

Sicherheitsanforderungen bei Beauftragung und Nutzung von externen Anwendungen und Diensten | Dienstleister (EXTERN)

Formularstand ZDF	26.03.2026
Auftragnehmer	
Abgabedatum	

					Schutzziel			Sicherheitsanforderungen EXT.[Nr.]		Erfüllung der Sicherheitsanforderungen durch den Anbieter
Nr.	Mapping CS	Domäne IS	Domäne DS	Anforderung	C	I	A	Schutzbedarf	Inhalt	Beschreibung der Umsetzung
EXT.1.1	OIS-01	ISMS	ISMS	Zertifizierung von Rechenzentren	x	x	x	normal	Alle beteiligten Rechenzentren, MÜSSEN im Rahmen eines Information Security Management System (ISMS) betrieben werden, welches nach ISO/IEC 27001, BSI IT-Grundschutz oder einem vergleichbaren, anerkannten Standard zertifiziert ist. Eine gültige Zertifizierung für das ISMS MUSS vor Beauftragung nachgewiesen werden.	
EXT.1.2	OIS-02	ISMS	ISMS	Fortführung der Zertifizierung gewährleisten und nachweisen	x	x	x	normal	Bei Ablauf der Zertifizierung während der Beauftragung MUSS der Dienstleister die Fortführung der entsprechenden Zertifizierung gewährleisten und nachweisen.	
EXT.1.3	OIS-01	ISMS	ISMS	Zertifizierung der Dienstleister bei hohem Schutzbedarf	x	x	x	hoch	Alle an der beauftragten Dienstleistung beteiligten Dienstleister MÜSSEN ein Information Security Management System (ISMS) nach ISO/IEC 27001, BSI IT-Grundschutz oder einem vergleichbaren, anerkannten Standard betreiben. Die Information Security Management Systeme SOLLTEN zertifiziert sein und eine gültige Zertifizierung vor Beauftragung nachgewiesen werden.	
EXT.2.1	IDM-01 COS-01	Zutrittskontrolle	Zutrittskontrolle	Umsetzung eines wirksamen Zutrittsschutzes	x	x	x	normal	Räumlichkeiten in denen Daten des Auftraggebers verarbeitet und gespeichert oder abgelegt werden, MÜSSEN gegen den Zutritt unbefugter Personen durch geeignete Maßnahmen abgesichert werden.	
EXT.2.2	IDM-01	Zutrittskontrolle	Zutrittskontrolle	Festlegung zutrittsberechtigter Personen	x	x	x	normal	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.	
EXT.2.3	IDM-01	Zutrittskontrolle	Zutrittskontrolle	Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen	x	x	x	normal	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.	
EXT.3.1	OPS-23	Härtung	Weitergabekontrolle	Härtung der Front- und Backendsysteme	x	x	x	normal	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.	
EXT.4.1	OPS-18 OPS-20 AM-02 OPS-22	Schwachstellen- und Patchmanagement	Detektion + Reaktion	Betrieb eines Schwachstellen- und Patchmanagements	x	x	x	normal	Der Dienstleister MUSS ein Verfahren für seine Verarbeitungsanlagen betreiben, das Schwachstellen erkennt, bewertet, priorisiert und zeitnah behebt. z.B. Patchmanagement, regelmäßige Penetrationstests	
EXT.5.1	OPS-05	Schutz vor Cyberangriffen	Detektion + Reaktion	Erkennung und Abwehr von Cyberangriffen	x	x	x	normal	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).	
EXT.6.1	COS-04	Netzinfrastruktur	Zugangskontrolle	Implementation von Sicherheitsgateways	x	x	x	normal	Zur Abwehr netzbasierter Angriffe MÜSSEN wirksame Sicherheitsmaßnahmen (d.h. Firewalls, Netzwerksegmentierung, unterschiedliche Sicherheitszonen) nach dem aktuellen Stand der Technik etabliert sein.	
EXT.7.1	CRY-01	Verschlüsselung	Weitergabekontrolle	Verschlüsselung nach Stand der Technik	x	x		normal	Der Dienstleister MUSS sich bei Verwendung von Verschlüsselungsverfahren nach dem aktuellen Stand der Technik (beispielsweise siehe BSI TR-02102) richten.	
EXT.7.2	CRY-02	Verschlüsselung	Weitergabekontrolle	Verschlüsselte Datenübertragung zu externen Systemen	x	x		normal	Transport: Jegliche Datenkommunikation MUSS auf dem Transportweg verschlüsselt werden.	
EXT.7.3	CRY-03	Verschlüsselung	Weitergabekontrolle	Verschlüsselung ruhender Daten	x	x		normal	Der Dienstleister MUSS die ruhenden Daten auf Datenträgern verschlüsselt speichern. Dabei MUSS ein Verfahren genutzt werden, dass dem aktuellen Stand der Technik entspricht.	
EXT.8.1	DEV-03	Test + Freigabe	Trennungskontrolle	Trennung von Produktiv-, Test und Entwicklungsumgebungen	x	x	x	normal	Es MUSS ein geeigneter Prozess für Tests und Freigabe für alle Komponenten der Dienstleistung etabliert sein.	
EXT.8.2	DEV-06 DEV-09	Test + Freigabe	Verfügbarkeitskontrolle	Test neuer Hard und Software	x	x	x	normal	Es MUSS sichergestellt werden, dass der produktive Einsatz von Komponenten erst nach erfolgreichem Test und Freigabe erfolgt.	
EXT.8.3	DEV-10	Test + Freigabe	Trennungskontrolle	Trennung von Produktiv-, Test und Entwicklungsumgebungen	x	x	x	normal	Die Produktivumgebung muss von Entwicklungs- und Testumgebung getrennt sein.	
EXT.9.1	OPS-24	Mandantentrennung	Trennungskontrolle	Trennung von Mandanten	x			normal	Es MUSS eine wirksame Mandantentrennung gewährleistet sein. Die Daten des Auftraggebers MÜSSEN dabei logisch von denen anderer Kunden getrennt sein.	

