ANLAGE 4

INFORMATIONSSICHERHEIT

ZU SAIT ZVB-IT

1. INHALTSVERZEICHNIS

1 PRÄAMBEL, BEGRIFFSBESTIMMUNGEN UND DEFINITIONEN

1.1 Dieses Dokument gilt für alle von vom AUFTRAGNEHMER erbrachten Leistungen.

1.2 Dieses Dokument enthält Vorgaben des AUFTRAGGEBERS an den AUFTRAGNEHMER in Bezug auf die IT- und Informationssicherheit (ISEC), für die Bereitstellung von Produkten und Leistungen für den AUFTRAGGEBER und in diesem Zusammenhang erhaltenem Zugriff auf Informationen, sowie den Betrieb von Systemen und Technologien.

1.3 Die vertragsgegenständlichen Systeme werden für alle Geschäftsfunktionen genutzt und müssen gegen Versagen und Missbrauch geschützt werden. Maßnahmen zum Schutz der Systeme erstrecken sich auf die Bereiche Standorte und Gebäude, Technik, Betriebssysteme, Anwendungen und Daten, sowie betriebliche Organisation und von dem AUFTRAGNEHMER eingesetzte Personen. Nur ein optimales Zusammenwirken dieser Bereiche ist in der Lage, die angestrebte Sicherheit der Systeme zu bewirken. Der AUFTRAGGEBER kann ergänzend spezifische bzw. weitergehende Sicherheitsanforderungen der einzelnen Informationen, Daten oder Systeme definieren und dem AUFTRAGNEHMER schriftlich mitteilen.

1.4 Der AUFTRAGNEHMER ist verpflichtet, die in dem Vertrag vereinbarten Vorgaben sowie die Vorgaben des AUFTRAGGEBERS, insbesondere hinsichtlich Schutzbedarfen oder Anforderungen, insbesondere aus Business-Impact-Analysen, vollständig umzusetzen. Im Zusammenhang mit der Leistungserbringung beachtet der AUFTRAGNEHMER diesbezüglich

- den jeweiligen „aktuellen Stand der Technik“ im Sinne der allgemein anerkannten Regeln der Technik (inklusive etwa zusammenhängender organisatorischer Regeln), die (i) der Richtigkeitsüberzeugung der vorherrschenden Ansicht der technischen Fachleute entsprechen und darüber hinaus (ii) in der Praxis erprobt und bewährt sind,
- die in der Industrie anerkannten Standards der Informationssicherheit sowie
- das Anwendbare Recht und
- alle anwendbaren regulatorischen Pflichten

und passt die Umsetzung der Vorgaben den jeweils aktuellen Erkenntnissen regelmäßig und, eigenständig an. Soweit dazu eine Mitwirkung des AUFTRAGGEBERS erforderlich ist, findet eine Abstimmung statt. Der AUFTRAGNEHMER stellt sicher, dass die relevanten Informationen, Auswertungen und regelmäßigen Berichte zur Verfügung stehen und die Anforderungen des AUFTRAGGEBERS berücksichtigt werden. Der AUFTRAGNEHMER weist weiterhin den AUFTRAGGEBER regelmäßig, jedoch mindestens halbjährlich, auf diesbezüglich fehlende Vorgaben und / oder nicht ausreichende Vorgaben in Bezug auf die IT- und Informationssicherheit hin.

1.5 Durch Beachtung dieser Informationssicherheitsanforderungen sollen die Schutzziele für Informationen, Systeme und Technologien des jeweiligen Kunden über die gesamte Dauer der Vertragsbeziehung und 5 (fünf) Jahre darüber hinaus durch den AUFTRAGNEHMER ausgelegt werden.

1.6 Der AUFTRAGNEHMER stellt die für die Gewährleistung der Informationssicherheit eventuell notwendige Software und Hardware, wenn nicht explizit etwas anderes vereinbart ist.

1.7 Sofern in diesem Dokument von „sicherstellen“, „stellt sicher“ oder Formulierungen dieser Wörter gesprochen wird, so sind diese als Garantien des AUFTRAGNEHMERS zu verstehen.

Bezug[1]: EN ISO/IEC 27001: 2022 Kapitel 4.1, Kapitel 4.2, A.5.31, A.5.32, A.5.33, A.5.34

[1]Eine Nennung von Controls relevanter Normen ist ausschließlich informativ und begrenzt nicht die jeweiligen Verpflichtungen des AUFTRAGNEHMERS aus den betreffenden Ziffern dieses Dokuments.

1.8 Für diese Anlage Informationssicherheit werden folgende Begriffsbestimmungen und Definitionen verwendet:

„Configuration Item“: Jede Anlage und / oder Komponente, welche für das Erbringen einer Leistung notwendig ist und gemanaged werden muss; dies umfasst auch den IT-Service selbst. Alle Configuration Items und die Beziehungen zwischen ihnen sind in einer Configuration Management Database erfasst.

„Antwortzeit“: Zeitspanne, die vom Ende der Nutzereingabe bis zur entsprechenden Reaktion der Applikation vergeht. Zur Sicherung der Antwortzeit sind Batch- bzw. Auswertungsläufe während des Online-Betriebes im Rahmen der betrieblichen Möglichkeiten grundsätzlich durch den Endanwender initiierbar, sollten jedoch bei zu erwartenden größeren Systembelastungen mit dem AN abgestimmt werden. Vorrangig werden in jedem Fall alle periodisch initiierten Batchläufe abgewickelt.

„Fix“: Auslieferung der Behebung eines Funktionsfehlers einer Software / Anwendung, z. B. im Quellcode

„Hotfix“: Fix mit sicherheitsrelevanten Anpassungen (z.B. mit Blick auf Betriebsstabilität, sonstige Informationssicherheit usw.)

„Batch“: Anwendung, welche keine Interaktion mit einer natürlichen Person erfordert. Ein Batch läuft nach dem (automatisch oder manuell) initiierten Start eigenständig ab, endet eigenständig und liefert ein vorbestimmtes Ergebnis zurück.

„Disaster“ oder „Katastrophe“: Ein oder mehrere eskalierte Notfälle, die den Fortbestand der Geschäftstätigkeit der FDG und / oder das Leben und die Gesundheit von Personen gefährdet (entspricht im Wesentlichen der Definition von Krise nach BSI 200-4).

„geschützter Bereich“: Ein geschützter Bereich ist eine Umgebung, die ausschließlich für dienstliche Zwecke eingesetzt wird und aus welchem man keinen Zugriff auf private Dateien oder Umgebungen erhält. Dies kann z.B. über Citrix oder Container-Technologie realisiert werden. Kernmerkmale dieses geschützten Bereiches sind

- separate Umgebung mit eigenem Login bzw. Anmeldedaten
- kein Copy & Paste möglich zwischen den geschützten und dem privaten Bereich
- i.d.R. keine Administrationsrechte und nur beschränkter Zugriff auf die jeweils zugewiesenen Ressourcen / Freigaben

„Informationssicherheitsereignis“: Erkanntes Auftreten eines System-, Service- oder Netzwerkzustandes, der einen möglichen Verstoß gegen die Informationssicherheitsleitlinie anzeigt. Ebenso beschreibt es einen Fehler von Maßnahmen oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte. Hierbei kann es sich auch um Hinweise auf Fehlverhalten handeln (Indicators of Compromise, IoC).

„Informationssicherheitsvorfall“:

Informationssicherheitsvorfälle sind Informationssicherheitsereignisse mit konkreter und nachweisbarer Verletzung der Informationssicherheitsgrundwerte, Verstößen gegen Informationssicherheitsvorgaben oder -Maßnahmen, Umgehungen von Sicherheitsmechanismen und insbesondere Angriffe oder mutmaßliche Angriffe. Einem Informationssicherheitsvorfall können ein oder mehrere Informationssicherheitsereignisse vorausgehen.

„Krise“: Eine Krise liegt vor, wenn eine Störung zu einem Notfall wurde und dieser Notfall mit bestehenden Notfallplänen nicht oder nur bedingt behoben werden kann, bzw. wenn kein Notfallplan vorhanden ist.

„Notfall“: Ein Notfall stellt eine besondere Form der Störung mit einer signifikanten Unterbrechung des Geschäftsbetriebs oder ein Informationssicherheitsvorfall mit einer signifikanten Gefährdung der Informationssicherheit der FDG dar. Durch dieses Ereignis kann die Verfügbarkeit, der betroffenen Prozesse und / oder Ressourcen möglicherweise nicht innerhalb der geforderten Zeit wiederhergestellt werden bzw. die Integrität und / oder Vertrau-

lichkeit von Informationen nicht (mehr) sichergestellt werden. Der Geschäftsbetrieb ist durch das Eintreten eines Notfalls stark beeinträchtigt oder kann stark beeinträchtigt werden. Ein Notfall kann durch die fortschreitende Beeinträchtigung der Geschäftsprozesse zu einem Disaster bzw. einer Krise führen.

„privilegierte Rechte“: Zusätzliche Rechte, die über die für eine regelmäßige Nutzung hinausgehen, jedoch keine Administrationsrechte sind

„(Disaster) Recovery“:

(a) Gesamtheit der Tätigkeiten nach einem Incident im Rahmen des Incident, Problem und Service Conituity Managements nach ITIL, die dazu führen, dass ein Configuration Item und / oder eine Leistung wiederhergestellt ist, d. h. regulär gemäß den Vereinbarungen betrieben wird

(b) Tätigkeiten der Wiederherstellung von Daten aus dem Backup (siehe Datensicherung), auch Restore

„Schutzbedarf“: Feststellung des notwendigen Grades von Verfügbarkeit, Vertraulichkeit und Integrität von Informationen und Werten

„Schwachstelle“: Sicherheitsrelevanter Fehler eines Systems, einer Instanz oder eines Prozesses. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Instanz oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Instanz oder ein System) anfällig für Bedrohungen.

„Stable Release“: Durch den Hersteller veröffentlichter, getesteter und als stabil gekennzeichneter Release, welcher nicht mehr innerhalb des Releases geändert wird.

2 ZIELE

2.1 Grundsätzlich dürfen weder durch bestimmungsgemäßes noch durch fehlerhaftes Verhalten der Informationssysteme oder der Anwender Wettbewerbsnachteile für die Kunden entstehen oder das Anwendbare Recht bzw. sich aus gesetzlichen Anforderungen ergebende Handlungsaufträge des jeweiligen Kunden (z.B. sichere Energieversorgung) verletzt werden. Dies bedeutet, dass

– der Geschäftsbetrieb weder unterbrochen noch nachhaltig beeinträchtigt werden darf,
– die für die Vertragsparteien relevanten Gesetze und Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen eingehalten werden,
– Unbefugte keinen Zugang zu Betriebsgeheimnissen sowie durch gesetzliche Bestimmungen geschützten Informationen erhalten dürfen und ein unkontrollierter Abfluss und / oder Manipulation von Daten, Kenntnissen und Informationen (nachfolgend zusammengefasst „Informationen“ genannt) verhindert wird,
– ein Schwachstellenmanagement unter anderem im Rahmen der kontinuierlichen Schwachstellenanalyse und des Softwareverteilungsservices von Updates von Software durchgeführt wird,
– durch Sicherheitsmängel im Umgang mit IT verursachte Ersatzansprüche, Schadensregulierungen und Image-Schäden infolge fehlerhafter Daten oder Systeme – etwa infolge der Verbreitung von Computerviren – vermieden werden müssen, sowie
– Informationen und IT-Systeme des jeweiligen Kunden nicht unberechtigt verändert, gelöscht oder anderweitig manipuliert werden dürfen.

2.2 Den Mitarbeitern und Nutzern des AUFTRAGGEBERS müssen die benötigten Daten und Systemressourcen durch den AUFTRAGNEHMER rechtzeitig, vollständig und fehlerfrei bereitgestellt werden. Gleichzeitig sind Zugriffe Unbefugter durch den AUFTRAGNEHMER zu verhindern. Der AUFTRAGNEHMER hat die von ihr eingesetzten Personen zu verpflichten, Informationen und die zur Verfügung gestellten Kommunikationsmittel gegen Verlust, Verfälschung bzw. Beschädigung und Missbrauch jeglicher Art zu schützen und die eingesetzten Arbeitsmittel mit der gebotenen Sorgfalt zu behandeln.

2.3 Der AUFTRAGGEBER und der AUFTRAGNEHMER schützen die Informationen gemäß den Grundwerten der Informationssicherheit („Informationssicherheitsgrundwerte“):

– Verfügbarkeit: Die Verfügbarkeit von Informationen, Systemen und Infrastruktur wird sichergestellt, so dass alle Systeme und Informationen, auf die von dem AUFTRAGGEBER vorgesehene bzw. intendierte Art und Weise genutzt werden können. Die Informationen, Systeme und Infrastrukturen sind so zu sichern, dass die vereinbarten Service Level eingehalten werden.
– Vertraulichkeit: Informationen werden vor unbefugter Preisgabe geschützt und ausschließlich Befugten in der zulässigen Weise bereitgestellt.
– Integrität: Es wird die Korrektheit von Daten und die korrekte Funktionsweise von Systemen sichergestellt.
– Authentizität: Es wird gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein.

Auch in Katastrophenfall-Situationen ist abhängig von der jeweiligen Situation, einschließlich des beauftragten Leistungsumfangs ein Höchstmaß der Einhaltung dieser Schutzziele durch den AUFTRAGNEHMER sicherzustellen.

2.4 Jeder, der Informationen nutzt, ist im Rahmen von Vorgaben für deren Sicherheit verantwortlich. Jede Information muss bei der Erstellung im Rahmen von Vorgaben klassifiziert werden. Nicht klassifizierte Informationen sind als der Klasse -intern- zugehörig zu handhaben. Jede schützenswerte elektronische Information muss gesichert werden. Nur eindeutig ausgewiesene Personen mit entsprechender Befugnis erhalten Zugriff auf schützenswerte Informationen. Jeder Zugriff auf Informationen muss eindeutig erkennbar, nachvollziehbar und nachweisbar sein. Auf die Regelungen der Vereinbarung zur Vertraulichkeit wird weiterhin verwiesen.

Bezug: EN ISO/IEC 27001:2022 Kapitel 5.2, Kapitel 6.2, A.5.1, A.5.29, A.8.14

3 INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM UND ZERTIFIZIERUNGEN DER AUFTRAGNEHMER

3.1 Der AUFTRAGNEHMER stellt sicher, dass dieser ein Informationssicherheitsmanagementsystem („ISMS“) und entsprechende -prozesse gemäß den Vorgaben der EN ISO/IEC 27001 in der jeweils gültigen Fassung implementiert hat und dieses von unabhängiger Stelle entsprechend zertifiziert ist. Das ISMS des AUFTRAGNEHMERS muss sich sowohl auf den vertragsgegenständlichen Betrieb von Systemen und Technologien als auch auf diesbezügliche Projekte und alle weiteren von dem AUFTRAGNEHMER für den AUFTRAGGEBER erbrachte Leistungen erstrecken.

3.2 Diese Prozesse sowie entsprechende Rollen und Verantwortlichkeiten müssen als Teil der Informationssicherheitsrichtlinien des AUFTRAGNEHMERS dokumentiert sein. Die Richtlinien müssen den von dem AUFTRAGNEHMER eingesetzten Personen bekannt sein und regelmäßig, jedoch mindestens jährlich, auf Aktualität und Richtigkeit überprüft werden.

3.3 Im Rahmen der Umsetzung der Vorgaben und Maßnahmen der EN ISO/IEC 27001 in der jeweils gültigen Fassung orientiert sich der AUFTRAGNEHMER an den Handlungsempfehlungen der ISO 27002 sowie des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik („BSI“) in der jeweils gültigen Fassung.

3.4 Weiterhin weist der AUFTRAGNEHMER folgende Zertifizierungen zu Beginn der Vertragsverhältnisses nach und hält diese in der jeweils gültigen Fassung aufrecht:

– ISO/IEC 27017
– EN ISO/IEC 27018

Bezug: EN ISO/IEC 27001:2022 Kapitel 4.4, A.5.31, A.5.32

4 MITWIRKUNGSOBLIEGENHEITEN DES AUFTRAGGEBERS

Der AUFTRAGGEBER verpflichtet sich, folgende Mitwirkungsleistungen gemäß den Regelungen des Vertrages zu erbringen:

– Benennung des CISO
– interne Umsetzung der EN ISO/IEC 27001 in der jeweils gültigen Fassung für den zertifizierten Anwendungsbereich
– Der AUFTRAGGEBER trägt dafür Sorge, dass Zutritt durch den AUFTRAGGEBER oder durch eingesetzte Personen des AUFTRAGGEBERS zu gemeinsam mit dem AUFTRAGNEHMER genutzten Räumen und Einrichtungen (z.B. Unterverteiler) gemäß den Regelungen in Ziffer 18 dieser Anlage durchgeführt wird.

