisher keine Verschlussstufe im Sinne der VSaV war und auch weiterhin **keine Klassifizierungsstufe im Sinne der GehSV** darstellt.
- 202** Für klassifizierte Informationen (**VERSCHLUSS**, **RESTREINT-UE** und **NATO-RESTRICTED**), die vor Inkrafttreten dieser Dienstvorschrift angefallen sind und nicht mehr weiter bearbeitet werden, ergeben sich keine Änderungen.
- 203** Im Bedarfsfall bzw. bei einer Weiterbearbeitung hat durch den Ersteller eine **Neubeurteilung der Klassifizierungsstufe** nach den Bestimmungen dieser Dienstvorschrift (s. RdNr. 34ff) zu erfolgen.
- 204** Grundsätzlich sind bestehende klassifizierte Informationen wie folgt zu **behandeln**:
- „**VERSCHLUSS**“ wie „**EINGESCHRÄNKT**“.
 - „**GEHEIM**“ und „**STRENG GEHEIM**“ unverändert.
- 205** Informationen der Klassifizierungsstufe **VERTRAULICH** und höher, ausgenommen multilateral klassifizierte Informationen, können weiterhin in den **bisher verwendeten Behältnissen** gelagert werden.
- Bei **Neubeschaffungen** ist nach den Bestimmungen dieser Dienstvorschrift vorzugehen.
- 206** Das Datum des Inkrafttretens dieser Dienstvorschrift ist in den Geschäftsbüchern und Bestandsverzeichnissen in roter Schrift zu dokumentieren.

III. Strafbestimmungen

207 Verstöße gegen die Bestimmungen dieser Dienstvorschrift sind ungeachtet einer allfälligen (verwaltungs-)strafrechtlichen Verfolgung dienstrechtlich zu ahnden.

BEILAGE I

Nachweis der Unterweisung

Nachweis der Geheimschutzverpflichtung

A: Identität der verpflichteten Person und Angaben zu deren Arbeitgeber¹

Name, Vorname, akad. Grad, Dienstgrad, Nationalität	Geburtsdatum: Geburtsort:
Wohnadresse	Ausweis/Reisepass Nr. ² : Ausstellungsbehörde: Ausstellungsdatum:
Bezeichnung der Dienststelle/Firma inkl. Adresse	

B: Grund der besonderen Verpflichtung zur Geheimhaltung sowie Bezeichnung der Klassifizierungsstufe

Zugang zu klassifizierter nationaler Information	³
Zugang zu völkerrechtlich klassifizierter Information	⁴
Zutritt zu Sicherheitsbereich Sicherheitsstufe A	⁵

VERPFLICHTUNG

zum Schutz klassifizierter Information

Die verpflichtete Person wurde über folgende Punkte unterwiesen:

1. Art der klassifizierten Information
2. Notwendige technische/organisatorische/personelle **Absicherungsmaßnahmen gem. den nationalen und völkerrechtlichen Sicherheitsvorschriften**
3. Gefährdung der Sicherheit durch indiskrete Gespräche
4. Vorsichtsmaßnahmen beim Umgang mit der Presse
5. Bedrohung durch nachrichtendienstliche Tätigkeiten⁶

¹ Falls zutreffend

² Amtlicher Lichtbildausweis:

a. bei der Ausstellung von Sicherheitsermächtigungen ist zwingend ein Reisepass vorzulegen

b. in jedem Fall sind die Ausweisnummer, die Ausstellungsbehörde und das Ausstellungsdatum anzugeben

³ Angabe der jeweiligen höchsten Klassifizierungsstufe sowie Funktion bzw. Zweck für den Zugang (z.B.: GEHEIM, SB VSa II G4Abt/ KdoEU)

⁴ Angabe des Staates oder der Organisation und der jeweiligen höchsten Klassifizierungsstufe sowie Funktion bzw. Zweck für den Zugang. Falls erforderlich auch Einschränkung auf konkrete klassifizierte Informationen.