EXT.10.1	OPS-06	Datensicherung und Wiederherstellung	Verfügbarkeitskontrolle	Durchführung von Datensicherungen			x	normal	Der Dienstleister MUSS Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.	
EXT.10.2	OPS-06	Datensicherung und Wiederherstellung	Verfügbarkeitskontrolle	Umsetzung eines Datensicherungskonzeptes			x	normal	Die Vorgaben des Auftraggebers zu Aufbewahrungszeiten und Wiederherstellungszeiten MÜSSEN umgesetzt werden können.	
EXT.10.3	OPS-06	Datensicherung und Wiederherstellung	Verfügbarkeitskontrolle	Durchführung von Datensicherung bei hohem Schutzbedarf			x	hoch	Bei hohem Schutzbedarf der Verfügbarkeit MUSS der Dienstleister dem Schutzbedarf angepasste Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.	
EXT.11.1	PI-03	Löschung	Weitergabekontrolle	Löschung und Entsorgung nach dem Stand der Technik	x			normal	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.	
EXT.11.2		Löschung	Weitergabekontrolle	Nachweis der Datenlöschung	x			normal	Als Nachweis ist dem Auftraggeber ein Löschprotokoll bzw. ein Löschbericht vorzulegen, der diesen Datenlöschprozess belegen kann.	
EXT.12.1	IDM-01 IDM-06	Identitäts- und Berechtigungsverwaltung	Zugangs- / Zugriffskontrolle	Dokumentierte Verwaltung von Identitäten und Berechtigungen	x	x		normal	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.	
EXT.12.2	IDM-01	Identitäts- und Berechtigungsverwaltung	Zugangs- / Zugriffskontrolle	Umsetzung des Need-to-know-Prinzips	x	x		normal	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).	
EXT.12.3	IDM-03 IDM-04	Identitäts- und Berechtigungsverwaltung	Zugangs- / Zugriffskontrolle	Meldung von personellen Veränderungen	x			normal	Bei personellen Veränderungen des Wartungspersonals (z.B. Funktionswechsel, Ausscheiden) MUSS der Auftraggeber informiert werden und nicht mehr benötigte Zugangs- bzw. Zugriffsrechte MÜSSEN entzogen werden.	
EXT.13.1	IDM-09	Authentisierung	Zugangskontrolle	Authentifizierung nach dem Stand der Technik	x	x		normal	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.	
EXT.13.2	IDM-09	Authentisierung	Zugangskontrolle	Zugang aus ungeschützten Netzen	x	x		normal	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.	
EXT.13.3	IDM-09	Authentisierung	Zugangskontrolle	Starke Authentisierung bei privilegierten Zugängen	x	x		normal	Für privilegierte Zugänge (administrative Zugänge) MUSS eine Multi-Faktor-Authentisierung verwendet werden. Dies gilt auch für alle Fernzugänge und Schnittstellen.	
EXT.13.4	IDM-09	Authentisierung	Zugangskontrolle	Einfache Authentifizierung (per Benutzername/Passwort) bei normalem Schutzbedarf	x	x		normal	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).	