5 VDMI

Zu jeder Komponente sind die folgenden Verantwortlichkeiten angegeben:

– die Komponente wird durchgeführt [D], d. h. erbracht,

– die Erbringung der Komponente wird verantwortet [V], d. h. damit zusammenhängende Entscheidungen werden getroffen und die technische, organisatorische und wirtschaftliche Verantwortung unter den Regelungen des Vertrages getragen,

– AUFTRAGNEHMER: Bei einer Komponente muss mitgewirkt [M] werden, d. h. der AUFTRAGNEHMER prüft, berät und stellt erforderliche Informationen zur Verfügung.

– AUFTRAGGEBER: Bei einer Komponente wird mitgewirkt [M], d. h. ihrer Durchführung wird vorab zugestimmt, erforderliche Informationen und vereinbarte Beistellungen werden zur Verfügung gestellt und auf Anforderung des AUFTRAGGEBERS unterliegt die jeweilige Leistung einer Abnahme bzw. Freigabe.

– Ist berechtigt, über den Beginn der Erbringung einer Komponente, die Erbringung selbst und deren Ergebnis durch den jeweils anderen Vertragspartner informiert [I] zu werden.

Die Frequenz definiert, in welcher Häufigkeit die so definierte Komponente erbracht wird:

– Ständig, d. h. andauernd bzw. kontinuierlich im täglichen Regelbetrieb [S],

– Täglich, d. h. einmal innerhalb 1 (eines) Arbeitstages [T],

– Wöchentlich, d. h. einmal innerhalb 1 (einer) Kalenderwoche [W],

– Monatlich, d. h. einmal innerhalb 1 (eines) Kalendermonats [M],

– Quartalsweise, d. h. einmal innerhalb 1 (eines) Quartals [Q],
– Halbjährlich, d. h. einmal innerhalb 1 (eines) Kalenderhalbjahres [H],
– Jährlich, d. h. einmal innerhalb 1 (eines) Kalenderjahres [J],
– Einmalig, d. h. einmal innerhalb des Lebenszyklus der jeweiligen Leistungen, z. B. bei der Erstinbetriebnahme [E],
– Bei Bedarf, d. h. nur nach Identifizierung einer Notwendigkeit [B],
– Auf Anfrage, d. h. nur nach direkter separater Beauftragung [A].
Mit „Basis“ gekennzeichnete Leistungen sind in den zwischen den Parteien vereinbarten Preisen enthalten und werden nicht gesondert berechnet.
„Optionale“ Leistungen können vom AUFTRAGGEBER gesondert beauftragt werden.
Jede Komponente ist aus einem Gesamtkatalog entnommen und kann über eine eindeutige, nicht fortlaufende Nummer (ID) identifiziert werden

ID	Leistung	Basis / Optional	Häufigkeit	Verantwortlichkeit		Anmerkungen
				AUFTRAG-NEHMER	AUFTRAG-GEBER	
00500	**Sicherheitsmanagement**					
00501	Planung, Implementierung und Betrieb der Sicherheitsinfrastruktur (Hard- und Software) gemäß den Anforderungen des AUFTRAGGEBERS und den Regelungen des Vertrages	Basis	S	V/D	M/I	
00502	Koordinierung und Durchführung des AUFTRAGNEHMER-internen Business Continuity Managements / Geschäftsfortführungsplanung gemäß den Regelungen des Vertrages	Basis	S	V/D	M/I	
00503	Pflege der für die Leistungen erforderlichen Sicherheits-Einstellungen (inkl. Antivirus-Software, Einspielen aktueller Signaturen)	Basis	S	V/D	I	
00504	Überprüfung der Zugriffsberechtigungen auf Systeme und Ergreifen relevanter Sicherheitsmaßnahmen (Systemsicherheit)	Basis	S	V/D	I	
00505	Erstellung Berechtigungskonzept (Pflege von Admin-Usern, -Rollen und -Profilen)	Basis	E	V/D	M/I	sofern nicht durch den AUFTRAGGEBER vorgegeben
00506	Pflege des AUFTRAGNEHMER-internen Berechtigungskonzepts	Basis	B	V/D	I	
00507	AUFTRAGNEHMER-interne Berechtigungsvergabe gemäß dem erstellten Konzept und der Sicherheitsvorgaben des AUFTRAGGEBERS	Basis	S	V/D	M/I	
00508	Zeitnahe Information der definiteren Stellen bei erkannten Verstößen gegen die vereinbarten Sicherheitsvorgaben oder Angriffen auf Systeme von innen oder von außerhalb	Basis	B	V/D	I	
00509	Ergreifen von Gegenmaßnahmen zur Abwehr drohender Angriffe oder zur Behebung entdeckter Sicherheitsmängel	Basis	B	V/D	M/I	
00510	Abwehr vermuteter oder tatsächlicher Angriffe auf die Systeme von innen oder von außerhalb	Basis	B	V/D	M/I	
00511	Minderung der Auswirkungen erfolgter Angriffe	Basis	B	V/D	I	
00512	Identifizierung, Diagnose und Beseitigung von Incidents und Problems mit Sicherheitsrelevanz sowie Monitoring der Ergebnisse	Basis	B	V/D	I	

ID	Leistung	Basis / Optional	Häufigkeit	Verantwortlichkeit		Anmerkungen
				AUFTRAG-NEHMER	AUFTRAG-GEBER	
00513	Aufsetzen aktiver Maßnahmen zur künftigen Vermeidung von Störungen	Basis	B	V/D	M/I	Optional, sofern Umsetzung nicht mit angemessenem Aufwand möglich
00514	Unterstützung bei der Entwicklung von Sicherheitsstandards, Grundsätzen und Verfahren mit Best Practices	Basis	B	V/D	I	
00515	Entwicklung, Dokumentation und Wartung von Informationssicherheit relevanten Anforderungen, Standards, Verfahren und Grundsätze, einschließlich Umsetzung behördlichen Anforderungen im Betriebs- und Prozesshandbuch	Basis	B	V/D	I	Optional, sofern Umsetzung der behördlichen Anforderungen nicht mit angemessenem Aufwand möglich
00516	Kontinuierliche Sicherstellung des aktuellen Stands der Technik bzgl. Sicherheitsbezogenen Trends, Bedrohungen, häufigen Schwachstellen, definierten Standards, Prozessen und Verfahren, Grundsätzen sowie Best Practices	Basis	B	V/D	I	
00517	Durchführung jährlicher Sicherheits-Assessments durch Fachpersonal	Basis	J	V/D	I	
00518	Bereitstellung von qualifizierten Ansprechpartnern für den AUFTRAGGEBER	Basis	B	V/D	I	
00519	Bereitstellung eines Security-Konzeptes auf Basis der relevanten Security Anforderungen, Standards, Verfahren, Grundsätze sowie Anforderungen des AUFTRAGGEBERS	Basis	E	V/D	I	
00520	Bereitstellung und Empfehlung von branchen- und servicespezifischen Best Practices für IT Service Continuity und Disaster Recovery Services	Basis	B	V/D	I	
00521	Dokumentation von IT Service Continuity und Disaster Recovery Services-Verfahren	Basis	B	V/D	M/I	
00522	Entwicklung und Pflege eines detaillierten Disaster Recovery Plans	Basis	B	V/D	I	
00523	Durchführung von Disaster Recovery Tests gemäß Vorgaben des AUFTRAGGEBERS	Basis	B	V/D	M/I	

6 UNTERAUFTRAGNEHMER

Der Einsatz von Unterauftragnehmern durch den AUFTRAGNEHMER richtet sich nach den vertraglichen Regelungen. Dabei sind Art und Umfang der Arbeiten der Unterauftragnehmer durch den AUFTRAGNEHMER kontinuierlich zu überwachen, zu dokumentieren und dem AUFTRAGGEBER auf Anfrage, mindestens jedoch einmal kalenderjährlich unaufgefordert zur Prüfung vorzulegen. Der AUFTRAGNEHMER stellt dem AUFTRAGGEBER eine transparente Darstellung der Lieferkette zur Verfügung und aktualisiert diese entsprechend. Die Anforderungen dieses Dokumentes in Bezug auf Informationssicherheit finden auch bei Änderungen der Unterauftragnehmer bzw. Lieferkette grundsätzlich Anwendung; abweichend dürfen Cloudleistungen von ISO/IEC 27001 zertifizierten Cloud-Anbietern nach deren Standardprozessen bezogen werden, wenn der AUFTRAGGEBER die betreffenden Cloud-Anbieter bereits über Direktverträge nutzt. In anderen Fällen gilt das, wenn diese den gleichwertigen Mindestanforderungen entsprechen. Weiterhin bleiben im Zusammenhang mit der Verarbeitung personenbezogener Daten die Regelungen der Vereinbarung zur Auftragsverarbeitung unberührt. Soweit hier Regelungen über technische und organisatorische Maßnahmen betroffen sind, gelten diejenigen Regeln, die einen höheren Schutz bieten. Vorrang genießen Datenschutzvereinbarungen, soweit dies zur Wirksamkeit der jeweiligen nach Datenschutzrecht erforderlichen Vereinbarung erforderlich ist. In diesem Zusammenhang ist auch der Ort der Datenverarbeitung zu dokumentieren.

Bezug: EN ISO/IEC 27001:2022 A.8.30, A.5.19, A.5.20, A.5.21, A.5.22

7 VORGABEN AN DIE ZUSAMMENARBEIT

7.1 Kooperation

Der AUFTRAGNEHMER verpflichtet sich, den AUFTRAGGEBER vollumfänglich in Bezug auf das Management der Informationssicherheit im Rahmen der Vertragsbeziehungen zu unterstützen, insbesondere durch Bereitstellung der notwendigen Informationen zur Erfüllung gesetzlicher Anforderungen durch den jeweilgen Kunden (z. B. Melde- und Berichtspflichten).

Dies umfasst auch die Unterstützung des AUFTRAGGEBERS durch den AUFTRAGNEHMER im Rahmen der gesetzlichen Verpflichtungen (u.a. gemäß BSIG, DSGVO), insbesondere die aktive Mitwirkung bei Prüfungen, unverzügliche Bereitstellung von durch den AUFTRAGGEBER angeforderten Nachweisen und dokumentierte Informationen und die zielgerichtete und zuverlässige Kooperation mit Dritten wie externen Auditoren.

Bezug: EN ISO/IEC 27001:2022 A.5.2, A.5.5, A.5.6, A.5.8

7.2 Aufgabentrennung

Der AUFTRAGNEHMER gewährleistet eine Trennung von Aufgaben und Verantwortungsbereichen sowie von Rollen und Personen, welche zueinander in Widerspruch geraten können, insbesondere hinsichtlich der Kontrolle bzw. Genehmigung und der Durchführung. Dies kann auch im Rahmen äquivalenter organisatorischer Maßnahmen geschehen, z. B. im Rahmen eines Vier-Augen-Prinzips.

Bezug: EN ISO/IEC 27001:2022 A.5.2, A.5.5, A.5.6, A.5.8

7.3 Kommunikations- und Meldewege

7.3.1 Beide Vertragsparteien benennen jeweils einen Verantwortlichen sowie einen Vertreter, welche zudem über ausreichend Befugnisse in Bezug auf Kommunikation und Abstimmungen zur Informationssicherheit verfügen.

7.3.2 Kommunikation im Zusammenhang mit Informationssicherheit hat grundsätzlich über diese Ansprechpartner zu erfolgen. Der AUFTRAGNEHMER muss den Ansprechpartner jeweils unverzüglich über möglicherweise erhebliche beeinflussende Sachverhalte informieren, sofern diese nicht

über den Ansprechpartner erfolgen. Bei Veränderungen der Besetzung dieser Rollen informiert die betreffende Vertragspartei unverzüglich per E-Mail die jeweilig andere Vertragspartei über den neuen Rolleninhaber.

7.3.3 Erkennt oder vermutet eine vom AUFTRAGNEHMER eingesetzte Person Schwächen in der Informationssicherheit, einen Sicherheitsvorfall oder ein Ereignis / Event mit Relevanz für die Informationssicherheit, ist unverzüglich der benannte Ansprechpartner des AUFTRAGGEBERS gemäß jeweiligen Maßgaben des AUFTRAGGEBERS zu informieren. Jegliche weitere Kommunikation mit dem AUFTRAGGEBER hat über die benannten Ansprechpartner zu erfolgen. Im Hinblick auf Cloudleistungen Dritter gilt, dass der jeweilige beauftragte Cloud-Provider ebenso über entsprechende Verfahren verfügt. Ungeachtet dessen erfolgt eine gesonderte Meldung über den AUFTRAGNEHMER an den AUFTRAGGEBER.

7.3.4 Jegliche Information über Informationssicherheitsvorfälle gilt als vertrauliche Information. Pressemeldungen / Veröffentlichungen von Informationssicherheitsthemen in Bezug auf die unter dem Vertrag durch den AUFTRAGNEHMER erbrachten Leistungen werden ausschließlich durch den jeweiligen Kunden veröffentlicht.

7.3.5 Der AUFTRAGNEHMER stellt sicher, dass in Bezug auf sicherheitsrelevante Ereignisse eine ununterbrochene 24/7/365-Erreichbarkeit des AUFTRAGNEHMERS für den AUFTRAGGEBER gegeben ist.

Bezug: EN ISO/IEC 27001:2022 A.5.24, A.6.8

7.4 Mitteilung des Schutzbedarfs und Maßnahmenableitung

7.4.1 Der AUFTRAGGEBER teilt nach freiem Ermessen dem AUFTRAGNEHMER schriftlich oder per E-Mail mit, welcher Schutzbedarf hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der Informationen, Systeme und Technologien besteht. Der AUFTRAGGEBER ist berechtigt, den Schutzbedarf nach freiem Ermessen jederzeit anzupassen. Der AUFTRAGNEHMER berät den AUFTRAGGEBER bei der Umsetzung seines Schutzbedarfs im Rahmen der durch den Cloudanbieter angebotenen Möglichkeiten und weist aktivg auf mögliche Umsetzungsdefizite hin.

7.4.2 Der AUFTRAGNEHMER ist verpflichtet, den mitgeteilten Schutzbedarf des AUFTRAGGEBERS im Rahmen der Informationssicherheitsrisikobeurteilung und Informationssicherheitsrisikobehandlung in Bezug auf alle für das Vertragsverhältnis zwischen den Vertragsparteien relevanten Assets zu berücksichtigen und alle notwendigen Maßnahmen zur Erfüllung der Vorgaben hinsichtlich der Schutzbedarfe abzuleiten und umzusetzen, insbesondere, im Rahmen seines ISMS. Der AUFTRAGNEHMER teilt dem AUFTRAGGEBER unverzüglich nach Abschluss der Prüfungen mit, durch welche Maßnahmen der Schutzbedarf von Informationen, Systemen und Technologien gewährleistet werden soll. Der mitgeteilte Schutzbedarf und die relevanten Maßnahmen werden zwischen den Vertragsparteien abgestimmt und dokumentiert. Abweichungen, bspw. aufgrund beschränkter Möglichkeiten seitens des ausgewählten Cloudanbieters, werden dem AUFTRAGGEBER proaktiv als Ausnahmen zur Beurteilung und Bestätigung vorgestellt. Das gilt nicht, wenn der AUFTRAGGEBER die betreffenden Cloud-Anbieter bereits über Direktverträge nutzt.

7.4.3 Teilt der AUFTRAGGEBER keine Einschätzung zum Schutzbedarf von Informationen, Systemen und Technologien mit bzw. stellt keine Informationssicherheitsanforderungen, so hat der AUFTRAGNEHMER den Schutzbedarf selbst nach dem aktuellen Stand der Technik sowie eigenen Kenntnissen und Erfahrungen festzulegen und den AUFTRAGGEBER über diese Festlegung unverzüglich zu informieren. Diese Festlegung gilt so lange, bis der AUFTRAGGEBER abweichende oder ergänzende Vorgaben an den AUFTRAGNEHMER kommuniziert.

