

**TLP:CLEAR**

Richtlinie zur Informationssicherheit

# Software-Entwicklung

|                     |   |
|---------------------|---|
| <b>Stand Datum:</b> | 21. Januar 2025   |
| <b>Version:</b>     | 2.0   |
| <b>Status:</b>      | <input type="checkbox"/> in Bearbeitung<br><input type="checkbox"/> vorgelegt<br><input checked="" type="checkbox"/> abgenommen |

# Inhaltsverzeichnis

|           |  |           |
|-----------|--|-----------|
| <b>1.</b> | <b>Geltungsbereich und Vertraulichkeit.....</b>  | <b>4</b>  |
| 1.1.      | Zielgruppe .....   | 4         |
| 1.2.      | Geltungsbereich.....   | 4         |
| 1.3.      | Einstufung .....   | 4         |
| 1.4.      | Zuständigkeit und Revision.....  | 4         |
| 1.5.      | Ausnahmen von dieser Richtlinie .....  | 4         |
| <b>2.</b> | <b>Zusammenfassung .....</b>   | <b>5</b>  |
| <b>3.</b> | <b>Anforderungen an die Informationssicherheit .....</b>   | <b>6</b>  |
| 3.1.      | Einsatz der Richtlinie im Projektverlauf.....  | 6         |
| 3.2.      | Grundlage und Verpflichtung zur Anwendung der Anforderungen .....  | 6         |
| 3.3.      | Zusammenstellung der Anforderungen an die Informationssicherheit .....   | 7         |
| 3.4.      | Anhang zur Richtlinie: Aufbau der Anforderungsscheckliste .....  | 8         |
| 3.5.      | Synergien zum Sicherheitskonzept.....  | 10        |
| <b>4.</b> | <b>Erläuterungen, Hilfestellungen und Anwendungshinweise.....</b>  | <b>11</b> |
| 4.1.      | Hilfestellung der/des ISB zu Schutzbedarf und Einstufung.....  | 11        |
| 4.2.      | Hilfestellungen zur Anforderungsscheckliste .....  | 11        |
| 4.2.1     | Hilfestellung „Umsetzungs-Beispiele“ .....   | 11        |
| 4.2.2     | Hilfestellung „Antwortaufbau“ .....  | 11        |
| 4.2.3     | Auslegung der Modalverben „MUSS / DARF NUR / SOLLTE“ .....   | 11        |
| 4.3.      | Anwendungshinweise zur Anforderungsscheckliste.....  | 12        |
| 4.3.1     | Vereinfachende Anwendungshinweise.....   | 12        |
| 4.3.2     | Anwendungshinweis 1: Standardsortierung als „sicherheitstechnischer Leitfaden“ .....   | 12        |
| 4.3.3     | Anwendungshinweis 2: Einteilung der Anforderungen nach Phasen .....  | 12        |
| 4.3.4     | Anwendungshinweis 3: Anforderungen nach Priorisierung .....  | 13        |
| 4.3.5     | Anwendungshinweis 4: „Zielgruppe“ - Anforderungen gemäß Outsourcing / Auftraggeber- und<br>Auftragnehmer-Verhältnisses ..... | 13        |
| 4.3.6     | Anwendungshinweis 5: Anwendung nur relevanter Anforderungen .....  | 14        |
| 4.4.      | FAQ / Weitere Fragestellungen bei der Anwendung der Richtlinie.....  | 15        |

|           |                             |           |
|-----------|-----------------------------|-----------|
| <b>5.</b> | <b>Anhang.....</b>          | <b>17</b> |
| 5.1.      | Glossar.....                | 17        |
| 5.2.      | Abkürzungsverzeichnis ..... | 17        |
| 5.3.      | Referenzen .....            | 18        |
| 5.4.      | Anlagen .....               | 18        |

# **1. Geltungsbereich und Vertraulichkeit**

## **1.1. Zielgruppe**

Diese Richtlinie gilt für alle BVA-Beschäftigten, die unmittelbar im Bereich der Software-Entwicklung tätig sind. Darüber hinaus gilt sie insbesondere für die im BVA tätigen externen Dienstleistungsunternehmen und ihre Beschäftigten, die in der Umsetzung, Unterstützung und Steuerung von Projekten im Bereich der Software-Entwicklung tätig sind.

