



Richtlinie zur Informationssicherheit

Fremdpersonal

- Einsatz von externem Personal (Beratung/Softwareentwicklung) -

Stand Datum:	25.04.2025
Version:	1.1
Status:	<input type="checkbox"/> in Bearbeitung <input type="checkbox"/> vorgelegt <input checked="" type="checkbox"/> abgenommen
Bearbeitung:	Van der Beek / stv. ISB
Eigentümerschaft:	Vangerow / ISB
Dokumenten-ID:	IS.ISB.ISR.019

Inhaltsverzeichnis

1.	Geltungsbereich und Vertraulichkeit.....	4
1.1.	Zielgruppe	4
1.2.	Geltungsbereich	4
1.3.	Einstufung	4
1.4.	Zuständigkeit und Revision.....	4
2.	Einleitung	5
3.	Allgemeine Regelungen unabhängig vom Ort der Leistungserbringung.....	6
3.1.	Verantwortlichkeit	6
3.2.	Vertragliche Regelungen	7
3.3.	Verpflichtung zur Verschwiegenheit	7
3.4.	Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH	7
3.5.	Verpflichtung des Fremdpersonals	8
3.5.1	Verpflichtung gemäß Verpflichtungsgesetz	8
3.5.2	Verpflichtung nach der Verschlusssachenanweisung des Bundes (VSA)	8
3.5.3	Verpflichtung nach dem Traffic Light Protocol (TLP).....	9
3.5.4	Erklärung der Kenntnisnahme zur Nutzung von BVA-Hardware	9
3.6.	Prüfung der Zuverlässigkeit / Sicherheitsüberprüfung	10
3.6.1	Erforderlichkeit eines Führungszeugnisses	10
3.6.2	Erforderlichkeit einer Sicherheitsüberprüfung	10
3.7.	Bereitstellung und Nutzung von Informationstechnik	11
3.7.1	Onboarding von Fremdfirmenpersonen.....	11
3.7.2	Nutzung des BVA E-Mail Service	12
3.8.	Sensibilisierung von Fremdpersonal.....	13
3.9.	Offboarding von Fremdfirmenpersonen	13
4.	Regelungen für die Leistungserbringung aus Liegenschaften des BVA	15
4.1.	Anmeldepflicht	15

4.2.	Ausweis-Tragepflicht	15
4.3.	Beaufsichtigung von Fremdpersonal.....	15
4.4.	Zutrittskontrolle	16
5.	Regelungen für die Leistungserbringung außerhalb von Liegenschaften des BVA....	17
6.	Anlagen.....	18
7.	Referenzen	18

1. Geltungsbereich und Vertraulichkeit

1.1. Zielgruppe

Dieses Dokument gilt für alle Beschäftigten im Bundesverwaltungsamt (BVA), in deren Fach-/Arbeitsbereichen (insbesondere im Rahmen der Softwareentwicklung und bei der Leistung von Beratungsaufträgen) externes Personal (Fremdpersonal) zur Aufgabenerfüllung eingesetzt wird. In dieser Richtlinie sind in diesem Zusammenhang verbindliche Vorgaben festgelegt. Für externes Personal im Bereich der Haustechnik und -sicherheit wird auf die ISR des Sachgebiets „Schutz und Sicherheit“ des Inneren Dienstes im Referat Z II 4 verwiesen.

1.2. Geltungsbereich

Dieses Dokument ist für den internen Gebrauch im BVA und für die Weitergabe an Unternehmen, die im Auftrag des BVA (IT-)Dienstleistungen erbringen bestimmt. Eine Vervielfältigung, Speicherung, Umformatierung, Übertragung und/oder Weitergabe bzw. Verteilung in elektronischer und/oder physikalischer Form, auch von Auszügen, an Personen/Firmen/Institutionen außerhalb des Geltungsbereiches bedarf der vorherigen Genehmigung der/des Informationssicherheitsbeauftragten (ISB) des BVA.

1.3. Einstufung

Für das vorliegende Dokument wird keine Einstufung nach der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) vorgenommen.

1.4. Zuständigkeit und Revision

Die Zuständigkeit für diese Richtlinie obliegt der/dem ISB BVA. Das Dokument ist entsprechend der jeweiligen IT-Sicherheitslage und Entwicklung fortzuschreiben. Die Richtlinie ist spätestens nach zwei Jahren einer Revision zu unterziehen.

Die Freigabe der Richtlinie erfolgt durch die Behördenleitung im BVA.

2. Einleitung

Externes Personal wird im Folgenden unter dem Begriff **Fremdpersonal** zusammengefasst, die zugehörigen Firmen werden als **beauftragte Unternehmen** bezeichnet. Für einzelne Personen wird der Begriff **Fremdfirmenperson** verwendet.