Beim Einsatz von Unterauftragnehmern liegen die Genehmigungs- und Kontrollrechte bei dem AUFTRAGGEBER. Dabei sind Art und Umfang der Arbeiten der Unterauftragnehmer durch den AUFTRAGNEHMER zu dokumentieren. Der AUFTRAGNEHMER stellt sicher, dass auch Unterauf-

tragnehmer bezogen auf für den AUFTRAGGEBER erbrachte Leistungen auf die Einhaltung der in diesem Dokument festgelegten Vorgaben vertraglich verpflichtet sind.Wenn der AUFTRAGGEBER die betreffenden Cloud-Anbieter bereits über Direktverträge nutzt und hiervon abweichende Regelungen getroffen hat, dürfen sie auch hier zur Anwendung kommen. In anderen Fällen gilt nach ISO/IEC 27001 zertifizierte Cloud-Anbieter dürfen bei der Erbringung von Cloudleistungen ihren zertifizierten internen Vorgaben folgen, insofern sie dem vereinbarten Mindeststandard entsprechen.

Bezug: EN ISO/IEC 27001:2022 Kapitel 6.1, Kapitel 8.2, Kapitel 8.3, A.5.24, A.6.8

8 UMGANG MIT INFORMATIONSSICHERHEITSEREIGNISSEN UND -VORFÄLLEN

8.1 Meldungen bzw. Erkenntnisse zu Informationssicherheitsereignissen, Informationssicherheitsvorfällen und Informationssicherheitsnotfällen oder Datenschutzverletzungen sind durch den AUFTRAGNEHMER gemäß der Tabelle in Ziff. 8.6 zu klassifizieren und unter Berücksichtigung der definierten Meldefristen an den bzw. die entsprechenden Empfänger des AUFTRAGGEBERS qualifiziert zu melden. Abweichend werden im Hinblick auf Cloudleistungen über den AUFTRAGNEHMER dem AUFTRAGGEBER die nach ISO/IEC 27001 standardisierten Klassifizierungen und Meldungen des Cloudanbieters nach Möglichkeit automatisiert, bereitgestellt und im Nachgang auf Grundlage der vorliegenden Erkenntnisse einer Klasse nach der genannten Tabelle zugeordnet.

8.2 Informationssicherheitsereignisse sind potenzielle Hinweise (Indikatoren) auf Informationssicherheitsvorfälle; im Rahmen eines Informationssicherheitsereignisses oder Informationssicherheitsvorfalls kann die Möglichkeit einer konkreten Verletzung der Informationssicherheitsziele (Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität) nicht ausgeschlossen werden. Informationssicherheitsereignisse können zum Beispiel in Form einer Meldung eines Mitarbeiters oder eines technischen Systems (insbesondere Informationssicherheitssystems) vorliegen.

8.3 Informationssicherheitsvorfälle sind Informationssicherheitsereignisse mit konkreter und nachweisbarer Verletzung der Informationssicherheitsgrundwerte, Verstößen gegen Informationssicherheitsvorgaben oder -Maßnahmen, Umgehungen von Sicherheitsmechanismen und insbesondere Angriffe oder mutmaßliche Angriffe. Einem Informationssicherheitsvorfall können ein oder mehrere Informationssicherheitsereignisse vorausgehen.

8.4 Verletzungen des Informationssicherheitsgrundwerts Verfügbarkeit, die auf nicht dolose Ursachen (im Sinne zumindest bedingt vorsätzlichen Verhaltens; nicht dolos sind z.B. technisches Versagen oder Bedienerfehler in Abgrenzung zu einem Versuch, sich unberechtigt Zugriff auf einen fremden Account zu verschaffen) zurückzuführen sind, werden nicht als Informationssicherheitsvorfall, sondern als Störung im Rahmen des Incident Managements behandelt.

8.5 Im Rahmen der Meldung eines Informationssicherheitsvorfalles ist dem AUFTRAGGEBER unverzüglich eine Einschätzung über potenzielle Ursache, entstandene Schäden sowie ergriffene bzw. zu ergreifende Sofortmaßnahmen zu melden. Dies umfasst auch Maßnahmen in Bezug auf die Sicherung von etwaigen Beweismaterialien. Soweit und sofern notwendig, sind bei Änderungen der vorgenannten Inhalte bzw. neuen Erkenntnissen unverzüglich Ergänzungsmeldungen an den AUFTRAGGEBER zu übermitteln.

8.6 Informationssicherheitsvorfälle sind durch den AUFTRAGNEHMER gemäß den Maßstäben der folgenden Tabelle für alle Kriterien zu klassifizieren. Die Gesamtklasse eines Informationssicherheitsvorfalls wird durch Abwägung der jeweiligen Einstufungen der Einzelkriterien ermittelt, dabei ist im Zweifelsfalle die höhere Gesamtklasse zu wählen. Unter Würdigung des Gesamt-Bildes kann auch die niedrigere Klasse gewählt werden, z.B. wenn eine erkannte Schwachstelle in einem Geschäftsprozess mit sehr hoher Kritikalität, ggfs. mit Hilfe eines Workarounds, nicht ausnutzbar ist oder die Schwachstelle eine niedrigere Gefährdung darstellt. In berechtigten Fällen kann der AUFTRAGGEBER verlangen, eine gemeinsame Neubewertung der Klassifizierung des Vorfalls vorzunehmen.

Ebenso kann im Bearbeitungsprozess bei Vorliegen weiterer Erkenntnisse ein Vorfall neu klassifiziert werden.

Klasse des Vorfalls	Kriterium Beschreibung möglicher Auswirkungen (nicht abschließende Beispiele)	Schutzbedarf der vom Informationssicherheitsvorfall betroffenen Informationen bzw. *CIs*	Kritikalität der vom Informationssicherheitsvorfall betroffenen Geschäfts-prozesse	Ursachen des Informationssicherheitsvorfalls
3 mäßig	Geringe Auswirkungen auf den jeweiligen Kunden, z. B. - Versuchte Angriffe ohne negative Auswirkung - Finanzielle Schäden von voraussichtlich insgesamt bis zu EUR 15.000,00 - Maximal zu vernachlässigende Beeinträchtigung des Ansehens oder Vertrauens für den jeweiligen Kunden - Manipulation unsensibler Daten (z. B. Speisepläne) – Leichte Beeinträchtigungen von Geschäftsprozessen	Normal / mäßig / Nicht definiert	gering – mittel / nicht definiert	bekannte nicht-dolose Ursachen
2 schwer-wiegend / hoch	Größere Auswirkungen auf den jeweiligen Kunden, z. B. - Geringfügige Verstöße gegen Vorschriften, Verträge oder Gesetze (z.B. geringe Bußgelder / Strafen) - Finanzielle Schäden von voraussichtlich insgesamt bis zu EUR 25.000,00 - Einzelne Missbräuche personenbezogener Daten - Maximal geringfügige (z.B. intern) Beeinträchtigung des Ansehens oder Vertrauens für den jeweiligen Kunden - Abfluss einzelner Vertraulicher Informationen; keine Veröffentlichung von Geschäftsgeheimnissen - Manipulation einzelner sensibler Daten oder Systeme - Kurzfristige (voraussichtlich < 2 (zwei) h) Beeinträchtigungen von Geschäftsprozessen	hoch	hoch	unbekannte Ursachen, bekannte dolose und ungezielte Ursache (z.B. erfolgreiche Vireninfektion)
1 kritisch	Kritische Auswirkungen auf den jeweiligen Kunden, z. B. - Schwerwiegende Verstöße gegen Vorschriften, Verträge oder Gesetze - Finanzielle Schäden von voraussichtlich über EUR 25.000,00 - Massiver Missbrauch personenbezogener Daten - Beeinträchtigung für Leib und Leben - Weitreichende Beeinträchtigung (z. B. bei Politik & Presse) des Ansehens oder Vertrauens für den jeweiligen Kunden - Massiver Abfluss Vertraulicher Informationen oder einzelner Geschäftsgeheimnisse - Massive Manipulation sensibler Daten oder mehrere Systeme - Langwierige (voraussichtlich > 2 (zwei) h) Beeinträchtigungen von Geschäftsprozessen	sehr hoch / kritisch	sehr hoch	bekannte dolose und gezielte Ursachen (z. B. vorsätzliche Manipulation)

8.7 Informationssicherheitsvorfälle sind durch den AUFTRAGNEHMER gemäß der folgenden Tabelle unter Berücksichtigung der definierten Meldefristen den entsprechenden Empfängern des AUFTRAGGEBERS qualifiziert zu melden:

Klasse	Meldefrist	Empfänger des AUFTRAGGEBERS
3 mäßig	schnellstmöglich, jedoch spätestens nächster Arbeitstag	**via e-Mail:** IT-Security@sita-airport-it.aero
2 schwerwiegend / hoch	unverzüglich	**via e-Mail:** IT-Security@sita-airport-it.aero sowie telefonisch an die benannten IT-Notfallkontakte des AUFTRAGGEBERS
1 kritisch	unverzüglich	**via e-Mail**: IT-Security@sita-airport-it.aero sowie telefonisch an die benannten IT-Notfallkontakte des AUFTRAGGEBERS

Die Form der Benachrichtigung per E-Mail ist mit dem AUFTRAGGEBER abzustimmen, insbesondere hinsichtlich Struktur und zu verwendenden Verschlüsselungen. Eine telefonische Meldung ist erst dann erfolgt, wenn ein direkter Kontakt (d. h. keine Sprachnachricht, SMS o. ä.) zu mindestens einem der Empfänger bestand.

8.8 Informationssicherheitsvorfälle der Klassen 1 und 2 sind durch den AUFTRAGNEHMER in Bezug auf ausgenutzte Schwachstellen, den Erfolg der entsprechenden (Gegen-) Maßnahmen und ggf. zu ergreifende Maßnahmen zur zukünftigen Verhinderung zu analysieren und zu bewerten. Bei Cloudleistungen ist der AUFTRAGNEHMER insoweit auf die seitens des Cloudanbieters im Einklang mit ISO/IEC 27001 standardmäßig bereitgestellten Informationen beschränkt und wird diese zur Bewertung heranziehen und bei Bedarf eigenen sachbezogenen Anreicherungen vornehmen. Der AUFTRAGGEBER ist bereits in dieser Phase einzubinden, sowie im Anschluss über die Ergebnisse der Analyse und Bewertung unverzüglich zu informieren und die entsprechenden, sich hieraus ergebenden Anmerkungen bzw. Maßgaben des AUFTRAGGEBERS sind durch den AUFTRAGNEHMER zu berücksichtigen.

8.9 Der AUFTRAGNEHMER wird im Falle eines Informationssicherheitsvorfalls die notwendigen Ressourcen zur Minderung und / oder Beseitigung des Informationssicherheitsvorfalls unverzüglich sowie den finalen Korrekturbericht innerhalb angemessener Frist bereitstellen.

8.10 Grundsätzlich sind sicherheitsrelevante Ereignisse einem Regelungsprozess zuzuführen. Fachverantwortliche, die Konzernsicherheit sowie weitere relevante Stellen sind in geeigneter Weise zu beteiligen.

8.11 Der AUFTRAGNEHMER unterstützt den jeweiligen Kunden auf Anforderung bei der Vorbereitung und Erstellung gesetzlicher Pflichtmeldungen und -informationen in Bezug auf die Informationssicherheit, beispielsweise bei Meldungen gemäß § 8b Abs. 4 BSIG und Art. 33, 34 DSGVO, Anlage 3 (DVO 1583/2019, Anlage 4 EASA Part-IS.

Bezug: EN ISO/IEC 27001:2022 A.5.25, A.5.26, A.5.27, A.5.28

9 GRUNDSÄTZLICHE VORGABEN FÜR INFORMATIONSSICHERHEITSMAßNAHMEN

Die Informationssicherheitsmaßnahmen des AUFTRAGNEHMERS orientieren sich an folgenden grundsätzlichen Vorgaben:

– Benutzerakzeptanz: Bei der Auswahl und Veränderung von Maßnahmen sind Auswirkungen auf die Benutzer der zu schützende Systeme und Informationen zu berücksichtigen. Die Wirkung der Maßnahmen sollte nicht zu einer Ineffizienz oder Fehleranfälligkeit in der Nutzung dieser Systeme und Informationen führen.
– Verbotsprinzip: Grundsätzlich sind alle Tätigkeiten untersagt, welche nicht ausdrücklich zur Erbringung vertragsgegenständlicher Leistungen erlaubt sind.
– Nachvollziehbarkeit: Es sind sämtliche administrativen Tätigkeiten (inklusive privilegierter Tätigkeiten, d.h. Tätigkeiten, die Auswirkungen haben, die über Aktionen eines Standardnutzers hinaus gehen) nachvollziehbar zu protokollieren (inklusive des jeweils aktiven Nutzers).
– Minimale Rechtevergabe: Berechtigungen sind immer nur im benötigten und angemessenen Umfang zu gewähren. Einer Anhäufung von Rechten ist vorzubeugen.
– Mehrfache Ebenen: Die Informationssicherheitsmaßnahmen sind so anzulegen, dass ein vielschichtiges System an Maßnahmen auch in der Tiefe der IT-Landschaft wirksam ist und nicht ausschließlich der Schutz der außenliegenden Schicht herbeigeführt wird (Defense in Depth).

10 ÄNDERUNG UND WARTUNG AN DER SICHERHEITSARCHITEKTUR

10.1 Änderungen an der vertragsgegenständlichen Sicherheitsarchitektur oder -konfiguration der AUFTRAGNEHMERS bedürfen der vorherigen Zustimmung des AUFTRAGGEBERS, außer wenn diese zur Vermeidung, Abwehr oder Eindämmung eines stattfindenden Informationssicherheitsvorfalls bzw. eines mit an hinreichender Sicherheit

grenzender Wahrscheinlichkeit stattfindenden Informationssicherheitsvorfalls (z. B. Angriffe von innen oder außen) oder auf Grund gesetzlicher Vorgaben durchgeführt werden müssen. In einem solchen Fall ist AUFTRAGGEBERS unverzüglich zu informieren und der operative Betrieb möglichst nicht zu gefährden. Sollte der Cloudanbieter seine Sicherheitsarchitektur und -konfiguration nach eigenem Ermessen ändern, gibt der AUFTRAGNEHMER die Kundeninformationen des Cloudanbieters unverzüglich an den AUFTRAGGEBER weiter und berät den AUFTRAGGEBER proaktiv zu den Auswirkungen der Änderungen. Dies mit besonderem Augenmerk auf den davon betroffenen Schutzbedarf möglichen Risiken und schlägt wo erforderlich kompensierenden Schutzmaßnahmen vor.

10.2 Durch geeignete Methoden ist durch den AUFTRAGNEHMER sicherzustellen, dass die installierten Sicherheitsmechanismen in regelmäßigen Intervallen auf einen aktuellen Stand gebracht werden. Dies umfasst insbesondere, aber nicht ausschließlich,

– aktuelle Systemreleases, -updates (z. B. Firmware, Betriebssysteme),
– Sicherheitspatches sowie Servicepacks der Hersteller von Hard- und Software zur Unterstützung bzw. Betrieb von Maßnahmen der Informationssicherheit sowie
– aktuelle Malware-Pattern.

Die Prüfung durch den AUFTRAGNEHMER in Bezug auf die Aktualität hat täglich zu erfolgen.

Bezug: EN ISO/IEC 27001:2022 Kapitel 8.1, A.7.13, A.7.14, A.8.32, A.8.7

11 VERANTWORTUNG FÜR WERTE

Für alle Verfahren, Maßnahmen, Informationen, Anwendungen und Systeme wird durch den AUFTRAGNEHMER ein Inventar („Asset-Management“) gepflegt und jeweils eine verantwortliche Person benannt, die für die Sicherstellung der Umsetzung der Vorgaben dieses Dokumentes verantwortlich ist. Diese Personen erteilen die notwendigen Zugriffsberechtigungen (Dateneigentümer-Prinzip) unter Beachtung des Schutzbedarfes gemäß Ziff. 7.4. Für alle verantwortlichen Funktionen sind durch den AUFTRAGNEHMER-Vertretungen einzurichten. Es muss mittels Unterweisungen und ausreichender Dokumentation durch den AUFTRAGNEHMER sichergestellt werden, dass AUFTRAGNEHMER-Vertreter ihre Aufgaben erfüllen können. Dem AUFTRAGGEBER sind auf Anforderung diese Werteübersichten zur Verfügung zu stellen. Abweichend werden bei Cloudleistungen ohne zuordenbare Assets die seitens des Cloudanbieters genutzten Assetes nicht berücksichtigt. Der AUFTRAGNEHMER wird jedoch die bestimmbaren Assets sowie die für den AUFTRAGGEBER innerhalb der Cloudleistung administrierten virtuellen Assets, sowie die digitalen Vermögenswerte gemäß Art. 2 (32) EU Data Act, inventarisieren.

