

# Sicherheitsanforderungen bei Ausschreibung

IT-gestützte Dienstleistung, Softwareentwicklung,  
Webanwendungen und Webserver

**Hinweis:**

Zur Vereinfachung der Lesbarkeit wird auf den folgenden Seiten die männliche Schreibweise verwendet.  
Das Dokument gilt für alle Geschlechter.

## Dokumenteninformation

<b>Klassifikation:</b>	Öffentlich		
<b>Versionsnummer:</b>	1.2		
<b>Dokumententitel:</b>	ISB-SA-01 Sicherheitsanforderungen bei Ausschreibung		
<b>Dokumentennummer:</b>	ISB-SA-01		
<b>Verantwortlicher:</b>	rbb Informationssicherheitsbeauftragter		
<b>Erstellt am:</b>	10.03.2022	<b>Erstellt von:</b>	Marcel Kuring
<b>Nächste Überarbeitung:</b>	02/2028	<b>Überarbeitung durch:</b>	Informationssicherheit
<b>Status:</b>	Freigegeben	<b>Letzte Bearbeitung:</b>	19.03.2026
<b>Freigabe am:</b>	22.09.2022	<b>Freigabe von:</b>	Informationssicherheitskreis

## Dokumentenverteiler

Berechtigte Rolle (Verteilerkreis)
Administratoren, Systemverantwortliche, Projektplaner, Bieter

## Versionsverlauf

Datum	Version	Beschreibung	verändert durch
10.03.2022	0.9	finaler Entwurf	Marcel Kuring
22.09.2022	1.0	Freigabe durch Informationssicherheitskreis	Marcel Kuring
15.01.2026	1.1	Erweiterung Anforderungen um IT-gestützte Dienstleistung	Marcel Kuring
19.03.2026	1.2	Anpassung in Anforderung IT-A12	Marcel Kuring

## Ergänzende Dokumente / Mitgeltende Unterlagen <sup>1</sup>

Dokumentennummer	Titel	Verantwortlicher
BSI TR-02102	<a href="#">Kryptographische Verfahren: Empfehlungen und Schlüssellängen</a>	BSI

<sup>1</sup> In der Tabelle sind alle Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden. Einzutragen sind auch alle Dokumente, auf die im nachfolgenden Dokument explizit verwiesen wird.

## Inhalt

<b>1</b>	<b>Selbstverpflichtung des Bieters .....</b>	<b>1</b>
<b>2</b>	<b>Sicherheitsanforderungen an IT-gestützte Dienstleistung .....</b>	<b>2</b>
	IT-A1 ISMS.....	2
	IT-A2 Zutrittskontrolle .....	2
	IT-A3 Härtung.....	2
	IT-A4 Schwachstellen- und Patchmanagement.....	3
	IT-A5 Schutz vor Cyberangriffen .....	3
	IT-A6 Netzinfrastruktur.....	3
	IT-A7 Verschlüsselung.....	3
	IT-A8 Test + Freigabe .....	3
	IT-A9 Mandantentrennung.....	4
	IT-A10 Datensicherung und Wiederherstellung.....	4
	IT-A11 Löschung.....	4
	IT-A12 Identitäts- und Berechtigungsverwaltung .....	4
	IT-A13 Authentisierung.....	4
	IT-A14 Protokollierung.....	5
	IT-A15 Exportierbarkeit / Portabilität .....	5
	IT-A16 Sicherheitsvorfall.....	6
	IT-A17 Subunternehmen .....	6
	IT-A18 Datenschutz.....	6
	IT-A19 Lokation + Gerichtsstand.....	7
	IT-A20 Rechte.....	7
	IT-A21 Unterweisung .....	7
<b>3</b>	<b>Sicherheitsanforderungen bei Softwareentwicklung .....</b>	<b>8</b>
	SE-A1 Sicheres Systemdesign .....	8
	SE-A2 Authentisierung.....	8
	SE-A3 Protokollierung sicherheitsrelevanter Ereignisse .....	8
	SE-A4 Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen .....	9
	SE-A5 Durchführung von entwicklungsbegleitenden Software-Tests.....	9
	SE-A6 Bereitstellung von Patches, Updates und Änderungen .....	9
	SE-A7 Versionsverwaltung des Quellcodes .....	9
	SE-A8 Überprüfung von externen Komponenten.....	10
<b>4</b>	<b>Sicherheitsanforderungen an Webanwendungen .....</b>	<b>11</b>
	WA-A1 Authentisierung bei Webanwendungen .....	11
	WA-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webanwendungen.....	11
	WA-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates .....	11
	WA-A4 Sichere Konfiguration der Webanwendung.....	11
	WA-A5 Zugriffskontrolle bei Webanwendungen .....	11
	WA-A6 Sicheres Session-Management .....	11
	WA-A7 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen.....	12
	WA-A8 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen .....	12
	WA-A9 Schutz vor Standardbedrohungen.....	12
	WA-A10 Schutz vertraulicher Daten.....	13
	WA-A11 Umfassende Eingabevalidierung und Ausgabekodierung .....	13
<b>5</b>	<b>Anforderungen an Webserver .....</b>	<b>13</b>

