Informationssicherheitsanforderungen an Auftragnehmer der Unternehmensgruppe Stadtwerke Bielefeld (bestehend aus: Stadtwerke Bielefeld GmbH, moBiel GmbH, BBF Bielefelder Bäder und Freizeit GmbH, BITel Gesellschaft für Telekommunikation mbH, Bielefelder Netz GmbH, Interargem GmbH, MVA Bielefeld-Herford GmbH und Enertec Hameln GmbH)

Letzte Änderung: 09.10.2026

1 Generelle Verantwortlichkeit

Der Auftragnehmer trägt die Verantwortung dafür, dass er sämtliche durch den Auftraggeber in diesem Dokument festgelegten Anforderungen und Vorgaben einhält. Hierzu zählt insbesondere seine Verpflichtung, im Rahmen seiner Leistungserbringung für die Unternehmen der Unternehmensgruppe Stadtwerke Bielefeld (SWB-Gruppe) die jeweils gültigen rechtlichen Vorgaben sowie die jeweils aktuellen Standards zur Informationssicherheit zu beachten und angemessen zu berücksichtigen.

Ziel dieser Verpflichtung ist es sicherzustellen, dass der Auftragnehmer Produkte liefert und Dienstleistungen erbringt, die die Integrität, die Vertraulichkeit, die Verfügbarkeit, die Authentizität und die Belastbarkeit aller im Kontext der Leistungserbringung und des Schutzes des eigenen Unternehmens relevanten, schutzbedürftigen Informationen und Systeme des Auftraggebers (nachfolgend „Schutzziele“ genannt) nicht beeinträchtigen.

2 Gewährleistung eines dem Leistungsgegenstand angemessenen Informationssicherheitsniveaus

Der Auftragnehmer ist verpflichtet, alle im Kontext der Leistungserbringung für den Auftraggeber relevanten Informationen und Systeme nach dem jeweils aktuellen Stand der Technik gegen unberechtigten Zugriff, Veränderung, Zerstörung und sonstigen Missbrauch zu sichern, um die Leistungserbringung sicherzustellen.

Dabei trifft der Auftragnehmer geeignete und angemessene technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau hinsichtlich der Schutzziele zu gewährleisten.

Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zum Risiko des Nichterreichens der Schutzziele steht.

Der Auftragnehmer verfolgt dabei einen kontinuierlichen Verbesserungsprozess, d. h. er überprüft ständig alle Einflussparameter mit dem Ziel, sein Sicherheitsniveau zu verbessern.

2.1 Grundlegende Anforderungen an die Informationssicherheit

- Je nach Art und Schutzbedarf der Informationen bzw. der Bedeutung der Leistungen des Auftragnehmers für den Geschäftsbetrieb des Auftraggebers kann der Auftraggeber vom Auftragnehmer ein besonderes Maß an Sicherungsmaßnahmen sowie einen geeigneten Nachweis über ein angemessenes Informationssicherheitsniveau im Betrieb des Auftragnehmers verlangen, insbesondere durch Vorlage geeigneter Zertifikate[1].
- Der Auftragnehmer sichert unabhängig von vorgenannten Nachweisen zu, dass

[1] z.B. ISO/IEC 27001, IT-Grundschutz, ISIS12 etc.

- in seiner Organisation alle erforderlichen Rollen, Verantwortlichkeiten und Kompetenzen mit Bezug zur Informationssicherheit festgelegt und bekannt sind,
- bezüglich der Zugangssteuerung in seiner Organisation mindestens folgende Maßnahmen etabliert sind:
  - Dokumentierte Freigabeprozesse für Berechtigungen auf Systeme und Informationen
  - Prozesse zur zeitnahen Löschung von Zugriffsrechten bei Austritt oder Abteilungswechsel
  - Angemessene Authentisierungsverfahren mit angemessener Passwortkomplexität und -gültigkeit und höheren Anforderungen an administrative Zugänge
  - Automatische Bildschirmsperre nach Inaktivität
  - Jederzeitige (auch spätere) eindeutige Nachvollziehbarkeit der Identität der Person, die zu einem bestimmten Zeitpunkt einen Zugang genutzt hat.