Mit dem Einsatz von Fremdpersonal im Sinne dieser Richtlinie ist ein spezifisches Gefährdungspotential verbunden. Fremdpersonal erhält in der Regel ein SINA Endgerät als IT-Arbeitsplatz oder hat über dedizierte Umgebungen wie die Softwareentwicklungsplattform ZSSI und entsprechende Einwahlmöglichkeiten für Fremdfirmen Zugriff auf schützenswerte Informationen. Fremdpersonal steht zwar außerhalb der dienstrechtlichen Steuerung und Kontrolle der beauftragenden Behörde, jedoch steht das Bundesverwaltungsamt als beauftragende Behörde weiterhin in der Verantwortung für die Vertraulichkeit, Integrität und Verfügbarkeit der Anwendungen, Daten und Informationen im Zugriff von Fremdpersonal.

Die vorliegende Richtlinie formuliert Anforderungen und Maßnahmen zum sicheren Einsatz von Fremdpersonal im BVA. Sie adressiert ausschließlich die Informationssicherheit. Die inhaltliche Steuerung des Einsatzes von Fremdpersonal, die Kontrolle der Arbeitsergebnisse oder die Ahndung von Minderleistungen obliegen den verantwortlichen Fach-/Arbeitsbereichen und werden in dieser Richtlinie nicht betrachtet.

Die Schlüsselworte (Modalverben) „MUSS“, „KANN“, „SOLLTE“, „SOLLTE NICHT“, „DARF NUR“ und „DARF NICHT“ haben, wie im IT-Grundschutz-Kompendium des BSI, die in RFC-2119 [Ref 01] definierte Bedeutung.

3. Allgemeine Regelungen unabhängig vom Ort der Leistungserbringung

3.1. Verantwortlichkeit

Je nach Anforderung und Beauftragung übernimmt Fremdpersonal unterschiedliche Aufgaben. Für jede Fremdfirmenperson MÜSSEN konkrete Ansprechpersonen innerhalb des BVA für alle Belange der Zusammenarbeit und Leistungserbringung benannt und dokumentiert werden. In der Regel sind dies die zuständigen Losmanagerinnen bzw. Losmanager (z. B. in den Referatsgruppen IT II und IT III). **Sollte es kein verantwortliches Losmanagement für eine Fremdfirmenperson geben (z. B. bei Beauftragung abseits eines BVA-Rahmenvertrages), MUSS der verantwortliche Fach-/Arbeitsbereich eine konkrete Ansprechperson vertraglich benennen. Die Verantwortlichkeiten, die gemäß dieser Sicherheitsrichtlinie dem Losmanagement zugeordnet werden, gelten insofern analog für diese vertraglich benannten Personen.** Folgende Tätigkeiten sind wahrzunehmen:

- Anwendung der in der vorliegenden Richtlinie beschriebenen Regelungen und Kontrolle der Einhaltung.
- Steuerung des On- und Offboarding Prozesses.
- Aufforderung der Fremdfirmenpersonen zur Durchführung der Lernmodule für Informationssicherheit, sofern dem Fremdpersonal IT-Arbeitsplätze des BVA zur Verfügung gestellt werden.
- Verpflichtung der Fremdfirmenpersonen nach der Verschlusssachenanweisung des Bundes (VSA) – falls erforderlich – sowie nach dem Traffic Light Protocol (TLP).
- Umsetzung der Informationssicherheitsrichtlinie „Sicherheitsüberprüfung“, sofern innerhalb der beauftragenden Organisationseinheit aufgrund der Einstufung der verarbeiteten Daten oder aufgrund der Kritikalität des betriebenen Verfahrens eine „Erweiterte Sicherheitsüberprüfung Ü2“ notwendig ist.
- Übergabe aller erforderlicher Vorgaben wie Informationssicherheitsrichtlinien und ggfs. individueller Regelungen für die Zusammenarbeit und die Leistungserbringung an die Fremdfirmenpersonen.
- Unterstützung des Antrags- und Genehmigungsverfahrens für die IT-Ausstattung sowie für die Ausgabe und den Entzug von Zutritts-, Zugangs- und Zugriffsberechtigungen.

- Die Beachtung der in der jeweils betroffenen Liegenschaft geltenden Meldungs-, Begleit- und Aufenthaltsregelungen, ggf. die Beantragung von Zutrittskarten.

3.2. Vertragliche Regelungen

Im vorgeschalteten Vergabeverfahren ist, soweit es vom BVA selbst durchgeführt wird, die Richtlinie zur Informationssicherheit Ausschreibungen, IT-Beschaffungen und Beauftragungen von Dienstleistungen für IT-Verfahren und dessen Anlagen zu beachten [Ref 08].