Bezug: EN ISO/IEC 27001:2022 A.5.9, A.5.10

12 PERSONAL DES AUFTRAGNEHMERS

12.1 Information über Vorgaben des AUFTRAGGEBERS

Alle Beschäftigten und arbeitnehmerähnlichen Personen des AUFTRAGNEHMERS sowie auch sonstige vom AUFTRAGNEHMER eingesetzte Personen, welche Zugriff auf Informationen erhalten bzw. möglichen Zugriff haben und Systeme und Technologien bereitstellen und / oder betreiben, sind durch den AUFTRAGNEHMER unverzüglich mit dem Inhalt dieses Dokumentes sowie der aktuell gültigen und vom AUFTRAGGEBER an den AUFTRAGNEHMER kommunizierten „IT-Sicherheitsrichtlinien“ des AUFTRAGGEBERS vertraut zu machen. Neue von dem AUFTRAGNEHMER eingesetzte Personen, welche zukünftig Zugriff auf Informationen erhalten bzw. möglichen Zugriff erhalten und Systeme und Technologien bereitstellen und / oder betreiben, sind durch den AUFTRAGNEHMER vor Aufnahme der jeweiligen Tätigkeit entsprechend zu unterrichten und zu unterweisen.

Der AUFTRAGNEHMER stellt sicher, dass alle vom AUFTRAGNEHMER eingesetzte Personen die Vorgaben dieses Dokuments sowie der aktuell

gültigen und von dem AUFTRAGGEBER an AUFTRAGNEHMER kommunizierten „IT-Sicherheitsrichtlinien“ der Kunden einhalten.

Diese Ziffer findet für öffentliche Cloudleistungen und Cloudleistungen, für die keine diesbzgl. rechtlichen Anforderungen zur konkreten Bestimmung der Personen mit Zugriff bestehen, keine Anwendung. Ebenso ausgenommen ist Personal, welches lediglich für die Bereitstellung der für den Betrieb der vom Cloud-Anbieter bereitgestellten Basis-Infrastruktur eingesetzt wird.

Bezug: EN ISO/IEC 27001:2022 A.5.1

12.2 Schulung des Personals

Alle vom AUFTRAGNEHMER eingesetzte Personen, welche Zugriff auf Informationen erhalten bzw. möglichen Zugriff haben und Systeme und Technologien bereitstellen und / oder betreiben, sind durch den AUFTRAGNEHMER periodisch in Bezug auf aktuelle Erkenntnisse der Informationssicherheit und entsprechende (Verhaltens-) Vorgaben zu unterweisen und zu schulen, insbesondere im Hinblick auf Security Awareness, sowie rollenspezifische Schulungen für Administratoren und Softwareentwickler. Weiterhin sind zusätzliche Schulungen durchzuführen, sofern ein Defizit an Kenntnissen in Bezug auf Informationssicherheit bei damit befassten von dem AUFTRAGNEHMER eingesetzten Personen erkennbar ist. Qualifizierungsnachweise sind dem AUFTRAGGEBER auf Anfrage vorzulegen.

Bezug: EN ISO/IEC 27001:2022 Kapitel 7.3, A.6.3

12.3 Fachkenntnis

Der AUFTRAGNEHMER beauftragt nur Personen mit entsprechenden Tätigkeiten, die über entsprechende Kenntnisse und Fähigkeiten bezüglich Installation, Soft- oder Hardware, Wartung oder Betrieb der jeweiligen Systeme und Technologien verfügen. Dies gilt auch für mit Themen der Informationssicherheit oder Softwareentwicklung betraute Personen.

Bezug: EN ISO/IEC 27001:2022 Kapitel 7.2, A.6.1

12.4 Bereitstellung von Informationen zur Identität

Der AUFTRAGNEHMER stellt sicher, dass jede Person, die im Namen des AUFTRAGNEHMERS agiert und / oder welche einen entfernten oder lokalen Zugriff auf das Informationssystem des jeweiligen Kunden hat oder sich diesen verschaffen kann, Informationen zu ihrer Identität bereitstellt. Der AUFTRAGNEHMER stellt sicher, dass in seinem Namen kein Zutritt oder Zugang missbraucht wird.

Bezug: EN ISO/IEC 27001:2022 A.6.1, A.5.18

12.5 Verpflichtung des Personals

Der AUFTRAGNEHMER stellt sicher, dass von dem AUFTRAGNEHMER eingesetzte Personen die als Appendix A dieses Dokumentes beigefügte Verpflichtungserklärung zu Geheimhaltung, Datenschutz und Datensicherheit unterzeichnen. Soweit bereits gleichermaßen geeignete schriftliche Verpflichtungserklärungen der vom AUFTRAGNEHMER eingesetzten Personen vorliegen, ist eine zusätzliche Verpflichtung entbehrlich.

Bezug: EN ISO/IEC 27001:2022 A.6.2, A.6.5, A.6.6, A.5.34

12.6 Verbot privater Nutzung

Der AUFTRAGNEHMER stellt sicher, dass alle IT-Systeme, von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen des jeweiligen Kunden möglich ist, durch die vom AUFTRAGNEHMER eingesetzten Personen ausschließlich für dienstliche Zwecke genutzt werden; eine private Nutzung durch diese Personen ist nur zulässig, sofern der Zugriff auf die Ressourcen des jeweiligen Kunden in einem geschützten Bereich erfolgt der von den privaten Bereich getrennt ist. Im Übrigen dürfen private Komponenten bzw. Systeme der von dem AUFTRAGNEHMER eingesetzten Personen nicht für den Zugang zu- und Zugriff auf Systeme und Informationen des jeweiligen Kunden benutzt werden und dürfen nicht an Systeme bzw. Netze des AUFTRAGNEHMERS angeschlossen werden, die für den Zugriff auf Ressourcen des jeweiligen Kunden vorgesehen sind.

Bezug: EN ISO/IEC 27001:2022 A.5.10

13 SICHERHEITSÜBERPRÜFUNG

Der AUFTRAGNEHMER ist verpflichtet, nur sicherheitsüberprüftes bzw. zuverlässigkeitüberprüftes Personal zum Umgang mit sensiblen Informationen und Systemen des jeweiligen Kunden und / oder für den Zutritt zu bestimmten Betriebsstätten, Räumlichkeiten und / oder Anlagen des jeweiligen Kunden einzusetzen. Diesbezüglich relevante Informationen (insbesondere die Identifizierung und Bestimmung der sensiblen Informationen und Systeme sowie die Art der Sicherheitsüberprüfung) werden durch den AUFTRAGGEBER bestimmt. Die von den lokalen gesetzlichen Bestimmungen festgelegten Ausnahmen sind zu beachten.

Für erbrachte Cloudleistungen Dritter gilt, dass Cloudanbieter ihr Personal gemäß lediglich auf Basis der mit ISO/IEC 27001 stehender standardisierter interner Verfahren auf Sicherheit und Zuverlässigkeit prüfen, insofern dieses Personal keine Systeme, Anwendungen oder Services administrieren, die aufgrund rechtlicher Anforderungen eine Zuverlässigkeitsüberprüfung erfordern. Ebenso ausgenommen ist Personal, welches lediglich für die Bereitstellung der für den Betrieb der vom Cloud-Anbieter bereitgestellten Basis-Infrastruktur eingesetzt wird. Dieses Personal hat keinen Zutritt zu Betriebsstätten oder Räumlichkeiten des AUFTRAGGEBERS oder des AUFTRAGNEHMERS. Der Zugriff auf Systeme, Anwendungen und Services des AUFTRAGGEBERS darf nur unter der Aufsicht des AUFTRAGNEHMERS erfolgen.

Bezug: EN ISO/IEC 27001:2022 A.6.1

14 BEREITSTELLUNG, REPARATUR, WARTUNG, AUßERBETRIEBNAHME

Zur Sicherstellung einer einwandfreien Funktionalität und Sicherheit aller Technologien darf durch den AUFTRAGNEHMER ausschließlich getestete und von dem AUFTRAGGEBER freigegebene Hard- und Software eingesetzt werden. Die Freigabe darf nicht ohne wichtigen Grund verweigert werden. Mit Hinblick auf § 9b Abs. 3 BSIG dürfen kritische Komponenten, die im Zusammenhang mit der Erbringung der Leistungen unter KRITISVO fallen, ausschließlich mit einer Garantieerklärung der Vertrauenswürdigkeit des Herstellers eingesetzt werden. In den Assetverzeichnissen sind diese entsprechend zu kennzeichnen und die entsprechenden Garantieerklärungen dem AUFTRAGGEBER auf Verlangen unverzüglich vorzulegen.

Für Cloud-Anbieter kommt dieser Absatz nicht zur Anwendung, Cloud-Anbieter folgen ihren internen diesbezgl. Verfahren gemäß ISO/IEC 27001.

Änderungen (z. B. Neuaufbau, Ersatz, Wartungen, Reparaturen) an der Technologie dürfen durch den AUFTRAGNEHMER nur zu vorher angekündigten und durch den AUFTRAGGEBER genehmigten Zeitpunkten durchgeführt werden. Zu diesem Zweck werden regelmäßige Standard-Wartungsfenster vereinbart, die als grundsätzlich genehmigt betrachtet werden. Der AUFTRAGNEHMER wird die Nutzung der Wartungsfenster ankündigen, der AUFTRAGGEBER kann eine Verlegung aus sach-

lichem Grund bis zu 2 (zwei) mal verlangen. Im Übrigen kann der AUFTRAGGEBER grundsätzlich eine Verlegung aus wichtigem Grund verlangen.

Für Cloud-Anbieter gilt: Der Cloud-Anbieter kündigt Wartungsfenster mit einer angmessenen Frist vorher an. Das Wartungsfenster kann bei nicht exklusiv bereitgestellten Lösungen nicht verschoben werden.

Wird Hardware zur Wartung oder Reparatur an Dritte (auch Kurierdienste) weitergegeben, sind alle sensitiven Informationen, die sich auf Datenträgern befinden, vorher durch den AUFTRAGNEHMER oder durch von dem AUFTRAGNEHMER eingesetzte Personen sicher zu löschen oder die persistenten Datenträger aus dem Gerät zu entfernen bzw. wirksam vor dem Zugriff Dritter zu schützen, insbesondere durch eine geeignete Verschlüsselung.

Für Cloud-Anbieter gilt, dass die sichere Löschung im Service-Vertrag zu regeln ist und dabei den Vorgaben der ISO 27001 folgt.

Wartungen sind stets durch den AUFTRAGNEHMER zu protokollieren und die Ergebnisse der Wartungen zu dokumentieren.

Wird ein System bzw. bei Cloudservices der Service außer Betrieb genommen, sind die Informationen des jeweiligen Systems gemäß den Regelungen der Ziff. 40 zu behandeln.

Bezug: EN ISO/IEC 27001:2022 A.7.10, A.7.14, A.7.13, A.7.14, A.8.32

15 CHANGE MANAGEMENT UND PROJEKTE

15.1 Bei allen Leistungen sowie Veränderungen von Leistungen und zusätzlichen Leistungen (z.B. im Rahmen von Changes) sind die Informationssicherheitsziele und -maßnahmen durch den AUFTRAGNEHMER zu berücksichtigen und zu implementieren, insbesondere in Form von Informationssicherheit durch Technikgestaltung und durch angepasste Voreinstellungen („Security by Design“, „Security by Default“).

15.2 Das Change Management ist nach den Maßgaben des Vertrages durchzuführen. Bei jedem Change sind auch die Auswirkungen auf die Informationssicherheit, insbesondere anhand einer Risikoeinschätzung verbunden mit dem Change, zu berücksichtigen.

15.3 Im Rahmen von Projekten sind durch den AUFTRAGNEHMER angemessene Maßnahmen zur Sicherstellung der Informationssicherheit durchzuführen, insbesondere

– Definition von Zuständigkeiten für Projektsteuerung / -portfoliomanagement
– Integration von Informationssicherheit in Projektmethodik und -anforderungen (z. B. PRINCE II: Anpassung an Projektumgebung, Managen eines Phasenübergangs)
– Initiale Risikobewertung bei Projektantrag / Aufnahme in Projektportfolio
– Einbindung der Informationssicherheit in Konzeptualisierung
– Durchführung von Risikobeurteilung in früher Projektphase, Maßnahmenplanung und -umsetzung
– Berücksichtigung von Auswirkungen von Veränderungen von Informationssicherheitskonfigurationen auf Projekte
– Zuweisung spezifischer Rollen für Informationssicherheit, Kommunikationsplan
– Abbildung von Informationssicherheitsaspekten in der Zusammenarbeit mit Dritten
– Sicherstellung der Informationssteuerung und -klassifizierung
– Sicherstellung der Anforderungen in Bezug auf das geistige Eigentum, Schutz von Aufzeichnungen und des Schutzes von Geschäftsgeheimnissen
– Kontinuierliche Dokumentation
– Stichprobenprüfungen / -audits

Bezug: EN ISO/IEC 27001:2022 A.5.8, A.8.32

16 SYSTEMHÄRTUNG

16.1 Prinzip der minimalen Installationen

16.1.1 Der AUFTRAGNEHMER stellt sicher, dass das Prinzip der minimalen Installationen bei den für

den AUFTRAGGEBER betriebenen Systemen eingehalten wird. Auf den Systemen dürfen nur folgende Komponenten installiert sein:

(i.) Alle Softwarekomponenten, Dienste und Benutzerkonten, welche für die Anwendung bzw. für die technische Umsetzung des Service notwendig sind
(ii.) Alle für die Integration mit anderen Systemen für die technische Umsetzung des Service notwendigen Softwarekomponenten
(iii.) Für Wartungsanforderungen notwendige Softwarekomponenten

16.1.2 Die Nutzung von Dienstprogrammen, insbesondere solchen mit privilegierten Rechten, ist durch den AUFTRAGNEHMER besonders zu überwachen und zu kontrollieren.

16.1.3 Softwareversionen sind nur dann einzusetzen und bereitzustellen, wenn ein offizielles, stabiles und sicheres Release (Stable Release) für die Software unter dem entsprechend eingesetzten Betriebssystem-Release veröffentlicht wurde.

16.1.4 Jede eingesetzte Komponente muss in einer sicheren Konfiguration betrieben werden. Es ist grundsätzlich durch den AUFTRAGNEHMER davon auszugehen, dass die Standardeinstellungen der Hersteller diese Anforderung nicht erfüllen. Der AUFTRAGNEHMER hat diesbezüglich jede Standardeinstellung zu prüfen und entsprechend den Vorgaben des AUFTRAGGEBER zu konfigurieren. Der AUFTRAGNEHMER kann sich bei fehlenden diesbzgl. Vorgaben des AUFTRAGGEBERS oder eigenen Standards an Empfehlungen des BSI Grundschutzes oder bspw. der CIS Benchmarks orientieren. Die korrekte und vollständige Umsetzung der Härtungsmaßnahmen sind in wirksamer Weise vor der Produktivsetzung eigenverantwortlich vom AUFTRAGNEHMER zu validieren.

Bezug: EN ISO/IEC 27001:2022 A.8.18, A.8.19

16.2 Netzwerkzugänge

Durch den AUFTRAGNEHMER sind nicht benötigte Netzwerkzugänge zu deaktivieren und die Nutzung jedes Ports zu dokumentieren. Sofern der AUFTRAGNEHMER die Notwendigkeit der Netzwerkzugänge nicht beurteilen kann, so ist der AUFTRAGGEBER im Rahmen des regelmäßigen Reportings zu informieren. Der AUFTRAGNEHMER stellt sicher, dass nur zulässige Geräte an der Netzwerkkommunikation teilnehmen können. Weiterhin ist eine Segmentierung des Netzwerkes derart zu gestalten, dass Netzwerke in funktionalen Gruppen aufgeteilt sind. Netzübergänge sind in angemessener Weise (bspw. per Firewall) abzusichern.

Bezug: EN ISO/IEC 27001:2022 A.5.14, A.8.22

16.3 Konfigurationsstandards

Der AUFTRAGNEHMER stellt sicher, dass die AUFTRAGNEHMER-eigenen bzw. sofern definiert die vom AUFTRAGGEBER vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden. Änderungen sind stets zu dokumentieren.