## **1.2. Geltungsbereich**

Dieses Dokument ist ausschließlich für den internen Gebrauch im BVA bestimmt. Im Rahmen der Beauftragung externer Dienstleister für die Software-Entwicklung darf diese Richtlinie auch Dritten zur Verfügung gestellt werden. Eine anderweitige Vervielfältigung, Speicherung, Umformatierung, Übertragung, Weitergabe bzw. Verteilung in elektronischer/physikalischer Form, auch von Auszügen, bedarf der vorherigen Genehmigung der/des Informationssicherheitsbeauftragten (ISB) des BVA.

## **1.3. Einstufung**

Das vorliegende Dokument ist nach Traffic Light Protocol (TLP) als TLP:GREEN eingestuft. Die Anforderungsscheckliste [Anl. 01] ist bei Befüllung als TLP:AMBER einzustufen.

## **1.4. Zuständigkeit und Revision**

Die Zuständigkeit für diese Richtlinie obliegt IT I 1 als Mitglied im Koordinierungsgremium Informationssicherheit (KoI). Das Dokument ist entsprechend der jeweiligen Informationssicherheitslage und Entwicklung fortzuschreiben. Die Richtlinie ist spätestens nach zwei Jahren einer Revision zu unterziehen. Die Freigabe der Richtlinie erfolgt durch die Behördenleitung im BVA.

## **1.5. Ausnahmen von dieser Richtlinie**

Die Richtlinie basiert auf verpflichtenden Vorgaben des „Umsetzungsplan Bund“, „Leitlinie für Informationssicherheit in der Bundesverwaltung (UP Bund)“ [Ref 3], auf den im Kapitel 3.2 eingegangen wird. Anfragen zur Umsetzung dieser Richtlinie müssen schriftlich an die Informationssicherheitsbeauftragte/den Informationssicherheitsbeauftragten des BVA gestellt werden. Die Bitte um Ausnahme oder Befreiung von einzelnen Vorgaben unterliegt dem Prozess zur Behandlung von Ausnahmen. Die/Der Informationssicherheitsbeauftragte lehnt die Anfrage ab, erteilt eine Ausnahme oder erteilt eine Ausnahme mit Auflage.

## **2. Zusammenfassung**

Die Berücksichtigung von Sicherheitsaspekten bei der Software-Entwicklung ist von wesentlicher Bedeutung für die Sicherheit der Software sowie der verarbeiteten Daten und Prozesse. Eine systematische Integration von Sicherheitsaspekten im Software-Entwicklungsprozess führt zu einer Verbesserung des Schutzniveaus sowie zu einer Optimierung des Informationssicherheitsmanagementsystems (ISMS) im BVA insgesamt.

Im Bundesverwaltungsamt werden Softwareprodukte entweder eigenentwickelt, im Rahmen einer Ausschreibung an externe Dienstleister vergeben oder eingekauft und gegebenenfalls angepasst. Der Großteil der Software-Entwicklungsprojekte im BVA sind Entwicklungen durch Dritte im Auftrag des BVA, daher liegt regelmäßig ein Auftraggeber-Auftragnehmer-Verhältnis vor und der Fokus dieser Richtlinie liegt auf solche Vorhaben.

Die Richtlinie stellt eine erste Auswahl der Anforderungen an die Informationssicherheit zusammen und versucht durch Hilfestellungen das Projekt von Beginn an bei der Erfüllung der Anforderungen zu unterstützen. Einen wesentlichen Bestandteil dieser Richtlinie bildet die Anforderungscheckliste [Anl 01] mit einem Anforderungskatalog, basierend auf dem IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Grundlage zur Anwendung der Anforderungen des BSI IT-Grundschutzes ist in „Umsetzungsplan Bund“, „Leitlinie für Informationssicherheit in der Bundesverwaltung“ (UP Bund)“ [Ref 02] verbindlich formuliert und festgelegt. Das Bundeskabinett hat am 19.07.2017 die Neukonzeption des

„Umsetzungsplan Bund 2017“ zur Steuerung und Umsetzung der Informationssicherheit in der Bundesverwaltung beschlossen. Dieser „Umsetzungsplan Bund 2017“ (UP Bund) tritt mit Wirkung vom 01.09.2017 in Kraft und formuliert die folgenden, verbindlichen Vorgaben, die auch für die Software-Entwicklung des BVAs gelten:

- „Die Festlegung der Mindestanforderungen erfolgt auf Basis der Standards für IT-Grundschutz des BSI in der jeweils gültigen Fassung.“
- „Bei der Durchführung von IS-Revisionen sind die Regelungen aus dem Leitfaden des BSI für die IS-Revision auf der Basis des IT-Grundschutzes zu beachten.“
- „Der Auftraggeber verpflichtet den IT-Dienstleister dazu, für die Bereiche der vertraglich bzw. in der Verwaltungsvereinbarung geschuldeten Leistungserbringung Informationssicherheitskonzepte auf der Basis von BSI-IT-Grundschutz zu erstellen, diese mit der auftraggebenden Seite abzustimmen und über die gesamte Dauer der Leistungserbringung ununterbrochen aufrecht zu erhalten und aktuell zu halten.“

Das BVA spiegelt diese wie auch weitere gesetzliche und datenschutzrechtliche Vorgaben in seiner Leitlinie [Ref 03] wider.

Die Detailtiefe und Rahmenbedingungen für die Erstellung der Sicherheitskonzeption und das konkretere Vorgehen wird durch die anzuwendenden BSI - IT-Grundschutz Standards 200-x verbindlich vorgegeben.

### **3.3. Zusammenstellung der Anforderungen an die Informationssicherheit**

Diese Richtlinie unterstützt das Vorhaben bei der Erfüllung der Anforderungen des BSI IT-Grundschutz-Kompodium [Ref 01] durch Berücksichtigung entsprechender Bausteine für die Software-Entwicklung, welche im Rahmen der Erstellung des Informationssicherheitskonzeptes bearbeitet werden müssen. Die Anforderungen dieser Sicherheitsrichtlinie betrachten die Grundschutzbausteine, die grundsätzlich für jedes Software-Entwicklungsvorhaben umzusetzen sind:

- [CON.8 Software-Entwicklung](#) → Fokus liegt auf Seite der AN
- [OPS 1.1.6 Software-Tests und Freigaben](#)
- [APP.7 Entwicklung von Individualsoftware](#) → Fokus liegt auf Seite der AG

Zusätzlich berücksichtigt die Richtlinie die nachfolgenden konkretisierten Anforderungen, die bei der Software-Entwicklung von Webanwendungen beachtet werden müssen:

- [CON.10 Entwicklung von Webanwendungen](#)

Weitere Standards wie die nachfolgend aufgeführten sind nicht Bestandteil dieser Richtlinie, jedoch als weitere Hilfsmittel im Rahmen einer sicheren Softwareentwicklung ausdrücklich empfohlen.

- [NIST Standard „Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems“](#)
- [OWASP Top 10](#)
- [OWASP Secure Software Development Lifecycle \(S-SDLC\)](#)
- [OWASP Code Review Guide](#)
- [OWASP Software Assurance Maturity Model](#)
- [BSI-Leitfaden für Auftraggeber zur Entwicklung sicherer Webanwendungen](#)
- [BSI-Leitfaden für Auftragnehmer zur Entwicklung sicherer Webanwendungen](#)
- [BSI - Sicherheit von Webanwendungen - Maßnahmenkatalog und Best Practices](#)

Anforderungen aus weiteren Vorgaben des BVA wie u. a.

- Basis-Kryptokonzept BVA
- Datenschutzkonzept BVA
- Informationssicherheitsrichtlinie „Ausschreibung, IT-Beschaffung und Beauftragung von Dienstleistungen für IT-Verfahren“ (Outsourcing)

gelten unverändert.

Die aus dem Blickwinkel dieser Richtlinie relevanten Anforderungen werden im Anhang „Anforderungscheckliste“ [Anl 01] zusammengestellt.

In ihrer Standardsortierung der „Anforderungscheckliste“ kann die Spalte „Anforderung“ auch als sicherheitstechnischer Leitfaden gelesen werden“. Die Liste der Anforderungen ist dann nach Phasen und Themen strukturiert.

### **3.4. Anhang zur Richtlinie: Aufbau der Anforderungscheckliste**

Die Anforderungscheckliste behandelt u.a. folgende Inhalte und Anforderungen, die hier nach Projektphasen dargestellt werden:

#### **Vorbereitung**

- Einbeziehung aller relevanten Ansprechpersonen
- Vorbereitung der Ausschreibungsunterlagen
- Feststellung des Schutzbedarfs