In den vertraglichen Regelungen MÜSSEN mindestens die folgenden Themen abgedeckt werden:

- Informationssicherheitsmanagementsystem/Meldepflichten
- Ort der Leistungserbringung (Mobiles Arbeiten und Telearbeit nur nach Zustimmung des AG)
- Geheimschutzbetreuung/ Nutzung von VS-IT
- Vereinbarung zur Auftragsverarbeitung
- Ggfs. einzelfallbezogene Regelungen zum Datenschutz, die nicht bereits Bestandteil der Auftragsverarbeitungsvereinbarung sind
- Haftung und Schadensersatz – insbesondere Ausschluss von haftungsausschließenden- oder mindernden Regelungen (z.B. in AGB)
- Bindung an diese Richtlinie zur Sicherheit Fremdfirmenpersonal

3.3. Verpflichtung zur Verschwiegenheit

Der Auftragnehmer ist zur Verschwiegenheit und zur Beachtung des Datenschutzes verpflichtet. Der Auftragnehmer sichert zu, dass er seine Mitarbeitenden hinsichtlich der zu bearbeitenden Aufgaben, Informationen, Unterlagen und Daten zur Verschwiegenheit und zur Beachtung des Datenschutzes verpflichtet hat. Die Pflicht zur Verschwiegenheit und zur Beachtung des Datenschutzes bleibt auch nach Beendigung der Rahmenvereinbarung bestehen. Die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) sowie der EU-Datenschutzgrundverordnung (EU-DSGVO) werden eingehalten.

3.4. Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades des VS-NUR FÜR DEN DIENSTGEBRAUCH

Bevor Fremdpersonal Zugang zu VS-NfD ermöglicht wird, muss mit dem Unternehmen (VS-NfD-Auftragnehmer) die Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades

VS-NUR FÜR DEN DIENSTGEBRAUCH abgeschlossen werden (Teil 1b der [Anl 3] dieser Richtlinie). Das verantwortliche Losmanagement tritt hier als VS-NfD-Auftraggeber auf.

3.5. Verpflichtung des Fremdpersonals

3.5.1 Verpflichtung gemäß Verpflichtungsgesetz

Jede Fremdfirmenperson MUSS gemäß Gesetz über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz, § 1 Abs. 1 Nr.1) auf die gewissenhafte Erfüllung ihrer Obliegenheiten verpflichtet und auf die strafrechtlichen Folgen einer Pflichtverletzung hingewiesen werden. Im Rahmen der förmlichen Verpflichtung MUSS dem Fremdpersonal die Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung zusammen mit dem Verhaltenskodex gegen Korruption [Anl 2b] ausgehändigt werden.

Falls IT III 5 oder D II 1 das zuständige Vertragsmanagement sind, werden diese Gespräche durch IT III 5 bzw. D II 1 vereinbart und mit der Fremdfirmenperson geführt. Die unterschriebene Niederschrift zur Verpflichtungserklärung [Anl 2] wird von IT III 5 bzw. D II 1 an den internen vertraglichen Ansprechpartner (z. B. Losmanager/Losmanagerin) übergeben. In allen anderen Fällen MUSS die Verpflichtung durch die jeweils vertraglich verantwortliche Person durchgeführt werden.

Die unterschriebene Niederschrift ist in jedem Fall im Anschluss an Z II 4 - SG Schutz und Sicherheit zu übersenden.

3.5.2 Verpflichtung nach der Verschlusssachenanweisung des Bundes (VSA)

Jeder Fremdfirmenperson, welche im Rahmen der Leistungserbringung Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH erhalten soll oder sich diesen verschaffen kann¹, MUSS das Merkblatt zur Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt, [Anl 3] dieser Richtlinie), verpflichtend zur Kenntnis gegeben werden. Fremdfirmen müssen im Rahmen der Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH eine konkrete Ansprechperson benennen, die diese Verpflichtung für die einzusetzenden Fremdfirmenpersonen durchführt. Die allgemeinen Hinweise (Teil 2 der [Anl 3] dieser Richtlinie), die Hinweise zur

¹ Durch die Nutzung eines SINA-Endgerätes ist diese Voraussetzung gegeben.

Nutzung von IT (Teil 3 der [Anl 3] dieser Richtlinie), die Hinweise zur Kennzeichnung (Teil 4 der [Anl 3] dieser Richtlinie) sowie die Behandlung von VS-NfD in der Privatwohnung (Teil 6 der [Anl 3] dieser Richtlinie) sind den verpflichteten Personen auszuhändigen.

Die Übersendung des Merkblatts an diese hierfür benannte Ansprechperson erfolgt durch die verantwortliche Losmanagerin / den verantwortlichen Losmanager. Der Nachweis der Verpflichtung (Teil 5 der [Anl 3] dieser Richtlinie) der jeweiligen Fremdfirmenpersonen muss von dieser zentralen Ansprechperson gegenüber dem Losmanagement per E-Mail bestätigt werden. Hierzu SOLL eine Kopie der unterschriebenen [Anl 3] dem Losmanagement zur dortigen Archivierung übergeben werden. Der Nachweis MUSS fünf Jahre nach dem Ausscheiden der betroffenen Person aus der Tätigkeit mit Bezug zu VS-NfD vernichtet werden. Eine frühere Vernichtung ist nicht zulässig.