⁵ Konkrete Bezeichnung des zu betretenden Sicherheitsbereiches gemäß Sicherheitsstufenerlass (z.B.: FIH ZELTWEG, FIWf 2)

6. **Verpflichtung zur unverzüglichen Meldung von:**

- Annäherungsversuchen/Handlungsweisen, die auf Spionage hindeuten
- Allen ungewöhnlichen Umständen mit Bezug zur mil. Sicherheit

7. **Strafrechtliche bzw. disziplinaire Folgen von Verstößen gegen die Geheimhaltungspflicht**

Die zur Kenntnis gelangten klassifizierten Informationen unterliegen der Geheimhaltung („need to know“) und sind jederzeit vor der Kenntnisnahme durch unbefugte Personen zu schützen.

Der verpflichteten Person werden folgende Dokumente (auszugsweise) zur Verfügung gestellt bzw. wurde darauf hingewiesen, wo diese einzusehen sind (Intranet, Internet etc.):

- VSaV (Geheimhaltungsvorschrift)
 - Richtlinien für den Geheimschutz von multilateralen Unterlagen
 - Sicherheitsbestimmungen der NATO (in der geltenden Fassung)
 - Sicherheitsbestimmungen der EU (in der geltenden Fassung)
- InfoSiG (Informationssicherheitsgesetz)
- InfoSiV (Informationssicherheitsverordnung)
- DSGVO (Datenschutzgesetz)
- Örtlich bedingte Absicherungsmaßnahmen⁷
 - Zutrittsbestimmungen
 - Verpflichtung zum Tragen der Identitätskarte
 - Verbot Fotografieren und Filmen
 - Verbot Mitnahme Mobiltelefon
 - Verbot Mitnahme IKT-Geräte (Laptop, Palm, Aufzeichnungsgeräte, udgl.)
 - Mitnahmeberechtigung
 - Schlüsselordnung
 - Brandschutz
-
-

(Zutreffendes ankreuzen)

Unterschriften

Ort und Datum	Die verpflichtete Person:	Der/Die Sicherheitsbeauftragte: Der/Die Geheimschutzbeauftragte:

⁶ Vor allem über den Modus operandi von Nachrichtendiensten

⁷ z.B. für Bedienstete, die dauerhaft in einem Sicherheitsbereich Dienst versehen

⁸ Raum für allfällige weitere vor Ort erforderliche oder sonstige Verhaltensregeln

Empfangschein

Innerhalb von 10 Tagen zurück an den Absender!

EMPFANGSCHEIN

EMPFÄNGER _____ bestätigt den
 (Dienststempel)

Empfang von:

StkZl.	ABSENDER (Dienststempel)	Erl-GeschZahl/ Ausfertigung	Beilg.	Ev. Nr.

..... am (Unterschrift)

BMLV R 1339/1
7530-0-104-0092

Geschäftsbuch für klassifizierte Informationen

Eigene Geschäftszahl	Des Schreibens		Von wem?	Anzahl der Belegen	Gegenstand	Datum der Genehmigung	Datum der Abfertigung	Anzahl der Belegen	Eriedigung	Hinterlegungsvermerk (Zahl)	Anmerkung
	Datum	Nr.									
612	2. 6. 08	3007 / 6. KontrA / 6. 08	KontrA	3	Kontrollbericht 2. Aufw				Oberst KAULMANN z.N. 10.6.2008		
	6. 6. 08	3771 / 6. 08	AbwA	2	Informationsersatz Datensicherheit EDI-Konzept - Akt -				Einrichtungsbeleg		Weitergabe an S II 16.6.2008
613	16. 6. 08		S I		Information für den Herrn BM über besonderen Vorfall - Akt - 13.6.2008		16. 6. 08	17. 6. 08	Verteiler: KBM S II S III 1. Aufw 2. Aufw 3. Aufw		

Kurierbescheinigung

(Dienststelle) (Unit / office / agency)		(Ort, Datum) (Place, date)
Kurierbescheinigung Courier Pass		
(Amtstitel / Dienstgrad) (Official title / rank)	(Name)	(GebDatum) (Date of birth)
Dienstausweis Nr.: / ID card no:		
Ist berechtigt, vom (am) bis Is authorised from (on) to		
klassifizierte Informationen folgender Klassifizierungsstufen anzunehmen bzw. zu übergeben. to take over and to hand over classified information for classifications		
<ul style="list-style-type: none"> - VERTRAULICH / CONFIDENTIAL – national *) – international *) - GEHEIM / SECRET – national *) – international *) - STRENG GEHEIM / TOP SECRET – national *) – international *) 		
Der / The (Dienststellung / official function)		
*) Nichtzutreffendes streichen / Delete as appropriate		
(Name, Amtstitel / Dgrad - Name, official title / rank)		