WS-A1 Authentisierung bei Webservern.....	13
WS-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webservern .....	13
WS-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates.....	13
WS-A4 Sichere Konfiguration eines Webserver.....	13
WS-A5 Schutz der Webserver-Dateien.....	14
WS-A6 Absicherung von Datei-Uploads und -Downloads.....	14
WS-A7 Verschlüsselung über TLS .....	14
WS-A8 Schutz vor Denial-of-Service-Angriffen.....	14

## 1 Selbstverpflichtung des Bieters

Der Bieter verpflichtet sich die nachfolgenden Sicherheitsanforderungen durch geeignete technische und organisatorische Maßnahmen zu erfüllen.

---

Ort, Datum

---

Unterschrift

## 2 Sicherheitsanforderungen an IT-gestützte Dienstleistung

IT-gestützte Dienstleistung liegt vor, wenn IT-Systeme zur Erfüllung der beauftragten Dienstleistung eingesetzt werden. Beispiele sind: Support / Wartung, Penetrationstests, Bereitstellung und Verwaltung von Cloud-Diensten, Softwareentwicklung, Web-Hosting.

*Handelt es sich bei der IT-gestützten Dienstleistung um Fernwartung sind nur die mit \* gekennzeichneten Anforderungen zu erfüllen.*

### IT-A1 ISMS

#### 1) **Zertifizierung von Rechenzentren**

Alle beteiligten Rechenzentren, MÜSSEN im Rahmen eines Information Security Management System (ISMS) betrieben werden, welches nach ISO/IEC 27001, BSI IT-Grundsatz oder einem vergleichbaren, anerkannten Standard zertifiziert ist. Eine gültige Zertifizierung für das ISMS MUSS vor Beauftragung nachgewiesen werden.

#### 2) **Fortführung der Zertifizierung gewährleisten und nachweisen**

Bei Ablauf der Zertifizierung während der Beauftragung MUSS der Dienstleister die Fortführung der entsprechenden Zertifizierung gewährleisten und nachweisen.

#### 3) **Bei hohem Schutzbedarf**

##### **Zertifizierung der Dienstleister bei hohem Schutzbedarf**

Alle an der beauftragten Dienstleistung beteiligten Dienstleister MÜSSEN ein Information Security Management System (ISMS) nach ISO/IEC 27001, BSI IT-Grundsatz oder einem vergleichbaren, anerkannten Standard betreiben. Die Information Security Management Systeme SOLLTEN zertifiziert sein und eine gültige Zertifizierung vor Beauftragung nachgewiesen werden.

### IT-A2 Zutrittskontrolle

#### 1) **Umsetzung eines wirksamen Zutrittsschutzes**

Räumlichkeiten in denen Daten des Auftraggebers verarbeitet und gespeichert oder abgelegt werden, MÜSSEN gegen den Zutritt unbefugter Personen durch geeignete Maßnahmen abgesichert werden.

#### 2) **Festlegung zutrittsberechtigter Personen**

Der Kreis der zutrittsberechtigten Personen MUSS festgelegt werden und die Zutrittsberechtigungen zu Räumlichkeiten in denen Daten des Auftraggebers verarbeitet und gespeichert oder abgelegt werden, MÜSSEN auf das notwendige Minimum beschränkt werden.

#### 3) **Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen**

Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. Entzug von Zutrittsrechten MÜSSEN personengebunden dokumentiert werden. Dies gilt auch für Besucher, Fremdpersonal, Reinigungs- und Wartungspersonal.

### IT-A3 Härtung

#### 1) **Härtung der Front- und Backendsysteme\***

Die für die Erbringung der Dienstleistung genutzten Systeme MÜSSEN gehärtet sein. Hierzu zählen u.a. die Deinstallation nicht notwendiger Software-Pakete; Deaktivierung/Abschaltung von nicht benötigten Programmen, Diensten, Konten, Services

und Ports; die Anpassung von Konfigurationen; das Erzwingen von Firewall-Regeln; Änderung von Standardpasswörtern.

#### IT-A4 Schwachstellen- und Patchmanagement

##### 1) **Betrieb eines Schwachstellen- und Patchmanagements**

Der Dienstleister MUSS ein Verfahren für seine Verarbeitungsanlagen betreiben, das Schwachstellen erkennt, bewertet, priorisiert und zeitnah behebt. z.B. Patchmanagement, regelmäßige Penetrationstests

#### IT-A5 Schutz vor Cyberangriffen

##### 1) **Erkennung und Abwehr von Cyberangriffen\***

Es MUSS ein geeigneter und aktueller Schutz vor Cyberangriffen nach dem aktuellen Stand der Technik eingerichtet sein. z.B. End-Point-Protection, Einbruchserkennungssysteme (IDS/IPS), zentrale Logauswertung (SIEM), Security Operation Center (SOC), Computer Emergency Response Team (CERT).

