

Anlage 13: Anforderungen an Zuverlässigkeit, IT-Sicherheit sowie Entwicklung und Betrieb von Individualsoftware (BSI-Grundsatz-konform)

1. Ziel und Geltungsbereich

Diese Anlage definiert verbindliche Anforderungen an die Informationssicherheit, Zuverlässigkeit sowie an Entwicklung, Änderung und Betrieb von Individualsoftware im Rahmen der Leistungserbringung.

Die Anforderungen sind durch den Auftragnehmer einzuhalten und orientieren sich an den einschlägigen Bausteinen des BSI IT-Grundsatzes (insb. APP.7, CON.8, CON.10, OPS.1.1.x).

Sie gelten für alle Phasen des Softwarelebenszyklus sowie für alle beteiligten Personen, einschließlich eingesetzter Dritter.

2. Grundsätzliche Verpflichtungen des Auftragnehmers

Der Auftragnehmer stellt sicher, dass:

- ein angemessenes Niveau an Informationssicherheit gewährleistet ist
- alle Leistungen unter Einhaltung anerkannter Sicherheitsstandards erbracht werden
- Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen geschützt sind

2.1 Vertraulichkeit und Zugriffsschutz

Der Auftragnehmer ist verpflichtet:

- alle im Rahmen der Leistungserbringung erlangten Informationen vertraulich zu behandeln
- diese ausschließlich für vertraglich vereinbarte Zwecke zu verwenden
- Zugriffe auf Systeme, Entwicklungsumgebungen und Daten nach dem Need-to-know-Prinzip zu beschränken
- eingesetzte Mitarbeitende vor Tätigkeitsaufnahme zur Vertraulichkeit zu verpflichten

3. Anforderungen an die Softwareentwicklung

3.1 Planung und Anforderungsdefinition

- Sicherheitsanforderungen sind frühzeitig verbindlich festzulegen
- der gesamte Softwarelebenszyklus ist unter Sicherheitsaspekten zu planen
- Anforderungen an Authentisierung, Autorisierung, Datenschutz und Protokollierung sind zu definieren
- ein geeignetes Vorgehensmodell (klassisch oder agil) ist festzulegen und einzuhalten

3.2 Sichere Entwicklung und Umsetzung

- Umsetzung erfolgt nach einem definierten und dokumentierten Entwicklungsprozess
- Sicherheitsanforderungen sind in allen Phasen umzusetzen (Design, Implementierung, Integration)
- sichere Programmierpraktiken (Secure Coding) sind anzuwenden
- Quellcode ist versionskontrolliert und vor unbefugter Änderung geschützt zu verwalten
- externe Komponenten sind vor Einsatz sicherheitstechnisch zu prüfen und freizugeben
- Entwicklungs-, Test- und Produktionsumgebungen sind strikt zu trennen

3.3 Webanwendungen (falls zutreffend)

- Schutz gegen typische Webangriffe (z. B. Injection, XSS) ist umzusetzen
- Eingaben sind systematisch zu validieren
- sichere Authentifizierungs- und Sitzungsmechanismen sind einzusetzen

4. Anforderungen an Test und Freigabe

4.1 Softwaretests

- Software ist vor Produktivsetzung vollständig zu testen
- Tests umfassen funktionale, sicherheitsrelevante und nicht-funktionale Anforderungen
- Regressionstests sind bei Änderungen verpflichtend
- Testergebnisse sind nachvollziehbar zu dokumentieren

4.2 Freigabeprozess

- Produktivsetzung erfolgt nur nach formaler Freigabe
- Freigaben sind revisionssicher zu dokumentieren
- mit Freigabe wird die Verantwortung für den produktiven Einsatz übernommen

5. Anforderungen an Änderungen und Weiterentwicklung

5.1 Änderungsmanagement

- Änderungen erfolgen ausschließlich über geregelte Verfahren
- jede Änderung ist zu dokumentieren, zu bewerten und zu testen
- sicherheitsrelevante Änderungen sind priorisiert umzusetzen

5.2 Umgang mit Schwachstellen

- Sicherheitslücken sind unverzüglich zu bewerten und zu beheben
- allgemein bekannte Schwachstellen sind aktiv zu berücksichtigen

- eingesetzte Komponenten sind regelmäßig zu überprüfen und zu aktualisieren

6. Anforderungen an den Betrieb

6.1 Allgemeiner IT-Betrieb

- Betrieb ist strukturiert, dokumentiert und kontrolliert durchzuführen
- Verantwortlichkeiten sind eindeutig festzulegen
- Systeme sind zu überwachen (Monitoring)
- eingesetzte Software und Komponenten sind zu inventarisieren

6.2 Betriebssicherheit und Administration

- administrative Tätigkeiten erfolgen nur durch autorisiertes Personal
- produktive und nicht-produktive Umgebungen sind strikt getrennt
- Systeme sind sicher zu konfigurieren und regelmäßig zu aktualisieren

6.3 Datensicherung und Verfügbarkeit

- geeignete Backup- und Wiederherstellungsverfahren sind umzusetzen
- Wiederherstellbarkeit von Entwicklungsständen und Daten ist sicherzustellen
- Versionsverwaltung ist verpflichtend einzusetzen

6.4 Schutzmaßnahmen im Betrieb

- Schutzmaßnahmen gegen Schadsoftware sind umzusetzen
- Sicherheitsupdates sind regelmäßig einzuspielen
- Systeme sind gegen unbefugten Zugriff zu schützen

7. Protokollierung und Nachvollziehbarkeit

- sicherheitsrelevante Aktivitäten sind zu protokollieren (z. B. Änderungen, Deployments)
- Protokolle sind vor Manipulation zu schützen
- Änderungen an produktiven Systemen sind nachvollziehbar zu dokumentieren

8. Identitäts- und Berechtigungsmanagement

- Zugriffe sind nach dem Need-to-know-Prinzip zu vergeben
- Berechtigungen sind regelmäßig zu überprüfen
- privilegierte Zugriffe sind besonders zu sichern

9. Sicherheitsvorfälle (Incident Management)

- Sicherheitsvorfälle sind unverzüglich zu erkennen und zu melden
- die Auftraggeberin ist bei relevanten Vorfällen sofort zu informieren

- der Auftragnehmer unterstützt bei Analyse und Behebung
- geeignete Wiederherstellungsmaßnahmen sind vorzuhalten

10. Einsatz von Dritten

- Unterauftragnehmer sind zur Einhaltung gleichwertiger Sicherheitsanforderungen zu verpflichten
- deren Einsatz ist gemäß vertraglichen Regelungen anzuzeigen
- der Auftragnehmer bleibt für die Einhaltung verantwortlich

11. Sichere Leistungserbringung (übergreifend)

Der Auftragnehmer stellt zusätzlich sicher:

- Schutz aller Umgebungen vor unbefugtem Zugriff
- Anwendung aktueller Sicherheitsstandards und Best Practices
- sichere Konfiguration aller eingesetzten Systeme

12. Abgrenzung zum Datenschutz

Die Verarbeitung personenbezogener Daten wird abschließend im separaten Auftragsverarbeitungsvertrag (AVV) geregelt.

Diese Anlage adressiert ausschließlich Anforderungen an die IT-Sicherheit.

13. Inkrafttreten und Verbindlichkeit

Diese Anforderungen sind verbindlich für alle an Entwicklung, Betrieb und Leistungserbringung beteiligten Parteien.

Abweichungen sind nur zulässig, wenn:

- eine dokumentierte Risikobewertung erfolgt ist und
- die Auftraggeberin ausdrücklich zugestimmt hat