- alle im Rahmen der Leistungserbringung eingesetzten Beschäftigten bezüglich der zu beachtenden Aspekte der Informationssicherheit sensibilisiert und unterwiesen wurden und entsprechende Lernzielkontrollen den Erfolg der Maßnahmen bestätigten.

- alle im Rahmen der Leistungserbringung eingesetzten Beschäftigten eine Verpflichtungserklärung zur Einhaltung der Vorgaben zur Informationssicherheit und zur Wahrung der Vertraulichkeit unterzeichnet haben, die, soweit gesetzlich zulässig, auch über das Ende ihres Beschäftigungsverhältnisses hinaus fortbesteht.

- angemessene und ausreichende Vorkehrungen zur physischen Sicherheit aller für die Leistungserbringung erforderlichen, schutzbedürftigen Informationen und Systeme getroffen wurden (sowohl bei stationärer Verarbeitung als auch beim Transport), insbesondere hinsichtlich
  - elementarer Gefährdungen (Feuer, Wasser, Blitz, Sturm, Katastrophen etc.),
  - höherer Gewalt (Temperatur, Feuchte, Korrosion, sonstige Umwelteinflüsse etc.),
  - technischem Versagen (Ausfall Versorgungseinrichtungen etc.) und
  - vorsätzlichen Handlungen (Einbruch, Sabotage, Diebstahl etc.).

- der Zutritt zu Bereichen mit schutzbedürftigen Informationen oder Systemen jeweils nur auf einen autorisierten, besonders vertrauenswürdigen Personenkreis beschränkt ist.

- nicht mehr benötigte schutzbedürftige Informationen und Datenträger in einer Form gelöscht bzw. vernichtet werden, dass ausgeschlossen ist, dass gelöschte bzw. vernichtete Daten von Dritten unautorisiert wiederhergestellt werden können.

- angemessene DV-technische Sicherheitsmaßnahmen zum Schutz aller für die Leistungserbringung erforderlichen, schutzbedürftigen Informationen und Systeme getroffen wurden, insbesondere durch
  - den Einsatz von geeigneten Firewalls und aktueller Virenschutz-Software
  - den Einsatz ausschließlich von der Organisation geprüfter und freigegebener Hard- und Software
  - aktuelles Patch-Management
  - geeignete System-Härtung

  - angemessene Authentisierungs-Maßnahmen
  - geprüfte Datensicherungs- und Wiederherstellungs-Mechanismen
- ein Inventar- / Wertverzeichnis aller schutzbedürftigen Informationen und Systeme, die für die Leistungserbringung relevant sind, vorliegt und in der Organisation bekannt ist.

- Der Auftragnehmer hat dem Auftraggeber jegliche Abweichungen von den in diesem Dokument vereinbarten Sicherheitsanforderungen unverzüglich in Textform zu melden.

- **Schwachstellen Management**

  Der Auftragnehmer hat alle Aspekte seiner Leistungserbringung einer kontinuierlichen Prüfung auf Schwachstellen zu unterziehen und so schnell wie möglich auf neu erkannte Schwachstellen zu reagieren.

  Hierzu sichtet er kontinuierlich Quellen für Sicherheitsempfehlungen und bewertet diese hinsichtlich der gegenüber dem Auftraggeber zu erbringenden Leistungen.

  Der Umfang der Prüfung hat jede potenzielle Schwachstelle zu umfassen, die Einfluss auf die Schutzziele sowohl des Auftraggebers als auch des Auftragnehmers hat oder haben kann.