#### IT-A6 Netzinfrastruktur

##### 1) **Implementation von Sicherheitsgateways\***

Zur Abwehr netzbasierter Angriffe MÜSSEN wirksame Sicherheitsmaßnahmen (d.h. Firewalls, Netzwerksegmentierung, unterschiedliche Sicherheitszonen) nach dem aktuellen Stand der Technik etabliert sein.

#### IT-A7 Verschlüsselung

##### 1) **Verschlüsselung nach Stand der Technik\***

Der Dienstleister MUSS sich bei Verwendung von Verschlüsselungsverfahren nach dem aktuellen Stand der Technik (beispielsweise siehe BSI TR-02102<sup>2</sup>) richten.

##### 2) **Verschlüsselte Datenübertragung zu externen Systemen\***

Transport: Jegliche Datenkommunikation MUSS auf dem Transportweg verschlüsselt werden.

##### 3) **Verschlüsselung ruhender Daten\***

Der Dienstleister MUSS die ruhenden Daten auf Datenträgern verschlüsselt speichern. Dabei MUSS ein Verfahren genutzt werden, dass dem aktuellen Stand der Technik entspricht.

#### IT-A8 Test + Freigabe

##### 1) **Prozess für Test und Freigabe**

Es MUSS ein geeigneter Prozess für Tests und Freigabe für alle Komponenten der Dienstleistung etabliert sein.

##### 2) **Test neuer Hard und Software\***

Es MUSS sichergestellt werden, dass der produktive Einsatz von Komponenten erst nach erfolgreichem Test und Freigabe erfolgt.

##### 3) **Trennung von Produktiv-, Test und Entwicklungsumgebungen\***

Entwicklungs-, Test- und Produktivumgebung SOLLTEN getrennt sein.

---

<sup>2</sup> Aktuelle Technische Richtlinie beim BSI: [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html)

### IT-A9 Mandantentrennung

#### 1) Trennung von Mandanten

Es MUSS eine wirksame Mandantentrennung gewährleistet sein. Die Daten des Auftraggebers MÜSSEN dabei logisch von denen anderer Kunden getrennt sein.

### IT-A10 Datensicherung und Wiederherstellung

#### 1) Durchführung von Datensicherungen

Der Dienstleister SOLLTE Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.

#### 2) Umsetzung eines Datensicherungskonzeptes

Die Vorgaben des Auftraggebers zu Aufbewahrungszeiten und Wiederherstellungszeiten MÜSSEN umgesetzt werden können.

#### 3) Bei hohem Schutzbedarf der Verfügbarkeit

##### Durchführung von Datensicherung bei hohem Schutzbedarf

Bei hohem Schutzbedarf der Verfügbarkeit MUSS der Dienstleister Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.

### IT-A11 Löschung

#### 1) Löschung und Entsorgung nach dem Stand der Technik\*

Nicht mehr benötigte Daten und Informationen MÜSSEN nach dem aktuellen Stand der Technik vernichtet bzw. gelöscht werden. Nach Beendigung der Beauftragung MÜSSEN alle Daten und Informationen des Auftraggebers unwiederbringlich gelöscht werden. Dem Auftraggeber darf kein Schaden durch nicht vernichtete bzw. gelöschte Daten und Informationen entstehen.

#### 2) Bei hohem Schutzbedarf der Vertraulichkeit

##### Nachweis der Datenlöschung

Als Nachweis SOLLTE dem Auftraggeber ein Löschprotokoll bzw. ein Löschbericht vorgelegt werden, der diesen Datenlöschprozess belegen kann.

### IT-A12 Identitäts- und Berechtigungsverwaltung

#### 1) Dokumentierte Verwaltung von Identitäten und Berechtigungen

Es MUSS eine dokumentierte und stets aktuelle Identitäts- und Berechtigungsverwaltung existieren, die mindestens eine Trennung zwischen Benutzer und administrativen Konten (schließt auch Konten des Dienstleisters ein) ermöglicht.

#### 2) Umsetzung des Need-to-know-Prinzips\*

Es MUSS gewährleistet werden, dass alle Benutzer und Administratoren nur diejenigen Berechtigungen besitzen, die zur Erfüllung der jeweiligen Aufgaben erforderlich sind (Prinzip der minimalen Rechte bzw. least privilege) und bei personellen Veränderungen (z.B. Funktionswechsel, Ausscheiden) Berechtigungen entzogen werden.

### IT-A13 Authentisierung

#### 1) Authentifizierung nach dem Stand der Technik\*

Der Zugang zu Informationen und Systemen MUSS durch eine sichere Authentisierung nach dem aktuellen Stand der Technik geschützt werden. Dies gilt auch für alle Fernzugänge und Schnittstellen.

#### 2) Zugang aus ungeschützten Netzen\*



Grundsätzlich MUSS immer eine Multi-Faktor-Authentisierung verwendet werden. Kann eine Multi-Faktor-Authentisierung nicht umgesetzt werden, darf der Zugang auf den Dienst ausschließlich auf vom Auftraggeber benannten IP-Adressbereichen (z.B. Datennetz der Rundfunkanstalt) erfolgen.