## **Definition / Planung**

- Auswahl eines Vorgehensmodells
- Definition von Zuständigkeiten / Verantwortlichkeiten
- Erstellung eines Projektplans / Sicherheitsprojektplans
- Aufstellung aller funktionalen / nicht funktionalen und Sicherheits-Anforderungen
- Durchführung einer Bedrohungsanalyse
- Aufbau einer Dokumentationsstruktur
- Beschreibung des Objektmodells
- Erstellung Testkonzept
- Erstellung Rollen- und Berechtigungskonzept
- Erstellung Fehlerbehandlungskonzept

## **Design und Entwicklung der Software**

- Sicherheit und Versionsverwaltung des Quellcodes
- Autorisierung und Authentisierung
- Umsetzung der Anforderungen der Bedrohungsanalyse
- Verwendung von Bibliotheken
- Sicherheit der Entwicklungsumgebung
- Vorgaben zur Entwicklung von Webanwendungen

## **Tests / Freigabe**

- Rahmenbedingungen für Tests
- Testverfahren und Auswahl von Testfällen
- Dokumentation von Tests
- Freigabeprozess und Abnahmeplanung
- Patch-Management

### **3.5. Synergien zum Sicherheitskonzept**

Für Anwendungen, die vom BVA entwickelt oder bei der Entwicklung begleitet werden, muss ein Sicherheitskonzept nach BSI-Vorgaben erstellt werden.

Das Sicherheitskonzept stellt die sicherheitstechnischen Anforderungen für die Projekte aus verschiedenen Blickwinkeln zusammen. Diese Anforderungen müssen durch das Projekt erfüllt werden. Idealerweise sind die Anforderungen bereits vor Beginn einer Entwicklung bekannt, da eine Umsetzung im Nachhinein einen vielfach höheren Aufwand und einen verringerten Schutz nach sich ziehen könnte.

Das Sicherheitskonzept formalisiert und dokumentiert den Umsetzungsstand bezüglich der sicherheitstechnischen Anforderungen. Es dient als kontrollierendes, den Status bestimmendes Instrument und unterstützt das Risikomanagement.

Die „Anforderungscheckliste“ [Anl 01] liefert als Anhang zu dieser Sicherheitsrichtlinie eine erste Auswahl aus diesen Anforderungen. Diese greifen zum größten Teil die Inhalte auf, die für das Sicherheitskonzept unter Anwendung des BSI IT-Grundschutzes benötigt werden. Durch die Beibehaltung des Bezugs zu den entsprechenden Bausteinen des BSI IT-Grundschutz-Kompendium können die Ergebnisse bei der Erstellung des Sicherheitskonzeptes im Rahmen des Grundschutzchecks leicht zugeordnet werden. Aus Sicht des BSI IT-Grundschutz-Kompendiums werden aus den jeweiligen Anforderungen jedoch nur Teilanforderungen sehr themengerichtet und sehr gezielt ausgewählt, um eine fokussierte Bearbeitung zu ermöglichen. Weitere Blickwinkel und (Teil-)Anforderungen werden bis zur Bearbeitung im Sicherheitskonzept zunächst zurückgestellt.

Ein kleiner Teil der Anforderungen resultiert aus anderen Vorgaben, wie BSI Leitfäden und Richtlinien des BVA.

## **4. Erläuterungen, Hilfestellungen und Anwendungshinweise**

### **4.1. Hilfestellung der/des ISB zu Schutzbedarf und Einstufung**

Der Schutzbedarf gemäß BSI IT-Grundsatz-Vorgehensweise ist zu Beginn eines jeden Projektes auf Seiten der auftraggebenden, fachlich zuständigen Stelle als Dateneigentümer im BVA oder – sofern zutreffend – über die jeweilige Kundenbehörde einzuholen. Für die Erhebung des Schutzbedarfes ist die im BVA veröffentlichte Vorlage zu verwenden. Diese Vorlage stellt die/den ISB des BVA zur Verfügung. Die Abnahme der Schutzbedarfsfeststellung erfolgt in letzter Instanz durch die/den ISB. Im Zuge der Schutzbedarfsfeststellung ist eine Einstufung der zu verarbeitenden Daten gemäß der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung VSA) zu erfragen bzw. durch die fachlich zuständige Stelle vorzugeben. Im Falle einer Einstufung ist die/der Geheimschutzbeauftragte des BVA in der Abnahme zu beteiligen. Dies wird durch die/den ISB sichergestellt.