Bezug: EN ISO/IEC 27001:2022 A.5.37

16.4 Umgehung von implementierten Sicherheitsmaßnahmen

Der AUFTRAGNEHMER stellt innerhalb seiner Einflusssphäre sicher, dass die Systeme frei von erkennbaren Möglichkeiten sind, die eine Umgehung der implementierten Sicherheitsmaßnahmen ermöglichen können, z. B. durch APT, Malware oder Backdoors. Die Funktionsfähigkeit der Sicherheitsmaßnahmen ist jederzeit zu überwachen (insbesondere durch automatisch prüfende Systeme, die nach den ihnen vorgegebenen Kriterien bei bestimmten Zuständen Aktionen auslösen („Watchdog“)) und ggf. unverzüglich wiederherzustellen.

Bezug: EN ISO/IEC 27001:2022 A.8.7, A.8.8, A.5.21

16.5 Schutzsysteme

16.5.1 Der AUFTRAGNEHMER stellt sicher, dass bei der Erbringung der Leistungen alle aktuellen Sicherheitsmechanismen, die geeignete administrative, technische und physische Maßnahmen zum Schutz der Integrität der Systeme und Daten des jeweiligen Kunden (z. B. personenbezogene Daten) vor unbeabsichtigter oder rechtswidriger Vernichtung, Änderung, unbefugter Offenlegung oder dem Zugriff durch Unbefugte beinhalten, effektiv eingesetzt werden, um die Integrität der Systeme und Daten des jeweiligen Kunden gemäß dem Anwendbaren Recht zu schützen. Verlangt der AUFTRAGGEBER vernünftigerweise eine Anpassung solcher Mechanismen oder die Ergreifung spezifischer Maßnahmen, die von dem AUFTRAGNEHMER bislang nicht eingesetzt werden, muss der AUFTRAGNEHMER einem solchen Verlangen unverzüglich nachkommen. Für Cloudleistungen Dritter gilt dies für die vom Cloudanbieter gemäß ISO/IEC 27001 angebotenen Werkzeuge und Konfigurationsmöglichkeiten. Abweichungen davon sind dem AUFTRAGGEBER proaktiv unter Angabe der Einschränkungen und ggfs. Anwendbarer Ersatzmechanismen vorzustellen und zu genehmigen.

16.5.2 Der AUFTRAGNEHMER stellt sicher, dass alle eingesetzten Schutzprogramme und -systeme (z. B. Firewalls, Virenscanner) einen effektiven und dauerhaften Schutz gewährleisten, stets über aktuelle Signaturen verfügen und Manipulationen verhindern. Es sind durch den AUFTRAGNEHMER angemessene Prozesse und Lösungen zu etablieren, um alle vertragsgegenständlichen Systeme frei von Schadsoftware jedweder Art zu halten. Der AUFTRAGNEHMER stellt sicher, dass Events aus allen Schutzsystemen in das Event und Incident Management eingebunden werden (z.B. SIEM Lösung).

16.5.3 Auf jedem durch den AUFTRAGNEHMER bereitgestellten und / oder betriebenen System, insbesondere allen Endgeräten der von dem AUFTRAGGEBER bezeichneten Nutzer, den vertragsgegenständlichen Systemen und Managementsystemen sowie den Systemen der Sicherheitsarchitektur, sind entsprechende Schutzsysteme, insbesondere Anti-Malware-Software (Endpoint-Protection), zu installieren und mit jeweils aktuellen Malware-Pattern zu betreiben. Für verschiedene Schutzzonen sind Schutzsysteme verschiedener Hersteller zu nutzen.

16.5.4 Sofern eine Antivirensoftware einen Malwarebefall auf einem System feststellt, so hat diese eine eigenständige Behebung des Befalls (z.B. Quarantäne) vorzunehmen. Sofern dies für Endgeräte der Nutzer des jeweiligen Kunden erfolgt, zeigt die Software dem betreffenden Nutzer eine entsprechende Nachricht auf dem Desktop an. Außerdem meldet sie den Befall und Status der automatisierten Bereinigung an ein Management-System des AUFTRAGNEHMERS und löst einen entsprechenden Sicherheitsvorfall aus. Für den Fall, dass die automatisierte Bereinigung fehlschlägt, erfolgt im Rahmen der Behandlung des Sicherheitsvorfalls eine manuelle Bereinigung durch den AUFTRAGNEHMER- für Cloudleistungen sind die vom Cloudanbieter gemäß ISO/IEC 27001 genutzten internen Verfahren und bereitgestellten Werkzeuge anzuwenden und bei Bedarf vom AUFTRAGNEHMER um wirksame Zusatzmaßnahmen zu ergänzen. Dazu nimmt der AUFTRAGNEHMER Kontakt mit der IT-Sicherheit und dem Nutzer des AUFTRAGGEBERS bzw. – sofern vom AUFTRAGGEBER entsprechend angewiesen und benannt – mit dem Nutzer des jeweiligen Kunden auf und bespricht mit diesem die individuell notwendigen Schritte. Bei einer erkannten Infektion informiert der AUFTRAGNEHMER den Verantwortlichen gem. Ziff. 8.7.

16.5.5 Der AUFTRAGNEHMER muss alle Datenmedien, die an den AUFTRAGGEBER ausgeliefert oder dieser auf andere Weise zur Verfügung gestellt werden, auf Malware, Viren und andere Programme, die sich potenziell schädlich auf die IT-Infrastruktur des AUFTRAGGEBERS auswirken können, mithilfe der Test- und Analyseprozesse (gemäß dem Stand der Technik) für die Erkennung solcher Programme untersuchen. Stellt der AUFTRAGNEHMER irgendwelche der oben genannten Programme fest, darf der AUFTRAGNEHMER das betreffende Datenmedium nicht an den AUFTRAGGEBER ausliefern oder auf andere Weise zur Verfügung stellen. Nach Absprache werden bezogen auf solche Vorfälle Beweise gesichert und die nächsten Schritte vom AUFTRAGNEHMER veranlasst (z.B. Ersatzbereitstellung, Abstimmung

mit dem AUFTRAGGEBER, Sicherung gegen Verbreitung von Schadsoftware).

Abweichend dürfen Datenmedien ersetzende Cloudleistungen von ISO/IEC 27001 zertifizierten Cloud-Anbietern nach deren Standardprozessen behandelt werden, wenn der AUFTRAGGEBER die betreffenden Cloud-Anbieter bereits über Direktverträge nutzt.

Bezug: EN ISO/IEC 27001:2022 A.8.7, A.8.22, A.8.20

17 PATCH-MANAGEMENT

Unbeschadet Ziff. 9 gilt: Der AUFTRAGNEHMER ist verpflichtet, in regelmäßigen Abständen, mindestens jedoch monatlich, die Release-Stände der eingesetzten Systeme auf Updates, Minor- und Major-Release-Changes zu prüfen, zu testen und derartige Changes nach Hersteller-Vorgaben durchzuführen. Der AUFTRAGGEBER wird durch den AUFTRAGNEHMER bei absehbaren Änderungen, insbesondere, aber nicht ausschließlich, bei auslaufenden Major-Releases ein Jahr im Voraus informiert. Der AUFTRAGGEBER wird rechtzeitig in die jährlichen AUFTRAGNEHMER-seitigen Planungen von Release- / Versionswechseln einbezogen. Der AUFTRAGGEBER kann Release- / Versionswechseln nur aus wichtigem Grund widersprechen.

Unbeschadet Ziff. 9 gilt: Emergency Patches oder ähnliche Updates bzw. Hotfixes mit Bezug zur Informationssicherheit sind entsprechend der in Ziff. 33 nach Kritikalität der unterliegenden Schwachstellen definierten Fristen durch den AUFTRAGNEHMER bereitzustellen.

Der AUFTRAGNEHMER erstellt nach Aufforderung und Maßgabe durch den AUFTRAGGEBER für im Patchzyklus adressierte Schwachstellen einen Bericht und stellt diesen dem AUFTRAGGEBER zur Verfügung. Der Bericht enthält mindestens detaillierte oder aggregierte Daten unter Berücksichtigung der Kritikalitätsstufe und des betroffenen Bereichs (Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität).

Für Cloudleistungen gilt diese Ziff. 17 abweichend mit der Maßgabe, dass der Cloudanbieter standardisierte interne Verfahren zum Patch Management gemäß ISO/IEC 27001 anwendet.

Bezug: EN ISO/IEC 27001:2022 A.7.13, A.8.32, A.8.8

17.1 Umfang

Der AUFTRAGNEHMER stellt sicher, dass das Patch-Management für alle Systeme und Technologien, welche für den AUFTRAGGEBER bereitgestellt / betrieben werden, sowie für alle indirekten, zur Erbringung der Leistungen unter dem Vertrag durch den AUFTRAGNEHMER genutzten Systeme (z. B. administrative Systeme des AUFTRAGNEHMER) durchgeführt wird. Zu diesen Systemen gehören insbesondere

– BIOS / Firmware
– Betriebssysteme
– alle Softwarepakete, welche Teil des Betriebssystems sind, z. B. Treiber
– alle Tools und Applikationen, welche der Hersteller der Systeme und / oder der AUFTRAGNEHMER zu Betriebs- und Wartungszwecken installiert hat,
– Zielapplikationen (i. S. d. Servicelogik) sowie
– alle Middleware-Application-Layer, Datenbanken, Access-, Monitoring- und Applikationsserver, eigene Softwareentwicklungen, welche für die Erbringung der Leistungen genutzt werden.

Sofern der Hersteller der Systeme ein Patch-Management der eingesetzten Komponenten nicht unterstützt, so wird der AUFTRAGNEHMER den AUFTRAGGEBER diesbezüglich informieren, auf mögliche Risiken hinweisen und eine Lösung abstimmen.

Bezug: EN ISO/IEC 27001:2022 A.8.32

17.2 Patch-Level während der Systemabnahme

Der AUFTRAGNEHMER stellt sicher, dass die dediziert für den AUFTRAGGEBER zu betreibenden, abzunehmenden bzw. freizugebenden Systeme zum Zeitpunkt der Abnahme bzw. Freigabe auf dem aktuellen, vom Hersteller/Lieferanten der Applikation freigegebenen Patch-Stand sind und muss alle verfügbaren und durch den AUFTRAGGEBER freigegebenen Patches als Teil der Lieferung bzw. Bereitstellung installieren. Eine Freigabe findet nach Maßgabe des AUFTRAGGEBERS statt.

Bezug: EN ISO/IEC 27001:2022 A.8.29

17.3 Funktionsfähigkeit bei Patches der unterliegenden Plattform

Sofern der AUFTRAGNEHMER reine Anwendungen und / oder andere Funktionalitäten liefert und der AUFTRAGGEBER oder Dritte (im Namen des AUFTRAGGEBERS) für das Update-Management auf den darunterliegenden Schichten verantwortlich sind, gewährleistet der AUFTRAGNEHMER eine kontinuierliche Funktionsfähigkeit seiner erbrachten Leistung auch bei Patches der unterliegenden Systemplattform.

Bezug: EN ISO/IEC 27001:2022 A.8.32

18 ZUGANGS-, ZUGRIFFS- UND ZUTRITTSSCHUTZ

Zugangs- und Zugriffsberechtigungen für Systeme und Informationen sind durch den AUFTRAGNEHMER nur in dem Umfang, wie für die Erbringung der Leistungen erforderlich zu erteilen und im Anschluss an die Beendigung der Erbringung der Leistungen unverzüglich zu entziehen bzw. anzupassen (Need-to-Know-, Need-To-Do-Prinzip). Zugriffsgenehmigungen werden nur so weit wie zur Erbringung der Leistungen erforderlich erteilt (Prinzip der Vergabe von minimalen Berechtigungen). Die Vergabe von Berechtigungen erfolgt über personalisierte Accounts, soweit nicht in den nachfolgenden Absätzen Abweichungen vorgesehen sind. Für Cloudleistungen Dritter zur Bereitstellung der Umgebung gilt dieser Absatz entsprechend, die folgenden Absätze dieser Ziffer 18 jedoch auf Basis der vom Cloudanbieter genutzten standardisierten internen Verfahren gemäß ISO/IEC 27001.

Gruppen-Accounts, d. h. Accounts für bestimmte Funktionen, bei welchem mehrere Personen das jeweilige Passwort kennen, sind nur nach vorheriger Genehmigung des AUFTRAGGEBERS für den jeweiligen Einzelfall einzurichten. Hierbei sind durch den AUFTRAGNEHMER auch die entstehenden Risiken und mögliche Gegenmaßnahmen zu beachten.

Funktionale Accounts, d. h. nicht für die interaktive Anmeldung vorgesehene Accounts, sind mit stärkeren Authentifizierungsmechanismen (z. B. zertifikatsbasiert oder mit hoch komplexen Passwörtern) abzusichern und die Authentifizierungsinformationen nach dem Need-to-know- und Need-To-Do-Prinzip zu schützen.

Zutritts-, Zugangs- und Zugriffsberechtigungen werden ausnahmslos auf Basis von Berechtigungskonzepten erteilt.

Ist der Zugriff auf Systeme mit einem hohen Schutzbedarf oder aus unsicheren Umgebungen (z.B. dem Internet) erforderlich, ist dieser durch starke Multi-Faktor-Authentifikationsmechanismen durch den AUFTRAGNEHMER zu schützen, z. B. in Bezug auf den Zugriff via Extranet (z.B. Telearbeit, VPN).

Für die Administration sind durch den AUFTRAGNEHMER sichere Basisprotokolle zu verwenden.

ITK-Infrastrukturen (z. B. Server, Rechenzentren, Verteilerräume) sind durch geeignete physische und logische Maßnahmen vor unerlaubten Zutritten, Umwelteinflüssen und Versorgungsengpässen zu schützen.

Bezug: EN ISO/IEC 27001:2022 A.5.16, A.5.18, A.8.5

18.1 Prozess, Prüfung

Der AUFTRAGNEHMER führt die Erteilung und den Entzug von Berechtigungen gemäß eines dokumentierten Prozesses aus; dies gilt auch für die unverzügliche Sperrung von Konten, bzw. Löschen von Berechtigungen bei Austritt oder Wechsel der Tätigkeit der Personen.

Der AUFTRAGNEHMER prüft zusätzlich quartalsweise die erteilten und entzogenen Zugangs- und Zugriffsberechtigungen für den AUFTRAGNEHMER, insbesondere von privilegierten Accounts, auf die korrekte Zuweisung, die Notwendigkeit und Angemessenheit sowie die erfolgte Durchsetzung von Änderungen bzw. der Entziehung und teilt dem AUFTRAGGEBER das Ergebnis der Prüfung unverzüglich mit.

Benutzer- und Gruppenkonten sind nach 60 Kalendertagen Inaktivität automatisiert zu sperren, sofern keine qualifizierte Bestätigung des Bedarfs solcher Konten durch eine berechtigte Stelle erfolgt ist. Nach weiteren 30 Kalendertagen sind den gesperrte Benutzer- und Gruppenkonten alle Berechtigungen zu entziehen und in eine berechtigungslose Gruppe zu verschieben und nach weiteren 30 Tagen zu löschen.

Bezug: EN ISO/IEC 27001:2022 A.5.16, A.5.18

18.2 Referenzdatenbank

Der AUFTRAGNEHMER stellt nach Maßgabe des AUFTRAGGEBERS eine Referenzdatenbank oder vergleichbare Übersicht bereit, in welcher alle Zutritt-, Zugangs- und Zugriffsanforderungen und Rechte fortlaufend mit Änderungsdaten und Gegenständen vorgenommener Änderungen aufgeführt sind. Der AUFTRAGGEBER hat das Recht, diese im Rahmen seiner Prüfungsrechte einzusehen.

Bezug: EN ISO/IEC 27001:2022 A.5.16, A.5.18, A.8.2, A.5.17

18.3 Verschlüsselung von Authentisierungsmerkmalen

Der AUFTRAGNEHMER stellt sicher, dass Authentisierungsmerkmale ausschließlich angemessen verschlüsselt übertragen werden.

Bezug: EN ISO/IEC 27001:2022 A.5.17

18.4 Vergabe von Administrationsrechten / privilegierten Accounts

18.4.1 Der AUFTRAGNEHMER stellt sicher, dass es sich bei Personen, die Administratorenrechte auf den produktiven Systemen des jeweiligen Kunden bzw. privilegierte Accounts haben, nicht um Werksstudenten, Praktikanten, Trainees, Auszubildende oder sonstige Personen mit einem dieser Personengruppen vergleichbaren Status handelt. Der AUFTRAGGEBER ist berechtigt, jederzeit die Logfiles einzusehen, um die Einhaltung dieser Verpflichtung durch den AUFTRAGNEHMER in angemessener Art und Weise zu prüfen. Auf Anfrage des AUFTRAGGEBERS teil der AUFTRAGNEHMER gegenüber dem AUFTRAGGEBER den jeweiligen arbeits- bzw. auftragsrechtlichen Status der dauerhaft oder auch nur vorübergehend eingesetzten Personen in pseudonymisierter Form schriftlich mit.