- 3) **Starke Authentisierung bei privilegierten Zugängen\***  
Für privilegierte Zugänge (administrative Zugänge) MUSS eine Multi-Faktor-Authentisierung verwendet werden. Dies gilt auch für alle Fernzugänge und Schnittstellen.
- 4) **Einfache Authentifizierung (per Benutzername/Passwort) bei normalem Schutzbedarf\***  
Bei Verwendung von Passwörtern:  
Es MUSS technisch sichergestellt werden, dass ausschließlich komplexe Passwörter verwendet werden (3 aus den folgenden 4 Merkmalen: Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen; Einhaltung einer definierten Mindestlänge von 10 Zeichen).
- 5) **Umsetzung von Vorgaben einer Passwortrichtlinie**  
Die Vorgaben einer Passwortrichtlinie MÜSSEN umgesetzt werden können (Definition von Passworthistorie, Passwortalter, Passwortlänge).
- 6) **Gesicherte Übertragung von Authentisierungsinformationen im Netzwerk**  
Übertragung der Authentisierungsinformationen (z.B. Passwörter, Pin, biometrische Merkmale):  
Die Übertragung der Authentisierungsgeheimnissen MUSS mit einem sicheren Verschlüsselungsverfahren nach aktuellem Stand der Technik (beispielsweise siehe BSI TR-02102) abgesichert werden.
- 7) **Speicherung von Authentisierungsinformationen\***  
Authentifizierungsinformationen MÜSSEN nach dem aktuellen Stand der Technik geschützt werden (z.B. TPM, sichere Hash-Verfahren wie Argon2).
- 8) **Änderung voreingestellter Authentisierungsinformationen**  
Voreingestellte Authentisierungsinformationen (z.B. Initialkennungen und Passwörter) MÜSSEN geändert werden können.

## IT-A14 Protokollierung

- 1) **Protokollierung sicherheitsrelevanter Ereignisse**  
Sicherheitsrelevante Ereignisse (z.B. erfolgreiche Zugriffe auf Ressourcen, fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Fehlern, allgemeine Fehlermeldungen, Löschen) MÜSSEN in der Art protokolliert werden, dass sie im Nachgang ausgewertet werden können.
- 2) **Sicherung der Protokolldaten vor Verlust und Veränderung**  
Protokollierungsdaten MÜSSEN vor unberechtigtem Zugriff und Manipulation geschützt werden.
- 3) **Kontrolle der Protokolldaten**  
Der Dienstleister MUSS die Protokolle regelmäßig auswerten. Unregelmäßigkeiten MÜSSEN dokumentiert und dem Auftraggeber unverzüglich gemeldet werden.

## IT-A15 Exportierbarkeit / Portabilität

- 1) **Portabilität bei Vertragsende**  
Bei Vertragsende MÜSSEN die Daten des Auftraggebers in elektronischen Standardformaten, wie z. B. CSV, XML, ZIP-Archiv portierbar und exportierbar sein.
- 2) **Bei hohem Schutzbedarf der Verfügbarkeit:**  
**Portabilität bei hohem Schutzbedarf**

Eine Übertragung bzw. Rückführung der Daten MUSS möglich sein. Dazu MÜSSEN durch den Dienstleister entsprechende Schnittstellen, wie z.B. API, Protokolle bereitgestellt werden.

### IT-A16 Sicherheitsvorfall

1) **Incident-Response-Management**

Der Auftraggeber MUSS über alle ihn betreffende Sicherheitsvorfälle und deren mögliche Auswirkungen unverzüglich und in geeigneter Weise informiert werden. Dafür MÜSSEN Ansprechpartner beim Auftraggeber und beim Dienstleister benannt werden.

2) **Notfallvorsorge**

Zur Schadensminimierung und weiterer Schadensabwehr MUSS der Dienstleister geeignete Verfahren zur Notfallvorsorge z.B. BCM etabliert haben.

3) **Angriffserkennung und -abwehr**

Es MÜSSEN Methoden und Technologien verwendet werden, um Cyberangriffe auf die Dienstleistung (z.B. DDoS, Brute-Force) zu erkennen und abzuwehren.

### IT-A17 Subunternehmen

1) **Verpflichtung von Subunternehmen\***

Der Dienstleister MUSS dafür sorgen, dass bei Involvierung von Subunternehmen die vom Auftraggeber gestellten Sicherheitsanforderungen auch von Subunternehmen erfüllt werden. Dies MUSS durch den Dienstleister kontinuierlich überprüft werden.

2) **Benennung von Subunternehmen\***

Der Dienstleister MUSS alle Subunternehmen vollständig benennen. Dabei MUSS ersichtlich sein auf welche Art und in welchem Umfang Subunternehmen in die Bereitstellung der Dienstleistung einbezogen werden.

3) **Bei hohem Schutzbedarf**

**Meldung von Änderungen bei Subunternehmen\***

Beabsichtigte Änderungen an vertraglichen Vereinbarungen mit Subunternehmen, die in die Bereitstellung der Dienstleistung involviert sind, MÜSSEN dem Auftraggeber unverzüglich, vor Umsetzung der Änderung, schriftlich oder per E-Mail mitgeteilt werden.