### **4.2. Hilfestellungen zur Anforderungscheckliste**

#### **4.2.1 Hilfestellung „Umsetzungs-Beispiele“**

Es wurden „Umsetzungs-Beispiele“ entwickelt, die eine mögliche Umsetzung/Beantwortung der Anforderung darstellen. Es handelt sich hier lediglich um Beispiele, um einen realen Bezug zu den teils abstrakten Anforderungen des BSI herzustellen.

#### **4.2.2 Hilfestellung „Antwortaufbau“**

Die Hilfestellung „Antwortaufbau“ kann als Checkliste und als Anhaltspunkte gesehen werden, um die konkreten Inhalte der eigenen Umsetzung zu beschreiben. Als Hilfestellung ist hier aufgeführt, welche Inhalte die Antworten im Idealfall haben sollten. In abstrakter Form sind für eine Menge von potenziellen Umsetzungs-Typen die empfohlenen, darzustellenden Inhalte in Stichpunkten aufgeführt.

Weiterhin kann diese Hilfestellung bei der Formulierung und Ausarbeitung weiterer Umsetzungsbeispiele helfen.

#### **4.2.3 Auslegung der Modalverben „MUSS / DARF NUR / SOLLTE“**

Zu den in den Anforderungen genutzten Modalverben „MUSS / DARF NUR“ ist zu erläutern, dass dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss. Das Modalverb „SOLLTE“ bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden. Unter einer stichhaltigen Begründung ist zu verstehen, dass nachgewiesen wird, dass Maßnahmen ergriffen wurden, die in ihrer Stärke der Mechanismen und Schutzwirkung gleichwertig oder höherwertig sind.

## **4.3. Anwendungshinweise zur Anforderungsscheckliste**

### **4.3.1 Vereinfachende Anwendungshinweise**

Diese Richtlinie beinhaltet mehrere, vereinfachende Anwendungshinweise. Die Anwendungshinweise sollen durch Aufteilung und gezielte Selektion die zu bearbeitenden Anforderungs-„Pakete“ in eine handhabbare Größe bringen. Die Aufteilung erfolgt dabei nach:

- Phasen
- Art der Anforderung
- Priorisierung
- nach „Zielgruppe“ - Anforderungen gemäß eines Auftraggeber- und Auftragnehmer-Verhältnisses
- Anwendung nur relevanter Anforderungen

Die Anzahl der Anforderungen, die im jeweiligen Bearbeitungsschritt erfüllt werden müssen, kann somit auf ein jeweils angepasstes, im entsprechenden Bearbeitungsschritt für das Vorhaben handhabbares Maß begrenzt werden.

### **4.3.2 Anwendungshinweis 1: Standardsortierung als „sicherheitstechnischer Leitfaden“**

Die Standardsortierung der Anforderungsscheckliste erfolgt nach der Spalte „ID“. Die Liste der Anforderungen ist dann nach Phasen und Themen strukturiert. Die Spalte „Anforderung“ kann in dieser Sortierung auch als „sicherheitstechnischer Leitfaden“ gelesen werden.

### **4.3.3 Anwendungshinweis 2: Einteilung der Anforderungen nach Phasen**

Die Richtlinie bietet eine Einteilung in Phasen, die zu einzelnen Projektphasen passen. Die ISR ist aufgeteilt in die folgenden Phasen:

1. Vorbereitung
2. Definition / Planung
3. Design
4. Entwicklung
5. Test / Freigabe

Dies erfolgt durch einen Filter auf die Spalte „Phase“. Die Phase gibt an, bis wann die Anforderung spätestens bearbeitet werden sollte. Sie gibt keine Auskunft über den frühesten Zeitpunkt der Bearbeitung, es muss ausdrücklich nicht alles zu Projektbeginn erfüllt werden.

Die vorausgefüllte Phasenzuteilung der Anforderungen ist nicht als Vorgabe, sondern als Vorschlag zu betrachten und sollte bei Bedarf angepasst werden.

#### **4.3.4 Anwendungshinweis 3: Anforderungen nach Priorisierung**

Wie bei den Phasen ist auch die Priorisierung keine Vorgabe und dient den Projekten als individuelles Hilfsmittel bzw. Projektsteuerungsinstrument.

Je nach Projekt und speziell Projektfortschritt sollten bestimmte Anforderungen vorrangig umgesetzt werden, es besteht jedoch kein direkter Zusammenhang mit der Projektphase. Es wird allerdings empfohlen die Priorisierung so zu gestalten, dass die jeweiligen Anforderungen innerhalb der zugehörigen Phase erfüllt werden. Wird von dieser Empfehlung abgewichen, so sollte eine kompensierende Planung erfolgen, die etwaige Lücken schließt.