- **Meldungen zu Sicherheitsvorfällen**

  Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die Einfluss auf die Schutzziele des Auftragnehmers haben oder haben können, unverzüglich per E-Mail an den Auftraggeber (Kontakt: cert@stadtwerke-bielefeld.de) zu melden. Die Meldung muss mindestens Art und Zeitpunkt des Vorfalls, betroffene Systeme, betroffene Informationen/Daten, bekannte oder vermutete Auswirkungen auf die Schutzziele, bereits ergriffene Sofortmaßnahmen, geplante weitere Maßnahmen sowie einen fachlich zuständigen Ansprechpartner enthalten. Der Auftragnehmer hat den Auftraggeber fortlaufend über wesentliche neue Erkenntnisse und den Stand der Abhilfemaßnahmen zu informieren.

- **Audit**

  Der Auftraggeber ist berechtigt, sich jederzeit vor und während der Leistungserbringung in angemessener Weise die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in der Vereinbarung festgelegten Verpflichtungen seitens des Auftragnehmers nachweisen zu lassen.

  Der Auftragnehmer ermöglicht hierzu dem Auftraggeber auf Verlangen, sich auch vor Ort von der Einhaltung der Verpflichtungen und Zusicherungen zu überzeugen. Der Auftragnehmer hat die Untersuchungen des Auftraggebers unentgeltlich zu unterstützen und Mitwirkungsleistungen, wie Auskünfte oder Einsichtnahme in die gespeicherten Informationen und Daten, zu erbringen, soweit dies für das Audit erforderlich ist.

Der Auftraggeber ist berechtigt, sich nach rechtzeitiger Anmeldung maximal einmal pro Jahr während der üblichen Geschäftszeiten in einem Zeitraum von bis zu zwei Stunden und, soweit möglich und zumutbar, ohne Störung der betrieblichen Abläufe auch in den Betriebsstätten des Auftragnehmers einschließlich der IT-Systeme von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen zu überzeugen.

Der Auftraggeber ist berechtigt, die Audits durch ein externes, gegenüber Dritten zur Verschwiegenheit verpflichtetes und qualifiziertes Unternehmen durchführen zu lassen. Hierbei darf es sich jedoch nicht um einen Mitwettbewerber im Rahmen der Leistungserbringung handeln. Gesetzliche Kontroll- und Auskunftsrechte des Auftraggebers werden hierdurch weder eingeschränkt noch ausgeschlossen.

Der Auftraggeber übermittelt dem Auftragnehmer zeitnah den Auditbericht.

Der Auftragnehmer erhält anschließend Gelegenheit, Stellung zu festgestellten Unregelmäßigkeiten zu nehmen und geeignete Vorschläge zum weiteren Umgang zu unterbreiten. Falls der Auftraggeber diesen Vorschlägen nicht zustimmt, ist der Auftragnehmer zur Nachbesserung verpflichtet.

Der Umfang des Audits bezieht sich ausschließlich auf für die Auftragserbringung relevante Dienste und Systeme. Die Überprüfung von Systemen anderer Kunden des Auftragnehmers ist ausgeschlossen.

- **Fernzugang**

  Fernzugänge zu Netzwerken des Auftraggebers werden ausschließlich vom Auftraggeber gesteuert und sind nur unter folgenden Bedingungen gestattet:

  - Der Auftragnehmer stellt sicher, dass bei Fernzugängen die Schutzziele im Umgang mit den (materiellen und immateriellen) Vermögenswerten des Auftraggebers jederzeit gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer, während eines Fernzugriffes Kenntnis erlangt hat. Der Auftragnehmer ist für alle Aktionen und Vorgänge, die unter Verwendung der ihm zur Verfügung gestellten Benutzerkonten mit Fernzugangsfunktion ausgelöst oder durchgeführt werden, verantwortlich.
  - Grundsätzlich hat der Auftragnehmer jedem Nutzer ein eigenes Benutzerkonto zur Verfügung zu stellen. Ausnahmen von dieser Regel sind begründet vorab mit dem Auftraggeber abzustimmen.
  - Wird vom Auftragnehmer ein Nutzerkonto nicht mehr benötigt, ist der Auftraggeber umgehend darüber zu informieren, so dass das entsprechende Konto gesperrt werden kann.
  - Der Auftragnehmer hat Nutzerkonten mit Fernzugangsfunktion regelmäßig zu überprüfen und den Auftraggeber über eventuell notwendige Änderungen zu informieren.