### IT-A18 Datenschutz

1) **Umsetzung von Anonymisierung**

Sofern vom Auftraggeber gefordert MÜSSEN Maßnahmen zur Anonymisierung, die eine Zuordnung bzw. Verbindung zu einer Person unmöglich machen (z.B. durch Informationsreduktion, datenveränderte Verfahren, Mikroaggregationsverfahren) umgesetzt werden.

2) **Umsetzung von Pseudonymisierung**

Sofern vom Auftraggeber gefordert MÜSSEN Maßnahmen zur Pseudonymisierung (z.B. Transformationsverfahren) nach Stand der Technik (z.B. aktuelle BSI-Richtlinien zu Kryptoverfahren) umgesetzt werden.

3) **getrennte Verarbeitung\***

Der Auftragsverarbeiter stellt sicher, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten wird so gestaltet, dass eine Vermischung von Daten für unterschiedliche Verarbeitungszwecke nicht möglich ist (z.B. physikalische bzw. logische Trennung von Systemen, Datenbanken und Datenträgern, Steuerung über Berechtigungskonzepte).

4) **Protokollierung bei Lese-, Eingabe-, Änderungs- und Löschtransaktionen**

Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen von personenbezogenen Daten MÜSSEN protokolliert werden.

#### IT-A19 Lokation + Gerichtsstand

1) **Angaben zur Gerichtsbarkeit**

Der Dienstleister MUSS nachvollziehbare und transparente Angaben zu seiner Gerichtsbarkeit sowie der Lokation der Daten bei Datenspeicherung, -verarbeitung und -sicherung machen.

2) **Verarbeitung im Europäischen Wirtschaftsraum**

Die Daten und Informationen SOLLTEN innerhalb des Europäischen Wirtschaftsraums (EWR) verarbeitet bzw. gespeichert werden.

3) **Bei hohem Schutzbedarf für Vertraulichkeit oder Integrität**

**Festlegung der Lokation bei hohem Schutzbedarf**

Der Auftraggeber MUSS in der Lage sein, die Lokationen (Ort/Land) der Datenspeicherung, -verarbeitung und -sicherung festzulegen.

#### IT-A20 Rechte

1) **Klärung von Urheber-, Nutzungs- oder Verwertungsrechten**

Der Auftraggeber MUSS alle Urheber-, Nutzungs- oder Verwertungsrechte an den Daten und Informationen, die im Rahmen der Beauftragung gespeichert, verarbeitet oder gesichert werden behalten.

#### IT-A21 Unterweisung

1) **Unterweisung in Datenschutz und Informationssicherheit\***

Alle an der Erbringung der Dienstleistung beteiligten Personen MÜSSEN regelmäßig hinsichtlich der Datenschutz- und Informationssicherheitsvorschriften unterwiesen werden.

### 3 Sicherheitsanforderungen bei Softwareentwicklung

#### SE-A1 Sicheres Systemdesign

- 1) Grundsätzlich MÜSSEN alle Eingabedaten vor der Weiterverarbeitung geprüft und validiert werden.
- 2) Bei Client-Server-Anwendungen MÜSSEN die Daten grundsätzlich auf dem Server validiert werden.
- 3) Die Standardeinstellungen der Software MÜSSEN derart voreingestellt sein, dass ein sicherer Betrieb der Software ermöglicht wird.
- 4) Es MUSS verhindert werden, dass bei Fehlern oder Ausfällen von Komponenten des Systems schützenswerte Informationen preisgegeben werden.
- 5) Die Software MUSS mit möglichst geringen Privilegien ausgeführt werden können.
- 6) Schützenswerte Daten MÜSSEN mit einer Methode, die dem aktuellen Stand der Technik entspricht, verschlüsselt übertragen und gespeichert werden. Die Empfehlungen der Technischen Richtlinie TR-02102<sup>3</sup> des BSI MÜSSEN beachtet werden.

#### SE-A2 Authentisierung

- 1) Es MUSS sichergestellt werden, dass sich Benutzer geeignet authentisieren, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür MUSS eine geeignete vertrauenswürdige Authentisierungsmethode ausgewählt werden (z.B. Anbindung an Microsoft AD / Azure AD).
- 2) Authentisierungsinformationen MÜSSEN verschlüsselt gespeichert oder übertragen werden. Die Empfehlungen der Technischen Richtlinie TR-02102 des BSI MÜSSEN beachtet werden.
- 3) Bei Nutzung von Passwörtern MÜSSEN Benutzer dazu gezwungen werden, sichere Passwörter zu benutzen (3 aus den folgenden 4 Merkmalen: Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen; Einhaltung einer definierten Mindestlänge) und die Vorgaben einer Passwortrichtlinie MÜSSEN umgesetzt werden können (Definition von Passworthistorie, Passwortalter, Passwortlänge).
- 4) Zugänge auf geschützte Ressourcen, die aus dem Internet erreichbar sind, MÜSSEN mit einer Multi-Faktor-Authentisierung geschützt werden.
- 5) Sollen Authentisierungsdaten auf einem Client gespeichert werden, MUSS der Benutzer explizit zustimmen („Opt-In“).
- 6) Es MUSS einen Schutz vor Brute-Force-Angriffen geben.
- 7) Alle angebotenen Authentisierungsverfahren MÜSSEN das gleiche Sicherheitsniveau aufweisen.
- 8) In der Standardeinstellung MÜSSEN Authentisierungsinformationen bei der Eingabe ausgeblendet werden.
- 9) Voreingestellte Authentisierungsinformationen (z. B. Standard- oder Initialkennungen und Passwörter des Herstellers / Entwicklers) MÜSSEN noch vor der Inbetriebnahme in den Produktivbetrieb geändert werden.