Die Priorisierung ist somit ein Projektsteuerungsinstrument, dass kontinuierlich angepasst werden muss, jedoch eine weitsichtige Planung ermöglichen kann.

#### **4.3.5 Anwendungshinweis 4: „Zielgruppe“ - Anforderungen gemäß Outsourcing / Auftraggeber- und Auftragnehmer-Verhältnisses**

Ein „Filter nach Zielgruppe“ kann dann sinnvoll sein, wenn es sich um eine BVA-externe Entwicklung handelt. Fragestellung ist hier, wo sich die Grenze bezüglich der Aufgaben und Verantwortlichkeiten befindet und ob es sich tatsächlich um Outsourcing handelt. Die Nutzung der Spalte ist optional.

Liegt nachweisbar ein Outsourcing-Verhältnis im Bereich der Software-Entwicklung vor, so verschieben sich die Anforderungen aus dem Baustein CON.8 zum Auftragnehmer. Im Rahmen dieses Outsourcings muss der Auftragnehmer durch das BVA vertraglich zur Einhaltung der Vorgaben gemäß CON.8 verpflichtet werden. Ist dies der Fall, so kann auf Baustein CON.8 gefiltert werden. Der Baustein kann über die Spalte „BSI-Baustein“ (ggf. ausgeblendet) selektiert werden. Nach der inhaltlichen Überprüfung der vertraglichen Abdeckung kann in die Spalte „Zielgruppe bei diesen Anforderungen“ der Wert „Auftragnehmer“ eingetragen werden. Alle anderen Anforderungen werden mit „Auftraggeber“ markiert. Fortan kann nach dieser Aufteilung selektiert werden.

Die Abgrenzung der Bausteine CON.8 und APP.7 formuliert das BSI wie folgt:

*„Wird Software entwickelt, liegt sehr häufig ein Auftraggeber- und Auftragnehmer-Verhältnis vor. Im IT-Grundschutz spiegelt sich dieser Sachverhalt wider, indem der Baustein APP.7 Entwicklung von Individualsoftware die Auftraggeberseite und der Baustein CON.8 Software-Entwicklung die Auftragnehmerseite umfassen. Die Anforderungen dieses Bausteins sind somit vom Auftragnehmer zu erfüllen. Die für die Software-Entwicklung relevanten Anforderungen (funktionale und nichtfunktionale Anforderungen,*

*Anforderungen an die sichere Vorgehensweise sowie das Sicherheitsprofil) werden vom Auftraggeber im Rahmen des Bausteins APP.7 Entwicklung von Individualsoftware erhoben.“*

#### **4.3.6 Anwendungshinweis 5: Anwendung nur relevanter Anforderungen**

Sobald der grundlegende Aufbau des Vorhabens absehbar und etwas gefestigt ist, sollte eine erste „Strukturanalyse“ als Arbeitsschritt aus dem Sicherheitskonzept durchgeführt werden. Hierbei kann erkannt werden, ob gegebenenfalls Anforderungen nicht relevant sind und entfallen können. Beispielsweise könnte in der Strukturanalyse festgestellt werden, dass die Anwendung eine zentrale Authentisierungskomponente nutzt und selbst keinerlei Zugangsdaten verarbeitet. Anforderungen zur sicheren Implementierung einer eigenen Authentisierung wären damit nicht relevant.

#### 4.4. FAQ / Weitere Fragestellungen bei der Anwendung der Richtlinie

*Gibt es generalisierbare Inhalte, die nicht vom Projekt bearbeitet werden müssen?*

Nein, keine Wesentlichen. Prinzipiell generalisierbar wäre eine Auswahl von ca. 15 Anforderungen. Davon sind allerdings nur maximal 2-3 übergreifend beantwortbar/generalisierbar. Dies kann aber wieder vom konkreten Szenario abhängen und umfasst im Wesentlichen beispielsweise Outsourcing, Beschaffung und Beauftragung von Eigenentwicklung.

*Ist eine Abgrenzung der Anforderungen der Richtlinie auf Basis der Projektklassifizierung möglich?*

Nein. Die Sicherheitsrichtlinie hat den Fokus auf die Software-Entwicklung für das BVA. In diesem Scope müssen auch kleine und mittlere Projekte ein Sicherheitskonzept erstellen. Beispielszenarien wie das „Ausgangsszenario 2 – externe Fachanwendung“ oder „Ausgangsszenario 3 – zusätzliche Online-Unterstützung“ im ISB-Dokument „Vorgaben für die Erstellung von Sicherheitskonzepten“ des ISB beschreiben ein anderes Szenario.