Von der vorstehenden Regelung können durch den AUFTRAGGEBER im Einzelfall Ausnahmen genehmigt werden; in diesem Falle stellt der AUFTRAGNEHMER sicher, dass die betreffende Person aus einer der o. g. Gruppen im Rahmen der Nutzung von Administrationsrechten stets durch eine berufene Person, welche nicht einer der o. g. Gruppen angehört, beaufsichtigt wird. Die weiteren Regelungen, insbesondere in Bezug auf die Protokollierung der Zugriffe, bleiben unberührt.

18.4.2 Das Prinzip der Vergabe von minimalen Berechtigungen ist für jedes vertragsgegenständliche System individuell durch den AUFTRAGNEHMER durchzusetzen.

18.4.3 Die Vergabe von Administrationsrechten hat auf Basis eines durch den AUFTRAGNEHMER zu erstellenden und zu pflegenden Zonenkonzepts

zu erfolgen; hierbei sind für verschiedene Systemgruppen bzw. Service-Layer (z. B. jeweils für Server, Applikationsebene, Clients, Domains, Informationssicherheitssysteme, Exchange und Kollaboration) verschiedene Administrationsaccounts vorzusehen; derselbe Account darf nicht in mehreren (> 1) Zonen über Rechte verfügen. Eine Benutzung desselben Accounts in verschiedenen Zonen ist durch den AUFTRAGNEHMER zu unterbinden und es sind entsprechende Maßnahmen zu ergreifen, insbesondere die Sperrung des Accounts für alle Zonen beim Versuch, diesen in einer anderen Zone zu nutzen.

18.4.4 An Benutzer des jeweiligen Kunden dürfen grundsätzlich keine Administrationsrechte vergeben werden, sondern es sind in Abstimmung mit dem AUFTRAGGEBER entsprechend privilegierte Rechte / Zugriffsrechte zu vergeben. Sofern Administrationsrechte an Benutzer des jeweiligen Kunden nach ausdrücklicher Aufforderung durch den AUFTRAGGEBER vergeben werden, sind durch den AUFTRAGNEHMER erweiterte Sicherungsmaßnahmen zu ergreifen, insbesondere, aber nicht ausschließlich, das Einrichten gesonderter Administrationsaccounts und ggf. Abbildung über Sandboxes / virtualisierten Betrieb. Der AUFTRAGNEHMER prüft in angemessener Weise, dass diese eingerichteten Administratorenaccounts nicht missbräuchlich genutzt werden und informiert bei Anzeichen der Zuwiderhandlung unverzüglich den AUFTRAGGEBER. Im Zusammenhang mit dem Exit-Prozess können die Parteien in Textform Abweichungen nach Maßgabe der Anlage 2 Exit Management der SAIT ZVB-IT abstimmen.

Bezug: EN ISO/IEC 27001:2022 A.8.2

18.5 Zutrittsschutz

Der Zutritt zu Bereichen mit Informationen oder Systemen mit erhöhtem Schutzbedarf wird durch den AUFTRAGNEHMER auf den durch ihn unter der Einhaltung der Vorgaben dieses Dokumentes hierzu autorisierten Personenkreis beschränkt. Dies umfasst auch die Zutrittsschutzmaßnahmen für Rechenzentren, insbesondere, aber nicht ausschließlich, die Überwachung der kritischen Bereiche, Zutrittsprotokollierungen, Einbruchsschutz und Absicherung des Perimeters. Für Büros, weitere Räume und Anlieferungs- und Ladebereiche trifft der AUFTRAGNEHMER entsprechende Maßnahmen zur Überwachung und Verhinderung des Zutritts unberechtigter Personen. Der AUFTRAGGEBER ist jederzeit berechtigt, eine Auflistung der autorisierten Personen (Name, Vorname, Geburtsdatum sowie Autorisierungsdatum) bei dem AUFTRAGNEHMER einzusehen.

Bezug: EN ISO/IEC 27001:2022 A.7.1, A.7.2, A.7.3

19 AUTHENTIFIZIERUNGSMAßNAHMEN

19.1 Grundsätze

Authentifizierungsmaßnahmen sind ein wichtiger Aspekt der Informationssicherheit. Sie stellen die erste Instanz zum Schutz der Nutzerkonten dar. Der AUFTRAGNEHMER ist dafür verantwortlich, die Vorgaben in Bezug auf die Wahl und die Absicherung der Authentifizierungsmaßnahmen einzuhalten.

Diese Vorgaben in Bezug auf Authentifizierungsmaßnahmen sind verbindlich für:

(i.) Personen, die einen Account besitzen oder dafür verantwortlich sind, welcher Zugriff auf Systeme des jeweiligen Kunden bzw. auf für den jeweiligen Kunden oder in dessen Auftrag betriebene Systeme ermöglicht und / oder
(ii.) Vertragsgegenständliche Systeme und Dienste, welche an einem Standort des jeweiligen Kunden betrieben werden, oder welche Zugriff auf das Netzwerk des jeweiligen Kunden haben, oder welche nicht-öffentliche Daten des jeweiligen Kunden speichern sowie für den administrativen Zugriff auf Systeme, welche öffentliche Daten des jeweiligen Kunden bereitstellen (z. B. Webserver).

Alle vom AUFTRAGNEHMER eingesetzten Personen, welche Zugriff auf Informationen des jeweiligen Kunden erhalten bzw. möglichen Zugriff haben

und Systeme und Technologien für den AUFTRAGGEBER bereitstellen und / oder betreiben, sind über diese Vorgaben zu unterrichten; dies umfasst auch Informationen zu sicheren Authentifizierungsmaßnahmen.

Es muss durch die Authentifizierung jederzeit ein eindeutiger Rückschluss auf eine bestimmte Person möglich sein und die Nutzung der Systeme darf nur nach vorheriger Authentifizierung möglich sein.

Bezug: EN ISO/IEC 27001:2022 A.5.17, A8.5

19.2 Durchsetzung mittels technischer Systeme

Für die Durchsetzung dieser Vorgaben sind technische Systeme durch den AUFTRAGNEHMER zu implementieren. Diese Systeme müssen die Authentifizierungsinformationen bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung schützen. Die Authentifizierungsinformationen sind getrennt von Applikationsdaten zu speichern, soweit die Systeme das unterstützen.

Bezug: EN ISO/IEC 27001:2022 A.8.5

19.3 Vorgaben für Authentifizierungsmaßnahmen

19.3.1 Die Wahl der Authentifizierungsmaßnahmen obliegt grundsätzlich dem AUFTRAGNEHMER, sofern diese als nicht kompromittiert gelten; hierbei ist auf Basis der Rollen der Account-Inhaber sowie der Systeme eine starke Authentisierung, mindestens eine Zwei-Wege-Authentifizierung auf Basis von „Wissen und Besitz (bzw. Inhärenz)“, vorzusehen. Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) erfolgt in einem geordneten Verfahren, das die Vertraulichkeit der Informationen sicherstellt.

19.3.2 Alle Authentifizierungsinformationen auf Benutzer-Ebene und Administrations-Ebene müssen – soweit technisch möglich – regelmäßig gewechselt werden. Selbiges gilt für Authentifizierungsmaßnahmen, welche kein automatisches, vom Hersteller vorgegebenes oder inhärentes Ablaufdatum haben. Ein Austausch von Token erfolgt nach den Vorgaben des Herstellers. Zertifikate dürfen mit einer maximalen Laufzeit von drei Jahren ausgestellt und müssen rechtzeitig vor dem Ablauf durch geordnete Verfahren ersetzt werden. Zertifikate, die für Dritte ausgestellt werden, dürfen eine maximale Laufzeit von zwei Jahren besitzen.

19.3.3 Der AUFTRAGNEHMER stellt sicher, dass jedes durch den Hersteller bzw. Produzenten gesetzte Standardpasswort unverzüglich geändert wird; sollte dies nicht möglich sein, darf das betreffende System nicht eingesetzt werden.

Initial zugewiesene Passwörter sind beim erstmaligen Gebrauch durch ein nutzergewähltes Passwort zu ersetzen. Dies ist systemseitig zu unterstützen, soweit diese das technisch unterstützen.

19.3.4 Sollte ein Authentifizierungsmechanismus kompromittiert werden oder Authentisierungsinformationen weiteren Personen zur Kenntnis gelangen, ist der Authentifizierungsmechanismus oder die Authentisierungsinformation unverzüglich zu wechseln bzw. der Account zu sperren.

19.3.5 Die Speicherung und Übermittlung der Authentisierungsinformationen sind durch den AUFTRAGNEHMER kryptographisch abzusichern.

19.3.6 Passwörter dürfen im Klartext nicht digital gespeichert werden; die Nutzung von Hinweisen, welche ein Kompromittieren erleichtert, ist ebenso untersagt. Die Verwendung eines Passwort-Safes mit hinreichend starker, marktüblicher Verschlüsselung und einem Logging des Zugriffs auf den Passwort-Safe ist zulässig. Die Regelungen dieses Dokuments und der weiteren Dokumente des Vertrages gelten auch für einen solchen Passwort-Safe, insbesondere in Bezug auf das Schreiben von Passwörtern auf Papier und die Vorgaben an das Passwort für den Passwort-Safe.

Bezug: EN ISO/IEC 27001:2022 A.5.17, A.8.5

19.4 Zusammensetzung von Passwörtern

Diese Unterziffer findet ebenso für Cloudleistungen Dritter Anwendung, wobei Technologieoffenheit z.B. hinsichtlich des Ersatzes von Passwörtern durch Zertifikate, Passkeys etc. oder SSO besteht.

19.4.1 Die Mindestlänge eines Passworts beträgt 12 (zwölf) Zeichen, ein rein zeitabhängiger Wechsel von Passwörtern soll nach Vorgabe des AUFTRAGGEBERS (bspw. alle 180 Tage) automatisiert erfolgen. Passwörter dürfen keine Teile / Zeichenfolgen der letzten Passwörter oder Worte aus Wörterbüchern (Deutsch, Englisch) enthalten.

19.4.2 Sollten die vorgenannten Vorgaben in einzelnen Systemen technisch nicht umsetzbar sein, so sind diese Ausnahmen zu dokumentieren sowie Risikoanalysen durchzuführen und wo erforderlich risikomindernde Maßnahmen umzusetzen.

19.4.3 Benutzer-Passwörter müssen sich aus Zeichen aus allen vier (4) Kategorien zusammensetzen:

– Großbuchstaben / Majuskeln (A – Z)
– Kleinbuchstaben / Minuskeln (a – z)
– Ziffern (0 – 9)
– Sonderzeichen (z. B. ! @ # $ % ^ & * ( ) _ + | ~ - = \ ‘ { } [ ] : " ; ’ < > ? ,), jedoch nicht Zeichen, welche nicht auf einer Standard-Tastatur mit deutschsprachigem Tastaturlayout gemäß jeweils gültiger Norm vorhanden sind.

19.4.4 Nicht zulässig sind Passwörter, welche:

– dem Benutzernamen entsprechen oder
– Teile / Zeichenfolgen des Benutzernamens von mehr als zwei aufeinanderfolgenden Zeichen entsprechen oder beinhalten oder
– einem der neun zuletzt genutzten Passwörter entsprechen oder diese beinhalten.
– Wörter aus dem Wörterbuch enthalten (Dictionary-Check)
– als bekannt komprimiert bestätigt sind.

Passwörter dürfen keine (Teil-)Zeichenfolgen der letzten (abgelaufenen) Passwörter enthalten.

19.4.5 Sollten die AUFTRAGNEHMER-internen Vorgaben an die Wahl des Passworts zu einer grundsätzlich höheren Passwort-Entropie führen als die Vorgaben dieser Ziff. 19.4, so haben diese AUFTRAGNEHMER-internen Vorgaben Vorrang vor dieser Regelung. Der AUFTRAGGEBER ist über den Inhalt der Regelung des AUFTRAGNEHMERS bei Vertragsbeginn in Kenntnis zu setzen. Gleichermaßen ist AUFTRAGGEBER berechtigt, Sicherheitsvorgaben dieser Ziff. 19.4 nach freiem Ermessen anpassen zu lassen.

Bezug: EN ISO/IEC 27001:2022 A.8.5

19.5 Bildschirmsperre, automatische Abmeldung, Verzögerung bei Falscheingabe

Der AUFTRAGNEHMER stellt sicher, dass nach einer durch den AUFTRAGGEBER definierten Zeitspanne die Bildschirmsperre aktiviert wird bzw. bei Verlassen des Arbeitsplatzes durch den Nutzer zu aktivieren ist und ein Passwort zur Freischaltung des Zugriffs eingegeben werden muss.

Durch den AUFTRAGNEHMER ist sicherzustellen, dass eine zeitgesteuerte Zwangstrennung bei Untätigkeit des Benutzers sowie eine geeignete Information (z.B. Hinweisfenster) bei vollzogener automatischer Trennung und Abmeldung umgesetzt wird.

Nach erfolglosen Authentifizierungsversuchen sollten die Systeme jeden weiteren Anmeldeversuch zunehmend verzögern (Time-delay). Mindestens jedoch sind die betreffenden Accounts nach Erreichen eines durch den AUFTRAGGEBER definierten Schwellenwerts an erfolglosen Anmeldeversuchen temporär zu sperren und gesonderte Prozesse für eine vorzeitige Entsperrung vorzusehen.

Diese Unterziffer findet für Cloudleistungen Dritter im Rahmen der technischen Möglichkeiten ebenso Anwendung.

Bezug: EN ISO/IEC 27001:2022 A.8.1, A.7.7

19.6 Administration der Authentifizierungsdaten

Es müssen durch den AUFTRAGNEHMER Sicherheitsfunktionen bereitgestellt werden, um Authentifizierungsdaten für Benutzer anlegen und verändern zu können. Diese Funktionen dürfen nur von autorisierten Administratoren oder im Falle der Änderung von den betroffenen Benutzern selbst ausgeführt werden können.

Bezug: EN ISO/IEC 27001:2022 A.5.17

19.7 Protokollierung und Prüfung

Der AUFTRAGNEHMER stellt sicher, dass in Bezug auf die Authentifizierung mindestens folgende Ereignisse protokolliert werden:

– Ein- und Ausschalten der Protokollierung
– Jeder Versuch, auf Mechanismen zum Management von Authentifizierungsinformationen zuzugreifen.
– Erfolgreiche Versuche, auf Authentifizierungsinformationen zuzugreifen.
– Jeder Versuch, unautorisiert auf Benutzer-Authentifizierungsinformationen zuzugreifen.
– Jeder Versuch, auf Funktionen zur Administration von Benutzer-Einträgen zuzugreifen.
– Änderungen an Benutzereinträgen.
– Jede Benutzung von Authentifizierungsmechanismen.

Die Protokolle sind in regelmäßigen Abständen, mindestens jedoch wöchentlich, durch den AUFTRAGNEHMER auf Auffälligkeiten und Abweichungen zu prüfen.

Die Protokollierung ist so weit wie technisch möglich zentralisiert durchzuführen.