#### SE-A3 Protokollierung sicherheitsrelevanter Ereignisse

- 1) Sicherheitsrelevante Ereignisse MÜSSEN in der Art protokolliert werden, dass sie im Nachgang ausgewertet werden können.

---

<sup>3</sup> Aktuelle Technische Richtlinie beim BSI: [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html)

- 2) Bei automatisierter Auswertung der Protokollierungsdaten MUSS sichergestellt werden, dass Schadcode in Protokoll-Einträgen vom Auswertungsprogramm nicht interpretiert werden.
- 3) Der Zugriff auf Protokollierungsdaten MUSS auf einen definierten Personenkreis beschränkt werden können.
- 4) Es MÜSSEN mindestens folgende Ereignisse protokolliert werden:
  - erfolgreiche Zugriffe auf Ressourcen
  - fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Fehlern
  - allgemeine Fehlermeldungen

#### SE-A4 Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen

- 1) Wird im Rahmen des Entwicklungs- und Implementierungsprozesses auf externe Bibliotheken zurückgegriffen, MÜSSEN diese aus vertrauenswürdigen Quellen bezogen werden.
- 2) Bevor externe Bibliotheken verwendet werden, MUSS deren Integrität sichergestellt werden.

#### SE-A5 Durchführung von entwicklungsbegleitenden Software-Tests

- 1) Schon bevor die Software im Freigabeprozess getestet und freigegeben wird, MÜSSEN entwicklungsbegleitende Software-Tests durchgeführt und der Quellcode auf Fehler gesichtet werden.
- 2) Die entwicklungsbegleitenden Tests MÜSSEN die funktionalen und nichtfunktionalen Anforderungen der Software umfassen. Die Software-Tests MÜSSEN dabei auch Negativtests abdecken. Zusätzlich MÜSSEN auch alle kritischen Grenzwerte der Eingabe sowie der Datentypen überprüft werden.
- 3) Die Software MUSS in einer Test- und Entwicklungsumgebung getestet werden, die getrennt von der Produktionsumgebung ist.
- 4) Es MUSS getestet werden, ob die Systemvoraussetzungen für die vorgesehene Software ausreichend dimensioniert sind.

#### SE-A6 Bereitstellung von Patches, Updates und Änderungen

- 1) Es MUSS sichergestellt sein, dass sicherheitskritische Patches und Updates für die entwickelte Software zeitnah durch die Entwickler bereitgestellt werden.
- 2) Werden für verwendete externe Bibliotheken sicherheitskritische Updates bereitgestellt, dann MÜSSEN die Entwickler ihre Software hierauf anpassen und ihrerseits entsprechende Patches und Updates zur Verfügung stellen.

#### SE-A7 Versionsverwaltung des Quellcodes

- 1) Der Quellcode des Entwicklungsprojekts MUSS über eine geeignete Versionsverwaltung verwaltet werden.
- 2) Es MUSS sichergestellt sein, dass durch die Versionsverwaltung alle Änderungen am Quellcode nachvollzogen und rückgängig gemacht werden können.
- 3) Es MUSS eine Datensicherung der Versionsverwaltung erfolgen.

### SE-A8 Überprüfung von externen Komponenten

- 1) Unbekannte externe Komponenten, deren Sicherheit nicht durch etablierte und anerkannte Peer-Reviews oder vergleichbares sichergestellt werden kann, MÜSSEN auf Schwachstellen überprüft werden.
- 2) Die Integrität von externen Komponenten MUSS durch Prüfsummen oder kryptographische Zertifikate überprüft werden.

## 4 Sicherheitsanforderungen an Webanwendungen

### WA-A1 Authentisierung bei Webanwendungen

- 1) Es MÜSSEN die Anforderungen [SE-A2 Authentisierung](#) erfüllt werden.

### WA-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webanwendungen

- 1) Es MÜSSEN die Anforderungen [SE-A3 Protokollierung sicherheitsrelevanter Ereignisse](#) erfüllt werden.

### WA-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

- 1) Die Webanwendung MUSS ein regelmäßiges Einspielen sicherheitsrelevanter Patches und Updates ermöglichen.