Eine Arbeit mit Verschlussachen der Stufen VS-VERTRAULICH oder höher bedarf einer vorherigen Einzelabstimmung mit dem Geheimschutz des BVA.

3.5.3 Verpflichtung nach dem Traffic Light Protocol (TLP)

Sollten Fremdfirmenpersonen TLP-eingestufte Informationen be- oder verarbeiten und noch nicht vertraglich auf die Einhaltung des TLP im BVA verpflichtet worden sein, MÜSSEN sie ebenfalls die TLP-Verpflichtung [Anl 5] unterzeichnen. Die Aushändigung, die zeitnahe Rückforderung und die Aufbewahrung und Dokumentation der TLP-Verpflichtungen ist Aufgabe der verantwortlichen Losmanagerin / des verantwortlichen Losmanagers.

3.5.4 Erklärung der Kenntnisnahme zur Nutzung von BVA-Hardware

Für die Nutzung von Informationstechnik des BVA gelten die relevanten Dienstanweisungen und Sicherheitsrichtlinien gleichermaßen auch für Fremdfirmenpersonen. Die für die jeweiligen Fremdfirmenpersonen verantwortlichen Losmanagerinnen bzw. Losmanager MÜSSEN diesen die folgenden Regelungen zur Kenntnis geben:

- Richtlinie für Informationssicherheit Fremdpersonal
- Dienstanweisung IT-Arbeitsplatz [Ref 03]
- Richtlinie zur Informationssicherheit Nutzung von Kommunikations- und Kollaborationssysteme / Kommunikationsmatrix [Ref 04]
- Richtlinie zur Informationssicherheit Einsatz mobiler IT [Ref 05]
- Richtlinie zur Informationssicherheit Meldung von wichtigen Ereignissen [Ref 06]

- Richtlinie zur Informationssicherheit Passwortsicherheit [Ref 07]

Die jeweiligen Fremdfirmenpersonen MÜSSEN die Kenntnisnahme dieser Regelungen gegenüber dem Losmanagement mittels [Anl 4](unterschrieben oder mit qualifizierter elektronischer Signatur) bestätigen.

3.6. Prüfung der Zuverlässigkeit / Sicherheitsüberprüfung

3.6.1 Erforderlichkeit eines Führungszeugnisses

Sollte für Fremdpersonal im Rahmen einer Leistungserbringung der unbegleitete Zutritt zum nichtöffentlichen Bereich einer Liegenschaft des BVA erforderlich sein, MUSS eine Prüfung der Zuverlässigkeit erfolgen und diese durch ein Führungszeugnis zur Vorlage bei Behörden – Belegart O - nach § 30(5) Bundeszentralregistergesetz (BZRG) belegt werden. Durch die Begleitung von Fremdpersonal KANN das Erfordernis einer Zuverlässigkeitsprüfung entfallen.

3.6.2 Erforderlichkeit einer Sicherheitsüberprüfung

Sollte für Fremdpersonal im Rahmen einer Leistungserbringung der unbegleitete Zutritt zu einem Sicherheitsbereich des BVA erforderlich sein, MUSS je nach Sicherheitsbereich eine „erweiterte Sicherheitsüberprüfung (SÜ2)“ bzw. eine „erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (SÜ3)“ nach dem Sicherheitsüberprüfungsgesetz erfolgen. Durch die Begleitung von Fremdpersonal KANN das Erfordernis einer Sicherheitsüberprüfung entfallen.

Eine „Erweiterte Sicherheitsüberprüfung“ ist auch dann erforderlich, wenn die Vorgaben der Informationssicherheitsrichtlinie „Sicherheitsüberprüfung“ auf die beauftragende Organisationseinheit zutreffend sind.

Die Durchführung einer Sicherheitsüberprüfung ist durch das Losmanagement mit dem Geheimschutz BVA bzw. der/dem Sicherheitsbevollmächtigten einer Fremdfirma abzustimmen. Wenn die Fremdfirma durch eine Sicherheitsbevollmächtigte bzw. einen Sicherheitsbevollmächtigten nach dem Handbuch für den Geheimschutz in der Wirtschaft betreut wird, erfolgt die Durchführung durch das Bundesamt für Wirtschaft und Klimaschutz (BMWK). Die Beauftragung des BMWK zur Durchführung erfolgt in diesem Fall durch den Sicherheitsbevollmächtigten.