*Müssen alle Projekt-Typen Sicherheitskonzepte schreiben?*

Ja, für die Sicherheitskonzepte im Fokus der Richtlinie. Für den Typ „Fach-Sicherheitskonzept“ ist die Richtlinie vollständig anzuwenden. Ein Anwendungslandschafts-Sicherheitskonzept enthält gegebenenfalls übergreifende, programmierte Elemente und ist daher nicht abgrenzbar. Die Richtlinie ist hier ebenfalls vollständig anzuwenden.

Für ein Infrastruktur-Sicherheitskonzept, das in der Regel durch das ITZBund erstellt wird, enthält die Richtlinie keine Anforderungen (beispielweise bezüglich Infrastruktur / Netz und System). Sie ist dafür nicht ausgelegt.

Das Basis-Sicherheitskonzept liegt beim ISB, die Einhaltung dieser Richtlinie für dieses Sicherheitskonzept obliegt dem ISB.

*Gibt es größere Mengen von Anforderungen, die ich unter bestimmten Bedingungen (kleines Projekt, keine Änderungen an der Architektur...) direkt auf entbehrlich setzen kann?*

Weitere Anforderungen können durch den Schritt der so genannten „Modellierung“ im Sicherheitskonzept entfallen. Im Rahmen der Modellierung werden die so genannten „Bausteine des BSI IT-Grundschutz-Kompendium ausgewählt und als zu erfüllende Anforderungen festgelegt. Da die Richtlinie Anforderungen aus den Bausteinen aufgreift, kann hier kann durch das Setzen eines Filters die Liste der Anforderungen reduziert werden. Da die zu Grunde liegenden Bausteine CON.8 „Software-Entwicklung“, CON.10 „Entwicklung von Webanwendungen“ sowie APP.7 „Entwicklung von Individualsoftware“ und OPS.1.1.6 „Software-Tests und -Freigaben“ aber typisch für den Geltungsbereich der Richtlinie sind, erscheint die Möglichkeit hieraus noch weitere Anforderungen pauschal als „entbehrlich“ einstufen zu können, eher als nicht gewinnbringend und Reduzierungen/Vereinfachungen unwahrscheinlich.

*Was passiert beim Wechsel der zu Grunde liegenden Version des BSI IT-Grundschutz-Kompendium?*

Das BSI IT-Grundschutz-Kompendium wird jährlich aktualisiert. Die Richtlinie sollte dieser Aktualisierung folgen. Welche Version wende ich in meinem Projekt an?

Um Synergien aus der Bearbeitung der Richtlinie auf das Sicherheitskonzept ableiten zu können, sollte die anzuwendende Version der Version folgen, die für das Sicherheitskonzept angewendet werden soll. Genauso wie für das Sicherheitskonzept der Projektstart relevant. Während der Projektlaufzeit ist ein Wechsel nicht erforderlich. Im Zweifel sollte hier der ISB kontaktiert werden.

*Anwendung von BSI Mindeststandards*

Das BSI formuliert weiterhin zur verpflichtenden Anwendung von Mindeststandards das folgende:

„Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes fest. Dies erfolgt auf der Grundlage des § 8 Absatz 1 BSIG im Benehmen mit den Ressorts. Als gesetzliche Vorgabe definieren Mindeststandards ein verbindliches Mindestniveau für die Informationssicherheit.

Bereits 2017 hat das Bundeskabinett mit dem Umsetzungsplan Bund 2017 (UP Bund) eine Leitlinie für Informationssicherheit in der Bundesverwaltung in Kraft gesetzt. Damit wurde die Beachtung der Mindeststandards für den Bereich der Stellen des Bundes verbindlich. Durch das IT-Sicherheitsgesetz 2.0 wurde die Einhaltung der Mindeststandards des BSI auch gesetzlich geregelt. Die Umsetzungspflicht der Mindeststandards ergibt sich aus dem dadurch neu gefassten § 8 BSIG.“

Die Mindeststandards formulieren nahezu ausschließlich Vorgaben für die Produktion, so dass eine Anwendung in dieser Richtlinie nicht relevant ist.