- **Einsatz kryptographischer Absicherungen**

  Der Auftragnehmer stellt sicher, dass eine kryptographische Absicherung der Kommunikation und Ablage überall dort erfolgt, wo es gemäß dem Stand der Technik und des

notwendigen Schutzniveaus erforderlich ist. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere dann notwendig, wenn Informationen mit hohem Schutzbedarf (z.B. Steuerungsdaten der Kritischen Infrastruktur oder vertrauliche Daten) über öffentliche oder als nicht ausreichend sicher anzusehende Netzwerke übertragen werden.

Der Auftragnehmer ist verpflichtet, von ihm im Rahmen der Leistungserbringung eingesetzte Kryptographielösungen in seinem Schwachstellen-Management (s.o.) zu berücksichtigen und hinsichtlich ihres Sicherheitsniveaus zu bewerten. Bei seinen Einschätzungen hat er sich an der BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen zu orientieren.

- **Sicherheit in Auslagerungsprozessen**

  Beabsichtigt der Auftragnehmer, Teile der Betriebsleistung oder anderer Dienstleistungen für den Auftraggeber an Subunternehmen auszulagern, stellt er sicher, dass die in diesem Dokument beschriebenen Sicherheitsanforderungen in den Vereinbarungen mit den Subunternehmen berücksichtigt sind. Der Auftragnehmer bleibt für die Einhaltung der Informationssicherheitsanforderungen durch eingesetzte Subunternehmen verantwortlich. Er hat sicherzustellen, dass der Auftraggeber oder ein von ihm beauftragter Dritter die Einhaltung der Anforderungen auch bei Subunternehmen überprüfen kann, soweit dies für die Leistungserbringung relevant ist und berechtigte Interessen Dritter gewahrt bleiben.
  Die von den Subunternehmen zu erfüllenden Sicherheitsanforderungen sind so zu definieren, dass die Sicherheitsstandards für die Daten und Leistungen des Auftraggebers jederzeit eingehalten werden und der Auftragnehmer seine eigenen Sicherheitsverpflichtungen gegenüber dem Auftraggeber vollständig erfüllen kann. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich aller Subunternehmen ist dem Auftraggeber vor Auftragserteilung nachzuweisen.

  Alle vom Auftragnehmer beabsichtigten Auslagerungen von Betriebs- oder Dienstleistungen an Subunternehmer bedürfen der vorherigen Zustimmung des Auftraggebers.

2.2 Erweiterte Anforderungen bei Leistungen mit Bezug zu IT-, OT-Systemen, Software und vernetzten Komponenten

Erbringt der Auftragnehmer eine der folgenden Leistungen für den Auftraggeber:

- Bereitstellung einer SaaS-/Cloud-Software oder -Lösung
- Entwicklung von Software und IT- sowie OT-Systemen
- Betrieb von Software oder IT- und OT-Systemen
- Bereitstellung von vernetzbaren IT- und OT-Systemen und Komponenten
- Fernwartung von IT- oder OT-Systemen

so muss zwingend die Checkliste *Freigabecheckliste Informationssicherheit SWB-Gruppe, Version 2.5* in ausgefüllter und durch den Auftraggeber akzeptierter Form vorliegen.

Der Anhang dieses Dokuments enthält einen Auszug der wesentlichen Anforderungen aus der Freigabecheckliste.

Die vollständige Checkliste wird im Rahmen oder im Vorfeld des Ausschreibungs- und Beauftragungsprozesses zusammen mit einer Verschwiegenheitserklärung (NDA) an die potenziellen Auftragnehmer übermittelt.