3.7. Bereitstellung und Nutzung von Informationstechnik

Sofern die Beauftragung einer Beratungsfirma über einen BVA-Rahmenvertrag erfolgt, MUSS das jeweilige Losmanagement gemäß den zu erledigenden Aufgaben unter Beachtung des Erforderlichkeitsprinzips über Art und Umfang der Nutzung von Informationstechnik sowie über die Bereitstellung von IT durch das BVA entscheiden. Bei einem Abruf abseits eines BVA-Rahmenvertrages (bspw. Kaufhaus des Bundes, 3PM) MUSS die beauftragende Leitung des Fach-/Arbeitsbereiches, in dem das Fremdpersonal eingesetzt wird, diese Entscheidung übernehmen. Weiterführende Informationen zur Ausgabe von BVA-Hardware an Externe sind [Ref 10] zu entnehmen.

3.7.1 Onboarding von Fremdfirmenpersonen

- Die Anforderung BVA-eigener Hardware und Benutzerkonten in der BVA-Domäne MUSS per IT-Antrag durch den Fach-/Arbeitsbereiches erfolgen.
- Benutzerkonten von Fremdfirmenpersonen MÜSSEN mit einer Befristung von höchstens 1 Jahr angelegt werden. Nach Ablauf eines Jahres werden diese Benutzerkonten automatisch deaktiviert. Sollte keine Verlängerung erfolgen, werden diese nach weiteren 3 Monaten gelöscht.
- Fremdpersonal DARF NUR mit BVA-Hardware ausgestattet werden, wenn entsprechende Voraussetzungen vorliegen (z.B. notwendige Zugriffe auf BVA-IT-Systeme, Entwicklungs- und Testumgebungen und/oder Bearbeitung von VS-NUR FÜR DEN DIENSTGEBRAUCH).
- Der Zugriff auf interne Laufwerke (z.B. Referats- oder Projektlaufwerke), das Intranet und weitere Interna ist nicht zulässig. Eine Ausnahmegenehmigung kann in begründeten Fällen beantragt werden. Ein Austauschlaufwerk KANN über einen IT-Antrag beantragt werden, dies bedarf keiner Ausnahmegenehmigung.
- Die Nutzung von IT-Systemen des beauftragten Unternehmens (Notebook, mobile Datenträger, E-Mail-System) zur Speicherung und Übertragung dienstlicher Daten des BVA oder dessen Kunden und Partner DARF NUR mit Zustimmung der Leitung des Fach-/Arbeitsbereiches, in dem das Fremdpersonal eingesetzt wird, erfolgen.
- Fremdpersonal DARF die bereitgestellten Arbeitsplatzsysteme, Token und Zugangsdaten NICHT an unberechtigte Dritte weitergeben oder zur Nutzung überlassen.
- Die Ausgabe von BVA-Hardware und SINA Token an Fremdfirmenpersonen MUSS, wenn es wirtschaftlich vertretbar ist, persönlich durch den Lokalen IT-Verantwortlichen (LIT) an einem Standort des BVA erfolgen. Sollte an einem Standort kein LIT vorhanden sein oder die

Übergabe wirtschaftlich unangemessen sein (z. B. bei Anreise aus dem Ausland), so können BVA-Hardware und SINA Token auch als **versicherter Versand** an einen hierfür explizit benannten und berechtigten Empfänger des Unternehmens versendet werden. SINA Token sind in diesen Fällen getrennt von der BVA-IT per Einschreiben mit persönlicher Übergabe zu versenden. Ein Versand an Postfächer, Poststellen, Pfortendienste etc. ist nicht zulässig.

- Nach Erhalt der Hardware und des SINA-Tokens muss von der entgegennehmende Fremdfirmenperson ein entsprechender Übergabebeleg quittiert werden. Sollte die entgegennehmende Person nicht die abschließend nutzende Fremdfirmenperson sein (z. B. bei Mitnahme von BVA-Hardware in Vertretung) oder die Übergabe per Versand erfolgen, so muss von der nutzenden Fremdfirmenperson ein (weiterer) Übergabebeleg unmittelbar nach Empfang der Hardware an das ITZBund (BVA-Uebergabebelege@itzbund.de) und das zuständige Losmanagement gesendet werden.
- Bei einer **geplanten** Abwesenheit einer Fremdfirmenperson von länger als 3 Monaten MUSS erhaltene BVA-Hardware an das BVA zurückgegeben werden.
- Für Maßnahmen bei Beendigung des Vertragsverhältnisses mit einer Fremdfirma oder dem Ausscheiden von Fremdfirmenpersonal aus einer Tätigkeit wird auf das Kapitel 3.9 verwiesen.

3.7.2 Nutzung des BVA E-Mail Service

Dem Fremdpersonal werden für die Tätigkeiten beim BVA / im Auftrag des BVA E-Mail-Konten bereitgestellt, sofern die Ausgabe von BVA-IT-Arbeitsplätzen an das Fremdpersonal erforderlich ist (siehe Kap. 3.6).