Bezug: EN ISO/IEC 27001:2022 A.5.18

19.8 Hinterlegung von Authentifizierungsinformationen

Der AUFTRAGNEHMER verpflichtet sich im Sinne der Übernahme einer Hauptleistungspflicht unter dem Vertrag, nach Aufforderung durch den AUFTRAGGEBER sämtliche Authentifizierungsinformationen, die für den unbeschränkten administrativen Zugang zu den von dem AUFTRAGNEHMER für den AUFTRAGGEBER unter dem Vertrag betriebenen Systemen erforderlich sind, nach Maßgabe des AUFTRAGGEBERS auf einem geeigneten, vorher vereinbarten und sicheren Weg zu übergeben. Dieser Datenträger bzw. Umschlag wird bei dem AUFTRAGGEBER in einem Safe verwahrt. Der AUFTRAGNEHMER hat eine entsprechende Passwortdatenbank für diesen Fall stets vorzuhalten. Des Weiteren verpflichtet sich der AUFTRAGNEHMER, diese Passwörter und anderen Authentifizierungsinformationen regelmäßig und unverzüglich entsprechend den vom AUFTRAGNEHMER durchgeführten turnusmäßigen Änderungen in den Systemen zu aktualisieren, um den AUFTRAGGEBER in die Lage zu versetzen, selbst und / oder mit der Unterstützung Dritter den Betrieb der Systeme aufrecht zu erhalten und / oder wiederherstellen zu können. Eine derartige Handlungsmöglichkeit für den AUFTRAGGEBER ist in den folgenden Fällen gegeben:

(1) Ein Notfall ist eingetreten bzw. wird mit an Sicherheit grenzender Wahrscheinlichkeit eintreten oder

(2) eine für das jeweilige System / die jeweilige Leistung festgelegte Ausfallzeit ist abgelaufen, ohne dass der AUFTRAGNEHMER dieses / diese zur vertragsgemäßen Nutzung durch den jeweiligen Kunden wiederherstellen konnte, es sei denn, dass durch den AUFTRAGNEHMER dem AUFTRAGGEBER vor Ablauf der Ausfallzeit bereits mitgeteilt wurde, dass der AUFTRAGNEHMER den Betrieb nicht mehr aufrechterhalten kann. In diesem Fall liegt ein Notfall bereits mit Zugang der dahingehenden Mitteilung an den AUFTRAGGEBER vor. Dies gilt nicht, wenn der AUFTRAGNEHMER dem AUFTRAGGEBER gleichzeitig über die bislang getroffenen Maßnahmen und den voraussichtlich über die Ausfallzeit hinausgehenden Zeitraum zur Wiederherstellung informiert und der

AUFTRAGGEBER diesen zusätzlichen Zeitraum ausdrücklich akzeptiert oder

(3) allen sonstigen Fällen, in denen der AUFTRAGNEHMER dem AUFTRAGGEBER von sich aus mitteilt, dass der AUFTRAGNEHMER den Betrieb des jeweiligen Systems / der jeweiligen Leistung nicht mehr aufrechterhalten kann oder auch die Gefahr besteht, dass dieser Fall eintritt oder

(4) sämtliche für die vertragsgemäße Erbringung der beauftragten Leistungen wichtigen Betriebsstätten des AUFTRAGNEHMER oder ein definierter Personenkreis des AUFTRAGNEHMER für einen Zeitraum von 48 (achtundvierzig) Stunden nicht erreichbar sind.

Der AUFTRAGNEHMER ist verpflichtet, die vorgenannten Mitteilungen an den AUFTRAGGEBER unverzüglich vorzunehmen, um jeglichen Ausfall der betroffenen Systeme zu verhindern bzw. dem AUFTRAGGEBER die Möglichkeit zu geben, für einen solchen Ausfall Vorkehrungen zur Schadenabwehr zu treffen. Derartige Mitteilungen sind auch vor dem Ablauf der Ausfallzeit zu machen, wenn für den AUFTRAGNEHMER erkennbar ist, dass er den vertragsgemäßen Betrieb nicht aufrechterhalten kann. Bei schuldhafter Verletzung dieser Mitteilungspflicht ist der AUFTRAGNEHMER verpflichtet, dem AUFTRAGGEBER die hieraus resultierenden Schäden zu ersetzen. Die gesetzliche Beweislast bleibt unberührt. Diese Mitteilungen müssen schriftlich per E-Mail oder Fax, und zusätzlich während der Geschäftszeiten dem AUFTRAGGEBER fernmündlich, an die definierten Ansprechpartner des AUFTRAGGEBERS erfolgen.

Die Festlegung der Passwörter und anderer Authentifizierungsinformationen im Sinne dieser Ziffer 19.8 werden die Vertragsparteien unverzüglich, spätestens innerhalb von 30 (dreißig) Kalendertagen nach Unterzeichnung dieses Dokumentes vornehmen. Dabei wird der AUFTRAGNEHMER insbesondere folgende Informationen bereitstellen:

– Bestimmung aller relevanten Passwörter und anderen Authentifizierungsinformationen
– Bestimmung der Hinterlegungsstelle, insbesondere unter Einschluss der Kommunikationsdaten, Ansprechpartner und Erreichbarkeiten
– Bestimmung der entsprechenden Personenkreise bei dem AUFTRAGNEHMER und dem AUFTRAGGEBER, inklusive entsprechender Vertreterregelungen
– Bestimmung der maximalen Ausfallzeiten, soweit diese nicht im bereits anderweitig im Vertrag zwischen AUFTRAGGEBER und AUFTRAGNEHMER geregelt sind
– Bestimmung des Personenkreises des AUFTRAGNEHMERS, welcher für den AUFTRAGGEBER durchgehend erreichbar sein muss
– Aussagen über den zulässigen Umfang der Nutzung der Passwörter und anderen Authentifizierungsinformationen, wobei hier der Bedeutung des ausgefallenen Systems / der Leistung für die Fortführung des Geschäftsbetriebes des AUFTRAGGEBERS bzw. von dessen Kunden vollumfänglich Rechnung getragen werden muss
– Aussagen über den Verantwortungsübergang für sämtliche betroffenen Systeme und Leistungen inkl. Service-Level während der Dauer des Notfalls
– Aussagen über den Rückübergang des Betriebs an den AUFTRAGNEHMER nach Wegfall / Behebung der Voraussetzungen für das Eintreten des Notfalls.

Diese Unterziffer findet für Cloudleistungen mit der Maßgabe Anwendung, dass der AUFTRAGNEHMER dem AUFTRAGGEBER seine Authentifizierungsinformationen für die Cloudleistungen und die darin enthaltenen Konfigurationsmöglichkeiten und Werkzeuge bereitstellt. Der Cloudanbieter kann jedoch seinen standardisierten internen Verfahren gemäß ISO/IEC 27001 folgen, insofern diese den vereinbarten Mindeststandard einhalten. Es besteht ausdrücklich kein Zugriff auf die Verwaltungs-Systeme des Cloudanbieters über den dem AUFTRAGGEBER und/oder dessen jeweilgen Kunden zugeordneten Tenant / Mandanten hinaus.

Bezug: EN ISO/IEC 27001:2022 A.5.29

20 FERNZUGÄNGE

Der AUFTRAGNEHMER stellt sicher, dass bei Fernzugängen (Zugang in das Netz des AUFTRAGGEBERS bzw. des AUFTRAGNEHMERS) die Vertraulichkeit, Verfügbarkeit, Integrität und

Authentizität der Assets und Services des AUFTRAGGEBERS sowie von dessen Kunden gewährleistet sind. Diese Verpflichtung erstreckt sich auch auf die nachträgliche Verwendung von Informationen, von denen der AUFTRAGNEHMER während eines Fernzugriffes Kenntnis erlangt hat. Der AUFTRAGNEHMER ist für alle Aktionen im Zusammenhang mit der Administration der Benutzerkonten mit Fernzugangsfunktion auf Systemen des jeweiligen Kunden verantwortlich, die durch den AUFTRAGNEHMER bereitgestellt werden. Ist der Zugriff auf Systeme von außen erforderlich, ist dieser durch starke Multi-Faktor-Authentisierungsmechanismen durch den AUFTRAGNEHMER zu schützen und die Nutzung dieser Zugänge zu protokollieren.

In Bezug auf Accounts für Fernzugänge finden die Regelungen der Ziff. 18 und 19 Anwendung.

Bezug: EN ISO/IEC 27001:2022 A.5.15, A.8.26

21 NUTZUNG VON MOBILEN ENDGERÄTEN

21.1 Mobile Endgeräte (z. B. Mobiltelefone, Smartphones, Tablets), von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen (z. B. IT-Systeme oder Informationen) des jeweiligen Kunden möglich ist, müssen angemessen geschützt werden, insbesondere durch Verschlüsselung der Geräte und etwaiger Datenverbindungen, ein Schutzkonzept gegen unberechtigten Zugriff, technische und organisatorische Maßnahmen zur Verhinderung der Außerkraftsetzung von Schutzmaßnahmen (z. B. Jailbreaking / Rooting, Installation aus Fremd-App Stores) sowie ein Verbot für den Einsatz von eigenen Endgeräten der von dem AUFTRAGNEHMER eingesetzten Personen (außerhalb durch den AUFTRAGGEBER genehmigter BYOD-Vereinbarungen), ist anzuwenden.

21.2 Der AUFTRAGNEHMER stellt sicher, dass keine administrativen Tätigkeiten über mobile Endgeräte durchgeführt werden können, bei denen keine gleichwertige Sicherheit eines stationären Endgerätes sichergestellt werden kann.

Bezug: EN ISO/IEC 27001:2022 A.8.1

22 NUTZUNG VON CLOUD-DIENSTEN ZUR ADMINISTRATION ODER INFORMATIONSVERARBEITUNG

Der AUFTRAGNEHMER stellt sicher, dass der Einsatz von über den AUFTRAGNEHMER bezogenen Public Cloud Computing-Diensten nach den Vorgaben des Vertrages und in Übereinstimmung der diesbzgl. Vorgaben des AUFTRAGGEBERS erfolgt, sollten diese über die Vereinbarung des Vertrages hinausgehen. Sofern dass nicht erreicht werden kann, wird der AUFTRAGNEHMER auf Abweichungen hinweisen.

22.1 Weiterhin stellt der AUFTRAGNEHMER sicher, dass

1. die Administration der vertragsgegenständlichen Cloudsysteme, Anwendungen und Services im Einklang mit den Regelungen dieses Vertrages erfolgt und
2. mittels Cloud Computing-Diensten keine vertraulichen Informationen oder sensible Informationen des AUFTRAGGEBERS (bspw. Authentisierungsinformationen) sicher verarbeitet und sicher gespeichert werden.

Ausnahmen hiervon kann der AUFTRAGGEBER im Einzelfall genehmigen und diese sind in einem Ausnahmeregister zu dokumentieren.

Bezug: EN ISO/IEC 27001:2022 A.5.14, A.5.8, A.8.31, A.5.20, A.5.21

23 DATENSICHERUNG UND -WIEDERHERSTELLUNG, DATENTRANSPORT

23.1 Die bei dem AUFTRAGNEHMER gespeicherten Daten verbleiben für die Dauer der Speicherung in dessen Verwaltung.

23.2 Der AUFTRAGNEHMER ist über die Vorgaben des Vertrages hinaus verpflichtet, alle Daten und Informationen des jeweiligen Kunden insoweit zu sichern, dass der Betrieb von Systemen und

Technologien sowie die Maßnahmen der Informationssicherheit bei Verlust oder Beschädigung von Teilen des operativen Datenbestandes entsprechend den technischen Möglichkeiten schnellstmöglich wieder aufgenommen werden kann. Es sind durch den AUFTRAGNEHMER Maßnahmen zu ergreifen, welche auch die Möglichkeit unbrauchbarer Sicherungen berücksichtigen und die daraus entstehenden Risiken verringern (z. B. physische Auslagerung von Sicherungsbeständen, regelmäßige Prüfung der Les- und Nutzbarkeit).

Der AUFTRAGNEHMER etabliert Datensicherungs- und Wiederherstellungsprozesse und führt gemäß den Regelungen des Vertrages regelmäßig wirksame technische Datenwiederherstellungstests durch. In Abstimmung und unter Mitwirkung des AUFTRAGGEBERS können auch fachliche Wiederherstellungstests erfolgen.

23.3 Sofern Daten außerhalb der Netze des AUFTRAGNEHMERS und / oder des jeweiligen Kunden transportiert werden müssen, sind diese durch den AUFTRAGNEHMER zuvor zu verschlüsseln sowie – im Falle des physischen Transports von Datenträgern – zusätzlich mit entsprechenden physischen Schutzmaßnahmen abzusichern.

23.4 Backup-Medien und -Datenträger sind sicher aufzubewahren und vor unbefugtem Zugriff und Veränderung oder Verlust zu schützen.

Bezug: EN ISO/IEC 27001:2022 A.8.13, A.5.29, A.8.14

24 SICHERHEITSBEREICHE, SCHUTZZONEN

Entsprechend der mit dem AUFTRAGGEBER abgestimmten bzw. sich aus dem Schutzbedarf ergebenden Sicherheitsanforderungen werden durch den AUFTRAGNEHMER unterschiedliche physische Sicherheitsbereiche / Schutzzonen innerhalb der IT-Infrastruktur und der Systeme realisiert. Hieran werden folgende Anforderungen gestellt:

– Alle Systeme und Nutzer müssen die geltenden Richtlinien der jeweils benutzten Sicherheitsbereiche und Schutzzone beachten und umsetzen.
– Die Abschottung der Sicherheitsbereiche / Schutzzonen untereinander erfolgt durch angemessene Maßnahmen. Dies schließt die Maßnahmen des Brand- und Katastrophenfall-Schutzes mit ein.
– Für die einzelnen Sicherheitsbereiche / Schutzzonen werden die jeweils notwendigen Maßnahmen zur Zutrittskontrolle zu Räumlichkeiten, Zugangskontrolle zu den Systemen und Zugriffskontrolle auf Informationen ergriffen.

Diese Unterziffer findet ebenso für Cloudleistungen Dritter Anwendung, wobei dies auf Basis der jeweils technischen Möglichkeiten des Cloudanbieters basiert (bspw. Sicherheitszonen) und dabei die Anforderungen der ISO 27001 berücksichtigt.

Bezug: EN ISO/IEC 27001:2022 A.7.4, A.7.8

25 MANDANTENFÄHIGKEIT GETEILTER INFRASTRUKTUREN

Ist es erforderlich, Systeme in einer geteilten Infrastruktur zu betreiben, sind diese durch den AUFTRAGNEHMER mandantenfähig zu gestalten. Als mandantenfähig werden IT-Systeme bezeichnet, welche auf derselben Infrastruktur, demselben Server oder Softwaresystem mehrere Kunden bedienen können. Werden mit einem IT-System auch andere Kunden als der den jeweiligen Kunden bedient, so garantiert der AUFTRAGNEHMER, dass keinerlei Zugriff auf die Daten, die Benutzerverwaltung und / oder ähnliche Bereiche des jeweiligen Kunden durch andere Kunden des AUFTRAGNEHMERS möglich ist. Im Fall eines messbaren oder absehbaren direkten oder indirekten Nachteils für den AUFTRAGGEBER, ist auf eine gemeinsame Nutzung durch den AUFTRAGNEHMER oder andere Kunden des AUFTRAGNEHMER zu verzichten und die Systeme, Anwendungen und Services dediziert für den jeweiligen Kunden zu betreiben.

Bezug: EN ISO/IEC 27001:2022 A.5.15, A.8.3

26 NETZWERKE, NETZWERKSEGMENTIERUNG, FIREWALLS

26.1 Die internen Netze des AUFTRAGNEHMERS dürfen nicht mit den Netzen des jeweiligen Kunden gekoppelt sein. Ist ausnahmsweise eine Kopplung für die Aufgabenerfüllung im Einzelfall notwendig, hat der AUFTRAGGEBER dem vorab schriftlich zuzustimmen und dies ist zu dokumentieren. Der Netzwerkverkehr zwischen gekoppelten Netzen ist prinzipiell durch ein Sicherheitsgateway (z.B. Firewall) zu kontrollieren und gemäß den Vereinbarungen mit dem AUFTRAGGEBER einzuschränken.

26.2 Direkte Zugriffe aus dem Internet in das interne Netz des jeweiligen Kunden sind nicht zulässig und müssen durch eine Firewall unterbunden werden. Sofern Remote-Access in das interne Netz möglich ist oder Dienste (z. B. Webserver, Mailserver, etc.) vom Internet aus erreichbar sind, darf dies nur mit einer angemessenen Sicherung erfolgen, die dem aktuellen Stand der Technik entspricht.

26.3 Der AUFTRAGNEHMER verpflichtet sich auf Basis eines mit dem AUFTRAGGEBER abgestimmten Konzeptes, Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen voneinander getrennt zu betreiben, mindestens hinsichtlich Administrationsnetzwerken (Out-of-Band Management), DMZ, Abschottung von Systemen mit sensiblen Informationen und funktionsfremdem Nutzen. Die Netzwerkperimeter sind durch den AUFTRAGNEHMER mit Hilfe von Firewalls abzusichern, deren Firewall-Regeln einen dokumentierten Freigabeprozess durchlaufen und auf das notwendige Minimum beschränkt werden.