### WA-A4 Sichere Konfiguration der Webanwendung

- 1) Webanwendungen SOLLTEN so konfiguriert sein, dass auf ihre Ressourcen und Funktionen ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade zugegriffen werden kann. Falls dies nicht möglich ist, MUSS der Zugriff so weit wie möglich eingeschränkt werden.
- 2) Der Zugriff auf nicht benötigte Ressourcen und Funktionen SOLLTE deaktiviert werden. Falls dies nicht möglich ist, MUSS der Zugriff so weit wie möglich eingeschränkt werden.
- 3) Folgendes MUSS bei der Konfiguration von Webanwendungen und Webservices umgesetzt werden:
  - Deaktivieren nicht benötigter HTTP-Methoden
  - Konfigurieren der Zeichenkodierung
  - Vermeiden von sicherheitsrelevanten Informationen in Fehlermeldungen und Antworten
  - Speichern von Konfigurationsdateien außerhalb des Web-Root-Verzeichnisses sowie
  - Festlegen von Grenzwerten für Zugriffsversuche

### WA-A5 Zugriffskontrolle bei Webanwendungen

- 1) Es MUSS mittels einer Autorisierungskomponente sichergestellt werden, dass Benutzer nur Aktionen durchführen können, zu denen sie berechtigt sind.
- 2) Jeder Zugriff auf geschützte Inhalte und Funktionen MUSS durch die Autorisierungskomponente kontrolliert werden, bevor er ausgeführt wird.
- 3) Es MÜSSEN alle von der Webanwendung verwalteten Ressourcen von der Autorisierungskomponente berücksichtigt werden.
- 4) Die Benutzer MÜSSEN serverseitig und zentral auf einem vertrauenswürdigen IT-System autorisiert werden.
- 5) Ist die Zugriffskontrolle fehlerhaft, MÜSSEN Zugriffe abgelehnt werden.
- 6) Es MUSS eine Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen geben.
- 7) Der Zugriff auf Dateien durch die Benutzer MUSS mit restriktiven Dateisystemberechtigungen beschränkt werden.
- 8) Es MUSS ein sicherer Umgang mit temporären Dateien vorgesehen werden.

### WA-A6 Sicheres Session-Management

- 1) Session-IDs MÜSSEN zufällig und mit ausreichender Entropie erzeugt werden.



- 2) Falls das Framework der Webanwendung Session-IDs generieren kann, MUSS diese Funktion des Frameworks verwendet werden. Sicherheitsrelevante Konfigurationsmöglichkeiten des Frameworks MÜSSEN berücksichtigt werden.
- 3) Die Session-ID MUSS ausreichend geschützt werden, wenn sie übertragen und vom Client gespeichert wird.
- 4) Eine Webanwendung MUSS den Benutzern die Möglichkeit geben, eine bestehende Sitzung explizit zu beenden.
- 5) Nachdem sich der Benutzer angemeldet hat, MUSS eine bereits bestehende Session-ID durch eine neue ersetzt werden.
- 6) Sitzungen MÜSSEN eine maximale Gültigkeitsdauer besitzen (Timeout).
- 7) Inaktive Sitzungen MÜSSEN automatisch nach einer bestimmten Zeit ungültig werden.
- 8) Nachdem die Sitzung ungültig ist, MÜSSEN alle Sitzungsdaten sowohl server- als auch clientseitig ungültig und gelöscht sein.

#### WA-A7 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen

- 1) Es MUSS sichergestellt werden, dass eine Webanwendung ausschließlich vorgesehene Daten und Inhalte einbindet und an den Benutzer ausliefert.
- 2) Falls eine Webanwendung eine Upload-Funktion für Dateien anbietet, MUSS diese Funktion so weit wie möglich eingeschränkt werden (z.B. Beschränkung auf definierte Dateiformate, Beschränkung auf definierte Dateigrößen, Beschränkung auf definierte Anzahl gleichzeitiger Uploads). Zugriffs- und Ausführungsrechte MÜSSEN in diesem Fall restriktiv gesetzt werden. Es MUSS sichergestellt werden, dass ein Benutzer Dateien nur im vorgegebenen Pfad speichern kann.
- 3) Die Ziele der Weiterleitungsfunktion einer Webanwendung MÜSSEN ausreichend eingeschränkt werden, sodass Benutzer ausschließlich auf vertrauenswürdige Webseiten weitergeleitet werden.
- 4) Verlässt ein Benutzer die Vertrauensdomäne, MUSS ihn die Webanwendung darüber informieren.

#### WA-A8 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen

- 1) Webanwendungen MÜSSEN vor automatisierten Zugriffen geschützt werden. Dabei MUSS jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Benutzer auswirken.
- 2) Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, MUSS dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden.