Die Zugehörigkeit eines BVA-E-Mail-Kontos zu einer Fremdfirmenperson MUSS erkennbar sein. Dazu MUSS die E-Mail-Adresse nach dem folgenden Muster erstellt werden:

`extern.Vorname.Nachname@bva.bund.de`

Fremdfirmenpersonen MÜSSEN sowohl für die BVA-interne als auch für die im Auftrag des BVA durchgeführte externe E-Mail-Kommunikation die Standard- Signatur ihrer externen Firma (ohne jegliche Zusätze wie „im Auftrag“ o.ä.) verwenden. Zusätzlich SOLLTE zu Beginn der E-Mail ein Hinweis erfolgen, dass es sich beim Absendenden nicht um einen Mitarbeitenden des BVA handelt, sondern für welches Unternehmen und in welchem Zusammenhang zum BVA die Kontaktaufnahme erfolgt.

Sollte eine Fremdfirmenperson bei begründeten Ausnahmen Zugriff auf ein Funktionspostfach des BVA erhalten, DARF ein Versand von E-Mails aus diesem Postfach NUR durch BVA Mitarbeiter mit BVA Signatur erfolgen.

Eine automatische Weiterleitung von E-Mails oder der Versand von Informationen zu eingegangenen E-Mails auf eine BVA-externe E-Mail-Adresse DARF NICHT erfolgen.

3.8. Sensibilisierung von Fremdpersonal

Fremdpersonal, welches IT-Systeme des BVA zur Verfügung gestellt bekommt, MUSS als Teil des Onboarding-Prozesses Online-Schulungen zur Informationssicherheit am Arbeitsplatz sowie zur Geheimschutzbelehrung innerhalb von 4 Wochen nach Erhalt der BVA-IT absolvieren². Sie sind durch das jeweilige zuständige Losmanagement auf die verpflichtende Bearbeitung hinzuweisen, die Durchführung der Lernmodule ist von den Fremdfirmenpersonen schriftlich gegenüber dem zuständigen Losmanagement zu bestätigen. Die Organisationseinheit Informationssicherheitsbeauftragter führt in regelmäßigen Abständen eine Kontrolle der Teilnahme durch und erinnert bei Bedarf an die fehlende Durchführung. Bei Nicht-Durchführung der Online-Sensibilisierung kann eine Sperrung der entsprechenden Benutzerkonten durch den ISB BVA veranlasst werden.

Sollte Fremdfirmenpersonal auch vor Ort in BVA-Liegenschaften tätig sein, so sind auch die Lernmodule für Arbeitsschutz und Brandschutz zu bearbeiten.

Die Online-Schulungen müssen jährlich wiederholt werden. Es erfolgt eine Protokollierung innerhalb der Lernumgebung über die erfolgreiche Bearbeitung eines Lernmoduls.

3.9. Offboarding von Fremdfirmenpersonen

Fremdpersonal DARF mit Beendigung des Auftrages KEINEN weiteren Zugriff auf die im Rahmen der Zusammenarbeit erhaltenen und erstellten Informationen haben. Hiervon ausgenommen sind Unterlagen, die für die Auftragnehmerin zur Sicherstellung von Gewährleistungsverpflichtungen erforderlich sind. Mit Beendigung des Vertragsverhältnisses MÜSSEN daher die folgenden Maßnahmen eingeleitet und deren Umsetzung dokumentiert werden:

² <https://ilias.bva.in.bund.de>

- Das Fremdpersonal MUSS sämtliche Arbeitsergebnisse, alle erhaltenen und ggf. erstellten Unterlagen (z. B. behördeninterne Dokumentationen, Revisionsunterlagen) und Betriebsmittel (z. B. Speichermedien) an die bedarfstragende Person / Organisationseinheit übergeben.
- Sämtliche in IT-Verfahren vergebenen Zugangs- und Zugriffsrechte MÜSSEN durch das zuständige Losmanagement entzogen werden, dem Fremdpersonal zur Kenntnis gelangte Passwörter MÜSSEN geändert werden.
- Die Löschung ausgehändigter Zutrittskarten, Zutrittsberechtigungen und Parkberechtigungen MUSS durch das zuständige Losmanagement veranlasst werden. Bereitgestelltes Material des BVA (Hardware, Software, Büromaterial) MUSS eingezogen werden.
- Das zuständige Losmanagement MUSS einen IT-Antrag zur Rückgabe der Hardware und SINA Token sowie zur Löschung des Accounts stellen, die ordnungsgemäße Rückgabe an das ITZ-Bund gewährleisten, quittieren und dokumentieren. Ein Verbleib zurückgegebener BVA-IT innerhalb der verantwortlichen Organisationseinheit ist nicht zulässig.
- Bei der Nutzung biometrischer Erkennungsverfahren (z. B. Iris Scanner, Fingerabdrücke und Handrückenenerkennung) MÜSSEN die gespeicherten biometrischen Daten gelöscht werden.
- Das Fremdpersonal MUSS durch das zuständige Losmanagement explizit darauf hingewiesen werden, dass die Auflagen gemäß Kap. 3.3 auch nach Beendigung der Tätigkeit weiterhin Bestand haben.