*Ist die Hilfestellung „Antwortaufbau“ (mit 10 verschiedenen Antwortmöglichkeiten) nicht zu theoretisch/akademisch gefasst?*

Die Hilfestellung "Antwortaufbau" muss sich im praktischen Einsatz beweisen. Diese Hilfestellung wird gegebenenfalls erst auf den zweiten Blick eine Unterstützung liefern.

*Warum werden in der „Anforderungscheckliste“ nicht zwecks Bedienungsfreundlichkeit Ausfüllhinweise direkt (z.B. via Kommentarfeld, Mouseover) integriert?*

Eine Überführung in Jira oder alternatives Tool ist angestrebt. Auf eine Spezialisierung unter Nutzung von Excel-Funktionalitäten wird bewusst verzichtet.



## 5. Anhang

### 5.1. Glossar

| Bezeichnung                 | Beschreibung   |
|-----------------------------|--|
| Anforderungscheckliste      | Die Anforderungscheckliste stellt die Anforderungen als Anforderungsliste zusammen. Sie ist eine Excel-Datei und besteht aus den Blättern:<br>Blatt "Empfohlenes Vorgehen"<br>Blatt "Anwendungshinweise"<br>Blatt "Anforderungsliste"<br>Blatt "Hilfestellung Antwortaufbau"                                   |
| Hilfestellung Antwortaufbau | Bestandteil des Anhangs „Anforderungscheckliste“ ist das Blatt „Hilfestellung Antwortaufbau“. Es führt Arten von Antworten auf. Diese Hilfestellung soll aufzeigen, welche Inhalte die Antworten im Idealfall abdecken oder haben sollten.   |
| IT-Grundschutz-Kompendium   | Die Bausteine des BSI „IT-Grundschutz-Kompendium“ formulieren Basis-Anforderungen und Standard-Anforderungen, die den Stand der Technik und den normalen Schutzbedarf adressieren. Ergänzend dazu bieten die Bausteine des „IT-Grundschutz-Kompendiums“ Vorschläge für Anforderungen bei erhöhtem Schutzbedarf |
| Entwicklungsumgebung        | Die Entwicklungsumgebung beschreibt die gesamte Infrastruktur zur Umsetzung der funktionalen und nichtfunktionalen Anforderungen an eine Software.   |
| Teil-Anforderung            | Aufteilung der Anforderungstexte einer Anforderung des „IT-Grundschutz-Kompendium“ auf einzelne Anforderungen. Die einzelne Anforderung wird in der Richtlinie als „Teil-Anforderung“ benannt.   |
| UP Bund                     | Umsetzungsplan Bund 2017. Leitlinie für Informationssicherheit in der Bundesverwaltung   |
| Umsetzungs-Beispiele        | Umsetzung-Beispiele, um einen realen Bezug zu den teils abstrakten Anforderungen des BSI herzustellen  |

### 5.2. Abkürzungsverzeichnis

| Abkürzung | Erläuterung |
|-----------|-------------|
|-----------|-------------|

|       |  |
|-------|--|
| NIST  | National Institute of Standards and Technology   |
| OWASP | Open Web Application Security Project (gemeinnützige Organisation zur Verbesserung der Informationssicherheit) |

### 5.3. Referenzen

| Referenz  | Dokument / Link / Quelle  |
|---|---|
| [Ref 01] Grundschutz-Kompodium                        | BSI IT-Grundschutz-Kompodium, Edition 2023<br><a href="https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html">https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html</a> |
| [Ref 02] UP Bund                                      | Umsetzungsplan Bund 2017. Leitlinie für Informationssicherheit in der Bundesverwaltung. Stand: September 2017<br><a href="https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html">https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html</a>  |
| [Ref 03] BVA Leitlinie Informationssicherheit         | Sicherheitsleitlinie für das Bundesverwaltungsamt.<br>Version 1.7. vom 17. Februar 2020   |
| [Ref 04] BVA Richtlinie Ausschreibung, IT-Beschaffung | BVA Richtlinie zur Informationssicherheit Ausschreibung, IT-Beschaffung und Beauftragung von Dienstleistungen für IT-Verfahren - Vorgaben zu Outsourcing und externer Cloud-Nutzung – Stand Datum: 02.03.2023 Version: 2.4  |

### 5.4. Anlagen

| Referenz                        | Dokument / Link / Quelle   |
|---------------------------------|--|
| [Anl 01] Anforderungscheckliste | Anforderungscheckliste für externe Dienstleister oder BVA Projekte |