Darüber hinaus gelten folgende generelle Anforderungen für die in Ziffer 2.2 genannten Arten der Leistungserbringung:

- **Aktualität der Software**

  Der Auftragnehmer stellt sicher, dass alle in Ziffer 2.2 genannten Leistungen zum Zeitpunkt der Abnahme dem aktuellen Herstellerstand entsprechen. Der Patchstand darf grundsätzlich nicht älter als 12 Monate sein. Für Systeme mit erhöhtem Schutzbedarf, direkter Internetanbindung oder sicherheitskritischer Funktion kann der Auftraggeber einen maximalen Rückstand von 3 bis 6 Monaten verlangen.

  Der Auftragnehmer verpflichtet sich, für alle im Rahmen der Leistungserbringung bereitgestellten Hard- und Softwarekomponenten während des gesamten vorgesehenen Produktlebenszyklus Sicherheitsupdates, Patches und sonstige sicherheitsrelevante Korrekturen bereitzustellen. Dies gilt mindestens bis zum vom Hersteller veröffentlichten Ende des Produktlebenszyklus (End of Support / End of Life).

  Der Auftragnehmer informiert den Auftraggeber unverzüglich über bekannte Sicherheitslücken sowie verfügbare Sicherheitsupdates und stellt diese innerhalb angemessener Fristen bereit. Der Wegfall der Unterstützung durch Vorlieferanten oder Hersteller entbindet den Auftragnehmer nicht von seiner Verpflichtung, die vereinbarten Sicherheitsanforderungen und die sichere Nutzbarkeit der gelieferten Leistung aufrechtzuerhalten.

  Beabsichtigt der Auftragnehmer die Einstellung des Supports oder die Erklärung eines End-of-Life-Zustands, so hat er den Auftraggeber mindestens 24 Monate im Voraus schriftlich zu informieren und geeignete Ersatz-, Migrations- oder Weiterbetriebsmaßnahmen aufzuzeigen, die einen weiterhin sicheren Betrieb gewährleisten.

- **Patchmanagement und End of Life**

  Falls der Drittanbieter eines Betriebssystems oder einer anderen Komponente (Software, Datenbanken, Anwendungen etc.), die entweder im Leistungsumfang des Auftragnehmers inkludiert ist oder vom Auftragnehmer für seine Leistungserbringung vorausgesetzt wurde, das Ende des Lifecycles verkündet, ist vom Auftragnehmer sicherzustellen, dass die Anforderungen des Auftraggebers weiterhin erfüllt werden (z.B. weitere Funktionsfähigkeit der Systeme, keine Einschränkungen der Leistungserbringung des Auftraggebers etc.).

  In Fällen, in denen der Auftragnehmer nur Anwendungen und / oder andere Funktionalitäten liefert und der Auftraggeber oder sonstige Drittanbieter in seinem Namen für das Update-Management auf den darunterliegenden Schichten wie Betriebssystem verantwortlich ist, gewährleistet der Auftragnehmer eine kontinuierliche Funktionsfähigkeit seiner gelieferten Leistung auch bei Patches der ggf. darunterliegenden Systemplattform.

- **Unerwünschte Funktionen**

  Der Auftragnehmer sichert zu, dass die im Rahmen der Leistungserbringung gegebenenfalls eingesetzte Hard- und Software frei von Funktionen ist, die die Schutzziele gefährden, beispielsweise durch Funktionen

  - zum unerwünschten Absetzen/Ausleiten von Daten
  - zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder
  - zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen

  „Unerwünscht“ in diesem Sinne ist eine Funktion, die weder vom Auftraggeber gefordert noch vom Auftragnehmer unter konkreter Beschreibung der Funktion und ihrer Auswirkungen angeboten, noch im Einzelfall vom Auftraggeber ausdrücklich autorisiert („opt-in“) wurde.