Sämtliche mit Sicherheitsaufgaben betraute Organisationseinheiten, insbesondere der BVA-Geheimschutz und das Sachgebiet „Schutz und Sicherheit“ des Inneren Dienstes MÜSSEN durch das zuständige Losmanagement über die Beendigung des Vertragsverhältnisses / den Projektabschluss o. Ä. und den endgültigen Weggang des Fremdpersonals unterrichtet werden.

4. Regelungen für die Leistungserbringung aus Liegenschaften des BVA

4.1. Anmeldepflicht

Benötigt Fremdpersonal zur Erfüllung seiner Aufgaben Zutritt zu Liegenschaften des BVA, MUSS das zuständige Losmanagement dies mit ausreichend zeitlichem Vorlauf dem Referat Z II 4, Sachgebiet Schutz und Sicherheit (sicherheit@bva.bund.de) melden und die Zutrittsberechtigung mit [Anl 1] beantragen.

Ad-Hoc- und Noteinsätzen von Fremdpersonal außerhalb der regulären Servicezeit MÜSSEN unverzüglich dem Referat Z II 4- SG Schutz und Sicherheit per E-Mail gemeldet werden.

4.2. Ausweis-Tragepflicht

Referat Z II 4 - Sachgebiet Schutz und Sicherheit KANN für Fremdpersonal die Pflicht zum Tragen eines Besucher- oder Hausausweises in nicht öffentlichen Bereichen einer Liegenschaft des BVA veranlassen.

Besteht diese Pflicht, MUSS die Leitung des Fach-/ Arbeitsbereiches, in dem das Fremdpersonal eingesetzt wird, die Einhaltung und korrekte Umsetzung sicherstellen und überwachen.

4.3. Beaufsichtigung von Fremdpersonal

Sofern keine Zuverlässigkeitsprüfung oder Sicherheitsüberprüfung des Fremdpersonals gemäß Kap.3.6 vorliegt, MÜSSEN Fremdfirmenpersonen grundsätzlich im gesamten internen, nicht öffentlichen Bereich der Liegenschaften des BVA begleitet und beaufsichtigt werden. Dabei gelten die folgenden Regelungen:

- Eine vom Fach-/Arbeitsbereich benannte Betreuungs-/Begleitperson MUSS während der Dauer des Besuches/Einsatzes für die Betreuung, Einweisung und ständige Begleitung des Fremdpersonals im gesamten internen, nicht öffentlichen Bereich der Behörde sowie für die Einhaltung bestehender Regelungen die persönliche Verantwortung übernehmen.
- Sofern Sicherheitsbereiche betreten werden müssen, MUSS die Begleitperson eigenständig zutrittsberechtigt sein. Werden Arbeiten in Sicherheits- oder sensiblen Bereichen durchgeführt, SOLLTE die Begleitperson annähernd fachlich versiert sein, um mögliche nicht durch den Auftrag zu begründenden Tätigkeiten (Manipulationen) zu erkennen und zu verhindern.

- Nicht auf das VS-NfD-Merkblatt verpflichtetes Fremdpersonal, das an VS-IT arbeitet, MUSS während der gesamten Zeit begleitet und beaufsichtigt werden. Die begleitenden Personen SOLLTEN annähernd über die notwendigen Fachkenntnisse verfügen, um die Tätigkeiten kontrollieren zu können.
- In begründeten Einzelfällen sind Ausnahmen von dieser Regelung mit dem Geheimschutz BVA, ISB BVA und dem SG Schutz und Sicherheit über den zuständigen Fach-/Arbeitsbereich, in dem das Fremdpersonal eingesetzt wird, abzustimmen.

4.4. Zutrittskontrolle

Für Fremdpersonal, für das keine Begleitpflicht vorliegt, KANN das Losmanagement ein personifiziertes Zutrittsmittel für die Einsatzdauer im BVA beantragen. Zutrittsrechte MÜSSEN dabei gemäß dem Erforderlichkeitsprinzip vergeben werden.

Fremdpersonal MUSS das Zutrittsmittel jeweils zu Dienstbeginn beim Betreten des Dienstgebäudes empfangen und nach Dienstende beim Verlassen wieder zurückgeben. Ist ein Empfang mit Sicherheitsdienstmitarbeiter vorhanden, erfolgt die Aus- und Rückgabe an dieser Stelle, ansonsten im entsprechenden Arbeits-/Fachbereich. Empfang und Rückgabe MÜSSEN dokumentiert werden. Der Verlust von Zutrittsmitteln muss umgehend dem SG Schutz und Sicherheit gemeldet werden.