#### WA-A9 Schutz vor Standardbedrohungen

- 1) Die folgenden Standardbedrohungen MÜSSEN bei der Entwicklung der Webanwendung beachtet werden:
  - SQL-Injection und andere Command-Injections
  - Cross-Site-Scripting,
  - Cross-Site-Request-Forgery
  - Sitzungsübernahme
  - Rechteausweitung
  - Bad credential Management
  - Manipulierte Cookies und Header
  - Buffer Overflow



- 2) Werden Daten an ein Datenbank-System weitergeleitet, MÜSSEN Stored Procedures bzw. Prepared SQL Statements eingesetzt werden, wenn dies von der Einsatzumgebung unterstützt wird. Wenn weder Stored Procedures noch Prepared SQL Statements eingesetzt werden können, MÜSSEN die SQL-Queries separat abgesichert werden.

#### WA-A10 Schutz vertraulicher Daten

- 1) Durch Direktiven MUSS gewährleistet werden, dass Webanwendung clientseitig keine schützenswerten Daten zwischenspeichern.
- 2) Es MUSS sichergestellt werden, dass in Formularen keine vertraulichen Formulardaten im Klartext angezeigt werden.
- 3) Dateien mit Quelltexten der Webanwendung MÜSSEN vor unerlaubten Abrufen geschützt werden.

#### WA-A11 Umfassende Eingabevalidierung und Ausgabekodierung

- 1) Alle an eine Webanwendung übergebenen Daten MÜSSEN als potenziell gefährlich behandelt und geeignet gefiltert werden.
- 2) Alle Eingabedaten sowie Datenströme und Sekundärdaten wie z. B. Session-IDs MÜSSEN validiert werden.
- 3) Fehleingaben SOLLTEN möglichst nicht automatisch behandelt werden (Sanitizing). Lässt es sich jedoch nicht vermeiden, MUSS Sanitizing sicher umgesetzt werden.
- 4) Ausgabedaten MÜSSEN so kodiert werden, dass schadhafter Code auf dem Zielsystem nicht interpretiert oder ausgeführt wird.

### 5 Anforderungen an Webserver

#### WS-A1 Authentisierung bei Webservern

- 1) Es MÜSSEN die Anforderungen [SE-A2 Authentisierung](#) erfüllt werden.

#### WS-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webservern

- 1) Es MÜSSEN die Anforderungen [SE-A3 Protokollierung sicherheitsrelevanter Ereignisse](#) erfüllt werden.

#### WS-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

- 1) Der Webserver MUSS ein regelmäßiges Einspielen sicherheitsrelevanter Patches und Updates ermöglichen.

#### WS-A4 Sichere Konfiguration eines Webserver

- 1) Den Webserver-Prozess MUSS ein Benutzerkonto mit minimalen Rechten zuweisen werden.
- 2) Der Webserver MUSS in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. Ist dies nicht möglich, SOLLTE jeder Webserver auf einem eigenen physischen oder virtuellen Server ausgeführt werden.
- 3) Dem Webserver-Dienst MÜSSEN alle nicht notwendige Schreibberechtigungen entzogen werden.
- 4) Nicht benötigte Module und Funktionen des Webserver MÜSSEN deaktiviert werden.

### WS-A5 Schutz der Webserver-Dateien

- 1) Alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, MÜSSEN vor unbefugtem Lesen und Ändern geschützt werden.
- 2) Es MUSS sichergestellt werden, dass Webanwendungen nur auf einen definierten Verzeichnisbaum zugreifen können (WWW-Wurzelverzeichnis).
- 3) Der Webserver MUSS so konfiguriert sein, dass er nur Dateien ausliefert, die sich innerhalb des WWW-Wurzelverzeichnisses befinden.
- 4) Es MÜSSEN alle nicht benötigten Funktionen, die Verzeichnisse auflisten, deaktiviert werden.
- 5) Es MUSS sichergestellt werden, dass vertrauliche Dateien nicht in öffentlichen Verzeichnissen des Webserver liegen.

### WS-A6 Absicherung von Datei-Uploads und -Downloads

- 1) Alle mithilfe des Webserver veröffentlichten Dateien MÜSSEN vorher auf Schadprogramme geprüft werden.
- 2) Es MUSS eine Maximalgröße für Datei-Uploads spezifiziert sein.
- 3) Für Uploads MUSS genügend Speicherplatz reserviert werden.

### WS-A7 Verschlüsselung über TLS

- 1) Der Webserver MUSS für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS, nach Stand der Technik, anbieten (HTTPS). Falls es aus Kompatibilitätsgründen erforderlich ist, veraltete Verfahren zu verwenden, MÜSSEN diese auf so wenige Fälle wie möglich beschränkt werden.
- 2) Wenn eine HTTPS-Verbindung genutzt wird, DÜRFEN alle Inhalte NUR über HTTPS verfügbar sein. Sogenannter Mixed Content DARF NICHT verwendet werden
- 3) Die Empfehlungen der Technischen Richtlinie TR-02102<sup>4</sup> des BSI MÜSSEN beachtet werden.

### WS-A8 Schutz vor Denial-of-Service-Angriffen

- 1) Es MÜSSEN Maßnahmen definiert und umgesetzt werden, die DDoS-Angriffe verhindern oder zumindest abschwächen.

---

<sup>4</sup> Aktuelle Technische Richtlinie beim BSI: [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html)