- **Einsatz von KI-Funktionen und KI-Anwendungen**

  Umfasst der in Ziffer 2.2 genannte Leistungsumfang den direkten Einsatz von KI-Lösungen (KI-Funktionen oder KI-Anwendungen), so ist dies transparent durch den Auftragnehmer gegenüber dem Auftraggeber darzustellen.

  Der Auftragnehmer hat für alle im Leistungsumfang enthaltenen KI-Funktionen oder KI-Anwendungen eine dokumentierte Risikobewertung durchzuführen und dem Auftraggeber auf Anfrage vorzulegen. Die Bewertung muss mindestens die verarbeiteten Datenarten, den Grad der autonomen Entscheidungsfindung, bestehende Systemzugriffe, die Auswirkungen fehlerhafter Ergebnisse berücksichtigen. Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Begrenzung identifizierter Risiken nachzuweisen. Änderungen, die zu einer erhöhten Risikoeinstufung führen können, sind dem Auftraggeber unverzüglich anzuzeigen und bedürfen einer erneuten Bewertung.

3 Schlussbestimmungen

Ist eine der genannten Regelungen unwirksam oder unvollständig, so bleiben die weiteren Regelungen hiervon im Übrigen wirksam. An die Stelle der unwirksamen Regelung tritt die gesetzliche Regelung.

Sämtliche mit diesem Dokument in Zusammenhang stehenden finanziellen Aufwände des Auftragnehmers werden nicht gesondert vergütet, sondern sind mit Zahlung der Vergütung nach dem Hauptvertrag abgegolten.

Änderungen dieses Dokuments, des Verarbeitungsgegenstandes oder Verfahrensänderungen sind nur einvernehmlich möglich und bedürfen der Schriftform.

Anhang: Spezielle Anforderungen für die Sicherheit von IT-, OT-Systemen, Software und vernetzten Komponenten

Die Anforderungen gelten für die Systeme & Komponenten, die im Rahmen der Leistungserbringung durch den Auftragnehmer bereitgestellt werden.

ID	Abfragen	Konkretisierung	Cloud	On Premise
A.51	Nutzung von KI	Falls in der Lösung Künstliche Intelligenz (KI) zum Einsatz kommt, ist Folgendes zu definieren: • Welche Daten verarbeitet die KI? • Welche Entscheidungen beeinflusst die KI? • Welche Aktionen kann die KI eigenständig ausführen? • Verpflichtung zur Einhaltung aller geltenden rechtlichen Anforderungen, bspw. des EU AI Act	x	x
A.9	Standort der Server	Es muss sichergestellt werden, dass der Standort der Server in der EU ist.	x	
A.10	Externes Hosting	Das externe Hosting findet in abgesicherten Rechenzentren (Orientierung an BSI-INF.2 *Rechenzentrum sowie Serverraum)* statt.	x	
A.15	Festplattenverschlüsselung	Die Daten müssen in verschlüsselter Form auf der Festplatte vorliegen.	x	
A.17	Mandantentrennung	Es muss eine vollständige logische Mandantentrennung umgesetzt werden, sodass Daten, Konfigurationen und Zugriffe eines Mandanten technisch und organisatorisch strikt von anderen Mandanten getrennt sind und ein mandantenübergreifender Zugriff ausgeschlossen ist.	x	x
A.18	Anti-DDoS Schutzmaßnahmen und WAF	Anti-DDoS-Schutzmaßnahmen und eine WAF werden eingesetzt (bei Webanwendungen und/oder Anwendungen, die aus dem Internet erreichbar sind).	x	
A.20	Patchkonzept & Patchmanagement	Es gibt für alle beteiligten Komponenten (Soft- und Hardware) ein definiertes Patchkonzept, um diese immer auf dem aktuellen Stand zu halten. Das Release- und Patchmanagement umfasst: • Betriebssystem • Alle Softwarepakete und Services, die Teil des Betriebssystems sind • Alle Tools und Applikationen, die der Hersteller zu Betriebs- und Wartungszwecken installiert hat • Zielapplikation (Servicelogik) • Alle Middleware-Application-Layer, Datenbanken, Access-, Monitoring- oder Applikationsserver, die für den Service genutzt werden	x	x
A.21	Lebenszyklus Softwarekomponenten	Die eingesetzte Software (Betriebssystem, Anwendungen etc.) wird durch den Hersteller unterstützt und befindet sich nicht im End-of-Life- oder End-of-Support-Zustand. Software, die diese Anforderung nicht erfüllt, ist im Rahmen des Patchprozesses zu erneuern.	x	x
A.24	Rollen- und Berechtigungskonzept	Ein Rollen- und Berechtigungskonzept über alle Rollen liegt vor. Änderungen an der Zuweisung der Rollen müssen über Changeprozesse im ITSM abgebildet werden.	x	x
A.26	Systembenutzer	Anzahl der Systembenutzer ist minimiert und deren Zweck dokumentiert.	x	x