Bei Liegenschaften, deren Zutritt durch einen Sicherheitsdienst kontrolliert wird, MÜSSEN Ausgabe, Entzug und Verwaltung der Zutrittsmittel für Fremdpersonal durch das zugehörige Sicherheits-Personal erfolgen. Die Ausgabe eines Zutrittsmittels durch den Sicherheitsdienst DARF NUR nach der Identifikation der Person über einen Personalausweis erfolgen.

5. Regelungen für die Leistungserbringung außerhalb von Liegenschaften des BVA

Wenn der mit der beauftragten Fremdfirma geschlossene Vertrag sowie die dort geltenden internen Vorgaben dies erlauben, DARF Fremdpersonal mit BVA-Hardware von folgenden Orten außerhalb von Liegenschaften des BVA Leistungen für das BVA erbringen:

- In den Räumlichkeiten des beauftragten Unternehmens. Befindet sich das Unternehmen im EU-Ausland, ist die Arbeit mit BVA-Hardware nur dann zulässig, wenn ein Geheimschutzabkommen zwischen der BRD und dem jeweiligen Einsatzland des Fremdpersonals vorliegt.
- In Telearbeit / aus dem Home-Office, sofern sich der häusliche Arbeitsplatz innerhalb der Bundesrepublik Deutschland befindet.
- Ortsungebunden (z.B. im Zug oder im Hotel) innerhalb der Bundesrepublik Deutschland

Alle Informationen zum Projekt und Bedarfsträger, jedwede Daten des Bedarfsträgers beim Auftragnehmer z. B. Echtdaten oder Zwischenstände der Inhalte der Systeme, Konzepte und der Software insbesondere der gesamte oder Teile des Quellcodes sind vor jedem unbefugten internen wie externen Zugriff mit geeigneten technischen, organisatorischen und infrastrukturellen Maßnahmen zu schützen.. Der Auftragnehmer stellt sicher, dass alle relevanten Informationen nur Befugten zur Kenntnis gelangen. Die Kontrolle der Einhaltung obliegt dem beauftragten Unternehmen. Das BVA hat das Recht, diese Maßnahmen jederzeit und in Stichproben zu überprüfen bzw. die Erläuterung dieser Maßnahmen einzufordern. Die erforderlichen Maßnahmen müssen durch den Auftragnehmer unverzüglich umgesetzt werden.

Für bestimmte Tätigkeiten KANN die/der Informationssicherheitsbeauftragte oder die/der Geheimschutzbeauftragte die Leistungserbringung von bestimmten Orten untersagen bzw. auf bestimmte Orte begrenzen.

6. Anlagen

Anlage	Inhalt
[Anl 1]	Antrag zum Betreten einer Liegenschaft des Bundesverwaltungsamtes
[Anl 2]	Niederschrift über die förmliche Verpflichtung nichtbeamteter Personen
[Anl 2a]	Auszüge aus dem Strafgesetzbuch
[Anl 2b]	Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung vom 30.07.2004 und Verhaltenskodex gegen Korruption
[Anl 3]	VS-NfD-Merkblatt – Anlage 4 zum Geheimschutzhandbuch der Wirtschaft
[Anl 4]	Bestätigung der Kenntnisnahme von BVA-Richtlinien bei Nutzung von BVA-IT
[Anl 5]	Verpflichtung auf das Traffic Light Protocol (TLP)

7. Referenzen

Referenz	Dokument / Link / Quelle
[Ref 01]	RFC 2119 – Verwendung von Schlüsselworten (englisch) Zu finden unter https://www.rfc-editor.org/rfc/rfc2119 (Stand 07/2023)
[Ref 02]	Mitarbeiteranweisungen „Verhalten bei Gefahr und im Alarmfall“ (Liegenschafts-bezogen) https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Navknoten&id=3116
[Ref 03]	Dienstanweisung IT-Arbeitsplatz https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Attachment&id=51457
[Ref 04]	Richtlinie zur Informationssicherheit Nutzung von Kommunikations- und Kollaborationssysteme / Kommunikationsmatrix https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Attachment&id=51239
[Ref 05]	Richtlinie zur Informationssicherheit Einsatz mobiler IT https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Attachment&id=51190
[Ref 06]	Richtlinie zur Informationssicherheit Meldung von wichtigen Ereignissen https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Attachment&id=55541
[Ref 07]	Richtlinie zur Informationssicherheit Passwortsicherheit https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Attachment&id=66896

Referenz	Dokument / Link / Quelle
[Ref 08]	Richtlinie zur Informationssicherheit Ausschreibung, IT-Beschaffung und Beauftragung von Dienstleistungen für IT-Verfahren https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Attachment&id=60767
[Ref 09]	Richtlinie zur Informationssicherheit Traffic Light Protocol im BVA
[Ref 10]	Hinweise zur Ausgabe von BVA-Hardware an Externe https://confluence.zssi.bva.in.bund.de/display/REFW028/Ausgabe+SINA+Laptop+an+externe+Mitarbeitende