Muster für Schriftstück mit korrekten Bezeichnungen

GEHEIM
Seite 1 von xxx



Bundesministerium
für Landesverteidigung und Sport
[VerantwOEKurzbez]

Sachbearbeiter:
NAME
Tel: TELNR
IFMIN: IFMINNR

GZ.xxx G/DSt /20xx

[GegenstandErl]

Bezug
Bezugszahl

An
Empfängerliste

TEXT

[GenDatum]
Für den Bundesminister:
[Genehmiger]

Beilagen:
xx Beilagen
xx Anhänge

Erght an:
Empfängerliste + AusfertigungsNr.

**Diese VSa ist nach
Zweckerfüllung // Weisung
zu vernichten**

GEHEIM

(Erledigung – Original)



Bundesministerium
für Landesverteidigung und Sport
[VerantwOEKurzbez]

Sachbearbeiter:
NAME
Tel: TELNR
IFMIN: IFMINNR

GZ xxx-G/DSI /20xx

GenDatum
1.Ausfertigung für DSI

[GegenstandErl]

Bezug:
Bezugszahl:

An
Empfängerliste

TEXT

[GenDatum]
Für den Bundesminister:
[Genehmiger]

Beilagen:
xx Beilagen
xx Anhänge

Ergeht an:
Empfängerliste+ AusfertigungsNr.

**Diese VSA ist nach
Zweckerfüllung // Weisung
zu vernichten**

GEHEIM

(Ausfertigung)

GEHEIM
Seite 10 von xxx

Beilage xxx zu GZ: xxx EvidNr: xxx

Beilage

,

GEHEIM

(Beilage)

AUT GEHEIM FREIGEgeben für GBR
AUT SECRET RELEASABLE TO GBR
Page 1 of xxx

GenDatum
xx. Copy



AUSTRIAN
FEDERAL MINISTRY
OF DEFENCE AND SPORTS
[VerantwDEKurzbez]

GZ: xxx-Geh/DSr /20xx

Subject
[GegenstandEri]

Reference:
[Bezugszahl]

To
[Empfänger]

TEXT

[GenDatum]
On behalf of the federal minister:
[Genehmiger]

Copy to / CC:

Attachments:
xx Annexes
xx Appendices

AUT GEHEIM FREIGEgeben für GBR
AUT SECRET RELEASABLE TO GBR

AUT GEHEIM FREIGEGBEN für NATO
NATO/PFP SECRET RELEASABLE TO NATO
Page 1 of xxx

[GenDatum]
xx. Copy



**AUSTRIAN
FEDERAL MINISTRY
OF DEFENCE AND SPORTS
[VerantwOEKurzbez]**

GZ: xxx-Geh/DSt /20xx

Subject
[GegenstandErl]

Reference:
[Bezugszahl:]

To
[Empfänger]

TEXT

[GenDatum]
On behalf of the federal minister:
[Genehmiger]

Copy to / cc:

Attachments:
xx Annexes
xx Appendices

AUT GEHEIM FREIGEGBEN für NATO
NATO/PFP SECRET RELEASABLE TO NATO
-1-

STICHWORTVERZEICHNIS

Die Zahlen bezeichnen jene Randnummern,
in denen der Gegenstand behandelt ist.

- A**
- Abfertigung
 - Eingeschränkt 127
 - Geheim/Streng Geheim 128
 - Vertraulich 128
 - Abhörsicherheit 156
 - Amtsverschwiegenheit 9
 - Änderung der Klassifizierung 30
 - Ausfertigungen 83
 - Ausfertigungen in Papierform
 - Vernichtung 77
 - Weitergabe 77
 - Auskunftspflicht 200
 - Ausnahmefall 135, 138
- B**
- Behältnis 159
 - Beilagen 42, 43, 44
 - Bestand 12
 - Bestätigung
 - Entfall 153
 - Bewaffnung 149
- C**
- Clear Desk Policy 11
- D**
- Deklassifizierung 27
 - Deklassifizierung dokumentieren 29
 - Dienst- oder Diplomatenpass 140
- Dienststellen** 3
- Disziplinarvorgesetzter 194
 - Dokumentation
 - IKT 61
 - Inhalt 60
 - Zugang 59
- E**
- Einsatz 6
 - Empfangsbestätigung
 - Entfall 91
 - Empfangsbestätigung 89
 - Erstschlüssel 161
- G**
- Geheimhaltungsstufe 8
 - Geheimenschutzbeauftragter 68, 71
 - Aufgaben 73
 - ZentrSt 69
 - Geheimschutzpersonal 62
 - Geheimschutzvorschrift 2
 - Geltungsbereich 2
 - Geschäftsbücher 106
 - Abschluß 107
 - Geschäftsstück 50
 - Geschäftsverkehr 47
 - Geschäftszahl 102
 - Grundsätze 7