A.27	Zugriffsmonitoring der privilegierten Benutzer (auf der Applikations-, Betriebssystem- und Virtualisierungsplattformebene)	Administrative Zugriffe auf das System werden überwacht und ausgewertet.	x	x
A.28	MFA (Multi-Faktor-Authentisierung)	MFA ist für alle Benutzertypen aktivierbar.	x	x
A.50	Umsetzung Passwortpolicy	Passwörter müssen mindestens 12 Zeichen lang sein und eine Kombination aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.	x	x
A.36	Datenlöschungskonzept liegt vor	Es liegt ein Prozess zur sicheren Löschung und Vernichtung vertraulicher Daten vor.	x	
A.37	Audit-Trail	Es wird ein vollständiger Audit-Trail (bspw. Logdateien) erstellt. Dies dient der Sicherstellung der Nachvollziehbarkeit und Nachweisbarkeit bzw. der Nichtabstreitbarkeit der Benutzertätigkeiten.	x	x
A.38	SIEM / SzA Anbindung	Die Anwendung muss an ein System zur Angriffserkennung (SzA), bspw. ein SIEM, angebunden sein. Alle sicherheitsrelevanten Ereignisse werden bspw. in Form von Logs synchron an die SzA übertragen.	x	x
A.40	Schwachstellenmanagement & Regelmäßige Sicherheitsüberprüfungen	Der Anbieter der Software betreibt ein aktives Schwachstellenmanagement für die Software und seine Infrastruktur, führt regelmäßig Sicherheitsüberprüfungen durch und schließt identifizierte Sicherheitslücken in angemessenen Zeiträumen (Patchmanagement).	x	
A.41	Regelmäßige Überprüfung der Wirksamkeit aller Maßnahmen	Alle technischen und organisatorischen Maßnahmen werden regelmäßig auf Wirksamkeit geprüft und dokumentiert (z. B. durch interne Audits oder Management-Reviews), sowohl aufseiten der SWB als auch aufseiten des Herstellers.	x	x
A.47	Auditrecht / Lieferantenaudit	Der Auftraggeber (ein Unternehmen der SWB-Gruppe) behält sich vor, maximal einmal jährlich ein Lieferantenaudit auf Basis der ISO 27001 beim Auftragnehmer durchzuführen. Der Umfang des Audits bezieht sich ausschließlich auf die für die Auftragserbringung relevanten Prozesse, Dienste und Systeme. Das Audit kann vor Ort oder remote erfolgen.	x	x
A.48	Zertifizierungen (bspw. ISO/IEC 27001, SOC 2, BSI C5)	Der Auftragnehmer muss über eine gültige Sicherheitszertifizierung verfügen: Cloud: BSI C5, ISO 27001 o. Ä.; On-Premise: ISO 27001 o. Ä. Die Zertifizierung muss den Anwendungsbereich der geprüften Applikation bzw. des geprüften Dienstes umfassen.	x	x