EXT.13.5	IDM-09	Authentisierung	Zugangskontrolle	Umsetzung von Vorgaben einer Passwortrichtlinie	x	x		normal	Die Vorgaben einer Passwortrichtlinie MÜSSEN umgesetzt werden können (Definition von Passworthistorie, Passwortalter, Passwortlänge).	
EXT.13.6	CRY-02	Authentisierung	Zugangskontrolle	Gesicherte Übertragung von Authentisierungsinformationen im Netzwerk	x	x		normal	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.	
EXT.13.7	IDM-08	Authentisierung	Weitergabekontrolle	Speicherung von Authentisierungsinformationen	x	x		normal	Authentisierungsinformationen MÜSSEN nach dem aktuellen Stand der Technik geschützt werden (z.B. TPM, sichere Hash-Verfahren wie Argon2).	
EXT.13.8	PSS-07	Authentisierung	Zugangskontrolle	Änderung voreingestellter Authentisierungsinformationen	x	x		normal	Voreingestellte Authentisierungsinformationen (z.B. Initialkennungen und Passwörter) MÜSSEN geändert werden können.	
EXT.14.1	OPS-10	Protokollierung	Zugangskontrolle	Protokollierung sicherheitsrelevanter Ereignisse	x	x	x	normal	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.	
EXT.14.2	OPS-10 OPS-12	Protokollierung	Eingabekontrolle	Sicherung der Protokolldaten vor Verlust und Veränderung	x	x	x	normal	Protokollierungsdaten MÜSSEN vor unberechtigtem Zugriff und Manipulation geschützt werden.	
EXT.14.3	OPS-13	Protokollierung	Eingabekontrolle	Kontrolle der Protokolldaten	x	x		normal	Der Dienstleister MUSS die Protokolle regelmäßig auswerten. Unregelmäßigkeiten MÜSSEN dokumentiert und dem Auftraggeber unverzüglich gemeldet werden.	
EXT.15.1	PI-02	Exportierbarkeit / Portabilität	Verfügbarkeitskontrolle	Portabilität bei Vertragsende			x	normal	Bei Vertragsende MÜSSEN die Daten des Auftraggebers in elektronischen Standardformaten, wie z. B. CSV, XML, ZIP-Archiv portierbar und exportierbar sein.	
EXT.15.2	PI-02	Exportierbarkeit / Portabilität	Verfügbarkeitskontrolle	Portabilität			x	normal	Eine Übertragung bzw. Rückführung der Daten MUSS möglich sein. Dazu MÜSSEN durch den Dienstleister entsprechende Schnittstellen, wie z.B. API, Protokolle bereitgestellt werden.	

EXT.16.1	SIM-01	Sicherheitsvorfall	Detektion + Reaktion	Incident-Response-Management	x	x	x	normal	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.	
EXT.16.2	SIM-02	Sicherheitsvorfall	Verfügbarkeitskontrolle	Notfallvorsorge	x	x	x	normal	Zur Schadensminimierung und weiterer Schadensabwehr MUSS der Dienstleister geeignete Verfahren zur Notfallvorsorge z.B. BCM etabliert haben.	
EXT.16.3	IDM-03	Sicherheitsvorfall	Detektion + Reaktion	Angriffserkennung und -abwehr	x	x	x	normal	Es MÜSSEN Methoden und Technologien verwendet werden, um Cyberangriffe auf die Dienstleistung (z.B. DDoS, Brute-Force) zu erkennen und abzuwehren.	
EXT.17.1	SSO-01	Subunternehmen	Subunternehmen	Verpflichtung von Subunternehmen	x	x	x	normal	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.	