H

Herstellung von Auszügen 124

I

IKT 16

Informationen

- internationale klassifizierte 5, 17
- klassifizierte 31
- multilateral klassifizierte 18
- nationale 5

Informationssicherheits-
beauftragter 5, 66

K

Kennzeichnung 13, 38, 41, 46

Klassifizierte Informationen 21, 22

- Ausfertigungen 82
- Besprechung 154
- Einsichtsverkehr 101
- Empfängerliste 81
- IKT-Systeme 75
- Lagerung 141
- scannen 114
- Überführung in Papier 116
- Überführung in IKT 113
- Übermittlung 126
- Verbringung 133
- Verlust/Preisgabe 191
- Vernichtung 169, 174
- Verwahrung 157, 166
- Weitergabe 151
- Weitergabe an Ressortfremde 199
- Wiederauffindung 196
- Zugang 51

Klassifizierung 23

Klassifizierungsstufe 24, 79

- dokumentieren 29
- Eingeschränkt 34
- Geheim 36
- höchste 167
- höhere 33
- Kopfzeile 40
- Streng Geheim 37
- verschiedene 32
- Vertraulich 35

Klassifizierungsvermerk 39, 45

- Zuordnung 48

Kopien

- Eingeschränkt 120
- Geheim/Streng Geheim 122
- multilaterale klassifizierte Information 123
- Vertraulich 121

kopieren 118

Kurier 145

Kurierbescheinigung 140, 147

Kuvert

- Eingeschränkt 129
- Vertraulich und höher 130

L

Leiter

- Abwehramt 4
- Heeres-Nachrichtenamt 4

Lesezugriffe 78

M

Militärstreife 136

O

Öffnungsberechtigter 92

Öffnungsvermerk 85, 86, 87

Originaldokumente 112

Originale 172

P

Prüfbescheinigung 63, 146
Prüfung Vollzähligkeit 94

R

Rechtsgrundlagen 1
Register 20, 106
– Abschluß 107
– getrennte 104
Registrierung 108
– IKT 105
Reserveschlüssel 162

S

Schlüsselausgabeliste 163, 164
Schutzbedarf 28
Sicherheitsvorschriften 54
Skartierung 170
Strafbestimmungen 207

U

Übergangsbestimmungen 201
Übermittlung
– IKT-Systeme 95
Überprüfung
– stichprobenartig 188
– vollständige 187
Überprüfung 185
Überprüfungsergebnis 189
Übungen 6
Untersuchungsergebnis 193
Unterweisung 52, 53, 55
– GehSB 57
– GehSB/ZentrSt 58
– Nachweis 56

V

Verantwortlichkeit 64
Verbote 155
Verbringung in das Ausland 139
Verbuchung 109
– Eingeschränkt 97
– Geheim 100
– sonstige Nachgeordnete 99
– Streng Geheim 100
– Vertraulich 98
Verlässlichkeitsprüfungen 93
Verlust eines Schlüssels 165
Vernichtung
– bei Gefahr 182
– Dokumentation 183
– Eintragung in Registern 181
– multilateral klassifizierte
Informationen 177
– NATO RESTRICTED 178
– Streng Geheim 176
– Vertraulich/Geheim 175
Vernichtungsprotokoll 179
– Entfall 180
Versand 134
Verschwiegenheit 9
Verteilung 84
Verwahrung 15
– Einsatz 168
– Übungen 168

W

Wachauftrag 145
Wiederverwahrung 142
Wirkungsbereich 4

Z

Zentralregister 19
Zugang zu klassifizierten
Informationen 10

Zulassungsverfahren 16
Zuordnung 40
– Klassifizierungsstufe 25, 26
Zustellbücher 152