26.4 Durch den AUFTRAGNEHMER ist ein aktives Firewall-Management auf Basis einer Policy vorzunehmen, welche das Verhalten in Bezug auf Informationen, Dienste und Protokolle definiert und nachvollziehbar dokumentiert, insbesondere hinsichtlich einer automatischen Regelverwaltung mit Vorgaben zum Ablauf und der Erneuerung von Regeln sowie den zu ergreifenden Gegenmaßnahmen bei erkannten Angriffen und entsprechende Alarmierungsmaßnahmen. Der AUFTRAGNEHMER definiert in Zusammenarbeit mit dem AUFTRAGGEBER Anforderungen, welche aktiven Inhalte als schädlich einzustufen und zu filtern sind. Die Aktivitäten in Sicherheitsgateways sind durch den AUFTRAGNEHMER durchgängig zu protokollieren und regelmäßig (mind. monatlich) zu analysieren.

26.5 Anbindungen an fremde IT-Infrastrukturen sind durch den AUFTRAGNEHMER mindestens durch Firewall-Technik und Intrusion-Detection-Maßnahmen abzusichern. Dies gilt insbesondere für Verbindungen mit dem bzw. über das Internet.

26.6 Alle an Netzwerke angeschlossene Endgeräte sind in Bezug auf die Zulässigkeit des Anschlusses zu überwachen und zum Zeitpunkt des Anschlusses bzw. der Authentifizierung auf Richtlinienkonformität zu prüfen und entsprechenden Maßnahmen zu ergreifen. Sollten nicht-zugelassene bzw. nicht-konforme Endgeräte angeschlossen werden, so ist dies über einen Security Incident zu melden.

Wenn durch den AUFTRAGNEHMER bereitgestellte drahtlose Netzwerke mit Verbindung zu internen Netzen des jeweiligen Kunden benutzt werden, sind diese durch den AUFTRAGNEHMER kryptographisch abzusichern und die Authentifizierung der Endgeräte auf Basis zertifikatsbasierter Verfahren durchzuführen. In diesem Zusammenhang trägt der AUFTRAGNEHMER dafür Sorge, dass Systeme sich nicht automatisch mit fremden Access-Points verbinden bzw. dass keine unautorisierten Netzwerke aufgebaut werden.

Bezug: EN ISO/IEC 27001:2022 A.5.15, A.8.5, A.5.14, A.8.20

27 PROTOKOLLIERUNG

27.1 Der AUFTRAGNEHMER hat ein Event Management zur Überwachung zu implementieren.

27.2 Netzwerkverbindungen, Systemzugriffe, administrative Tätigkeiten sowie notwendige Ausnahmen, Störungen, Informationssicherheitsereignisse und Informationssicherheitsvorfälle sind zur Nachvollziehbarkeit von Angriffen oder Fehlbedienungen durch den AUFTRAGNEHMER zu protokollieren. Die Protokollierung ist so auszugestalten, dass eine Nachvollziehbarkeit sämtlicher relevanter Aktivitäten durch einen sachkundigen Dritten jederzeit möglich ist. Die Aufbewahrung der Protokolle richtet sich nach den geltenden gesetzlichen, geschäftlichen und AUFTRAGGEBER-seitigen Anforderungen. Sowohl die Protokollierung selbst als auch die Protokolle sind durch den AUFTRAGNEHMER vor Manipulation zu schützen.

27.3 Die in den Protokollen aufgezeichneten Ereignisse sind durch den AUFTRAGNEHMER täglich und mindestens auf unberechtigte Zugriffe bzw. diesbezügliche Versuche, Fehlfunktionen, fehlerhafte Protokollierungen sowie weitere Auffälligkeiten (z. B. Pattern) auszuwerten und das Ergebnis dieser Auswertung bei Auffälligkeiten dem AUFTRAGGEBER unverzüglich nach Abschluss vorzulegen.

27.4 Im Falle eines ungewöhnlichen Datenabflusses oder sonstigen Sicherheitsverstoßes informiert der AUFTRAGNEHMER den AUFTRAGGEBER im Rahmen des Informationssicherheitsvorfalls unverzüglich über die Art und Details des Verstoßes (z. B. Menge der Daten und die zu Grunde liegenden Ausgangs- und Ziel-IP-Adressen) und legt die betroffenen Userkennungen gegenüber dem AUFTRAGGEBER im Rahmen einer kurzfristigen Konferenz im Beisein von Vertreter(n) des Betriebsrates des jeweiligen Kunden, der Compliance- und Personalabteilung des jeweiligen Kunden sowie des genannten Ansprechpartners des jeweiligen Kunden zur Verarbeitung personenbezogener Daten (Datenschutzbeauftragter) offen.

Bezug: EN ISO/IEC 27001:2022 A.8.15, A.5.34

28 ENTWICKLUNGSPROZESSE

Sofern der AUFTRAGNEHMER die Entwicklung von Programmen, Programmcodes, Software, Applikationen und / oder Systeme individuell für den AUFTRAGGEBER durchführt, verpflichtet sich der AUFTRAGNEHMER im Rahmen der Entwicklungsprozesse, die folgenden Vorgaben des AUFTRAGGEBERS einzuhalten:

– Vorhandene Standards in Bezug auf die sicherere Entwicklung werden eingehalten.
– Produktiv-, Test- und Entwicklungsumgebungen sind grundsätzlich zu trennen.
– Die vom AUFTRAGNEHMER eingesetzten Personen halten interne Standards des AUFTRAGNEHMERS ein. Diese Standards sind dokumentiert und den von dem AUFTRAGNEHMER eingesetzten Personen in Schulungen bekannt gemacht.
– Der Zugang zu und Zugriff auf Quellcodes unterliegt den Regelungen der Ziff. 19.
– Secure-Code-Reviews werden im Rahmen der Qualitätssicherung und des Testings nach Industriestandards (z.B. OWASP 10) durchlaufen. Die Ergebnisse werden dem AUFTRAGGEBER zur Verfügung gestellt.
– Im Fall der Benutzung von Open-Source-Komponenten ist auf eine angemessene Konfiguration, Dokumentation und Wartung dieser Komponenten zu achten.
– Die Testverfahren beinhalten explizit die jeweilig implementierten Sicherheitsmechanismen und -funktionen (z. B. Verschlüsselung, Zugriffskontrollen, Authentisierung und andere). Der AUFTRAGNEHMER stellt zu jeder Lieferung und zu jedem Update dem AUFTRAGGEBER die notwendige Menge von funktionalen Testfällen und -skripten zur Verfügung, die zum diesbezüglichen Funktionsnachweis benötigt werden. Testdaten sind zu schützen, Produktivdaten dürfen nur in bestätigten Ausnahmefällen zum Testen herangezogen werden. Personenbezogene Daten sind in jedem Fall vor Nutzung zu anonymisieren.
– Prüfungen der Sicherheit entsprechend den vorgesehenen Betriebsumgebungen, z. B. unabhängige Penetrationstests, werden nach Maßgabe des AUFTRAGGEBERS durchgeführt. Die Ergebnisse werden dem AUFTRAGGEBER zur Verfügung gestellt.

– Sofern technisch möglich, sind die Entwicklungen vor der Auslieferung an den AUFTRAGGEBER so zu konfigurieren, dass sicherheitsrelevante Operationen nur von dazu besonders berechtigten Personen (Administratoren) durchgeführt werden können. Die Konfiguration ist darüber hinaus durch den AUFTRAGNEHMER so zu wählen, dass sicherheitskritische Funktionen so weit wie technisch möglich deaktiviert sind („security by default“). Eventuell vor der Auslieferung eingerichtete Kennwörter sind bei der Auslieferung von dem für das System Verantwortlichen des jeweiligen Kunden) zu ändern. Der AUFTRAGNEHMER hat hierauf vor der Inbetriebnahme deutlich hinzuweisen.
– Die Entwicklung ist in angemessenem Umfang dokumentiert, mindestens hat der AUFTRAGNEHMER alle für die Entwicklung und den späteren Betrieb relevanten Informationen, insbesondere das Sicherheitskonzept sowie den angemessen kommentierten Quellcode, zu dokumentieren. Für die Dokumentationen gelten die Vorgaben des Vertrages.

Die gleichen Anforderungen gelten für ausgelagerte Entwicklungen; diese sind durch den AUFTRAGNEHMER zu überwachen und zu steuern.

Diese Unterziffer findet, insofern zutreffend, ebenso für Cloudleistungen Dritter Anwendung und erfolgt auf standardisierten Verfahren gemäß der ISO/IEC 27001.

Bezug: EN ISO/IEC 27001:2022 A.8.18, A.8.31, A.8.25, A.8.32, A.8.27, A.8.30, A.8.29, A.8.33

29 KRYPTOGRAPHIE

29.1 Der AUFTRAGNEHMER stellt sicher, dass die eingesetzten kryptographischen Systeme und Schlüsselmaterialien, interne Zertifikate und PKIs angemessen geschützt, nicht veraltet oder als unsicher bekannt sind und dass der Lebenszyklus von diesen kryptographischen Systemen und Schlüsselmaterialien geplant und gesteuert wird. Weiterhin stellt der AUFTRAGNEHMER sicher, dass die kryptografischen Systeme und Schlüsselmaterialien den Empfehlungen des BSI (insbesondere BSI TR-02102/1-4 und entsprechende Nachfolgerrichtlinien) entsprechen.

29.2 Die Datenkommunikation mit externen Dritten, sowie die Übermittlung von Authentisierungsinformationen hat nach Maßgabe des AUFTRAGGEBERS verschlüsselt zu erfolgen.

Bezug: EN ISO/IEC 27001:2022 A.8.24, A.5.31

30 UHRENSYNCHRONISATION

Die Uhren aller relevanten informationsverarbeitenden Systeme des AUFTRAGNEHMERS werden mit einer einzigen Referenzzeitquelle synchronisiert. Dabei ist das Network Time Protocol (NTP) nur innerhalb des eigenen Netzwerkes einzusetzen. Falls für die Zeitsynchronisation auf externe Quellen zurückgegriffen wird, muss sichergestellt werden, dass die empfangenen Zeit-Informationen nicht ungeprüft übernommen werden. Die Software des lokalen Zeit-Servers beziehungsweise NTP-Proxys muss eine Plausibilitätsprüfung vornehmen, bevor sie die empfangenen Zeit-Informationen übernimmt.

Bezug: EN ISO/IEC 27001:2022 A.8.17

31 NOTFALLKONZEPTE, -VORSORGE UND -MAßNAHMEN

Diese Ziffer findet für Cloudleistungen Dritter ebenso und im Rahmen der jeweiligen Umsetzbarkeit und SLA Vereinbarungen Anwendung. Der Cloudanbieter folgt dabei dem standardisierten internen Verfahren gemäß ISO/IEC 27001 und auf Basis geschlossener Servicevereinbarungen.

31.1 Grundsätze

31.1.1 Zur Begrenzung größerer Schäden infolge von Notfällen bzw. zur Vorbeugung gegen solche Schäden muss seitens des AUFTRAGNEHMERS entsprechend zügig und konsequent reagiert werden. Für die Systeme und Technologien sind durch

den AUFTRAGNEHMER diesbezüglich Notfallkonzepte und -Maßnahmen zur Fortführung und Wiederherstellung des Betriebes sowie zu Prozessen im Umgang mit Notfällen und der Notfallkommunikation zu erarbeiten und umzusetzen. Die entsprechenden Notfallmaßnahmen sind mindestens einmal je Kalenderjahr oder in Verbindung mit Neuvorhaben oder wesentlichen Veränderungen durch den AUFTRAGNEHMER zu üben. Bei Bedarf ist hierbei der AUFTRAGGEBER in die Übung einzubinden, insbesondere für organisatorische Übergabepunkte.

31.1.2 Der AUFTRAGNEHMER legt die Notfallkonzepte unverzüglich nach jeder Veränderung dem AUFTRAGGEBER zur Prüfung vor, sofern der jeweilige Kunde davon betroffen ist. Der AUFTRAGNEHMER informiert den AUFTRAGGEBER unverzüglich über die Erkenntnisse der Übungen in Bezug auf das Notfallkonzept.

31.1.3 Der AUFTRAGNEHMER stellt in Bezug auf seine Business Continuity / Geschäftsfortführung der vertragsgegenständlichen Leistungen weiterhin die Einhaltung relevanter Normen, in der jeweils gültigen Fassung, sowie die Einhaltung der entsprechenden Vorgaben des AUFTRAGGEBERS sicher.

31.1.4 Dem AUFTRAGNEHMER steht es frei, sich für nicht aus eigener Kraft bewältigbare Notfälle Dienstleistungen Dritter zu bedienen, welche bei der Schadenbegrenzung, dem Notbetrieb und ggf. dem Wiederanlauf unterstützen. Der AUFTRAGGEBER ist über eine diesbzgl. Vereinbarung zu informieren.

Bezug: EN ISO/IEC 27001:2022 A.5.29

31.2 Kennzeichnung von Komponenten

Diese Ziffer findet für Cloudleistungen Dritter keine Anwendung. Der Cloudanbieter folgt dem standardisierten Verfahren gemäß ISO/IEC 27001 und auf Basis geschlossener Servicevereinbarungen, so dass Services für den AUFTRAGGEBER eindeutig identifiziert werden können.

31.2.1 Alle für den Betrieb von Systemen und Technologie eingesetzten (Infrastruktur-) Komponenten einschließlich der durch den AUFTRAGGEBER beigestellten Komponenten sind wie folgt durch den AUFTRAGNEHMER zu kennzeichnen, um ein Auffinden durch einen unabhängigen Dritten zu gewährleisten:

– Auflistung aller Komponenten in einer Asset-Management-Datenbank mit abzustimmenden Attributen. Diese sollten nach Möglichkeit folgende Informationen tragen:
- Inventarnummer
- Komponententyp
- Modellnummer
- Seriennummer
- Standort von Komponenten außerhalb eines Rechenzentrums (Adresse, Gebäude, Stockwerk, Zimmer, Benutzer)
- Standort von Komponenten innerhalb eines Rechenzentrums (Adresse, Gebäude, Stockwerk, Koordinate im Rechenzentrum, Rack-Nummer, Position im Rack, verantwortlicher Administrativer Kontakt)
- Schutzbedarfskategorie nach Vorgabe des AUFTRAGGEBERS (Kritisches System iSd ITSiG 2.0)
- Anschaffungsdatum
- End Of Life Datum, sofern zutreffend
- Hersteller
- Owner

31.2.2 Eine Kennzeichnung der Komponenten außerhalb von Betriebsstätten des jeweiligen Kunden darf nicht die Firma des jeweiligen Kunden oder einen sonstigen Hinweis auf den jeweiligen Kunden enthalten. Die Kennzeichnung erfolgt pseudonymisiert, eine Zuordnung über die Inventarnummer in den Geschäftsunterlagen des AUFTRAGNEHMERS muss aber eindeutig und unzweifelhaft hergestellt werden können.

31.2.3 Diese Kennzeichnungspflicht umfasst alle Komponenten, die für die Erbringung der Leistungen des AUFTRAGNEHMERS erforderlich sind und gegebenenfalls nicht exklusiv dem AUFTRAGGEBER dienen (z. B. Monitoring-Systeme, Rechenzentrums-Infrastruktur) sowie auch Bereitstellungen und Beistellungen durch den AUFTRAGNEHMER.

32 VERHINDERUNG DER INFORMATIONSGEWINNUNG DURCH DRITTE

Der AUFTRAGNEHMER hat eigene Vorgaben zu definieren und Maßnahmen durchzuführen, um eine Gewinnung von Informationen durch Dritte, insbesondere zur Vorbereitung möglicher sog. „Social Engineering"-Angriffe oder für Konkurrenzanalysen durch Mitbewerber des jeweiligen Kunden, so weit wie möglich zu verhindern bzw. zu beeinträchtigen. Hierzu sind insbesondere

– die von dem AUFTRAGNEHMER eingesetzten Personen daraufhin zu belehren, Informationen per E-Mail, Chat, Telefon oder andere Kommunikationskanäle nicht an unbekannte Personen weiterzugeben und ein entsprechender Regelprozess zur Erkennung und Behandlung solcher Vorkommnisse zu etablieren,
– eine Richtlinie zum Umgang mit Informationen für die von dem AUFTRAGNEHMER eingesetzten Personen aufzustellen, insbesondere zum Verhalten in der Öffentlichkeit (z. B. Nutzung von sog. „Privacy-Filtern" für Notebooks, keine Nennung des jeweiligen Kunden oder von Namen von Nutzern des jeweiligen Kunden, ständige Beaufsichtigung aller Informationen und Informationsträger),
– Informationen, welche durch einen Dritten auf öffentlichem Wege erlangt werden können, insbesondere Informationen auf öffentlich erreichbaren Internetseiten, automatisierte Abwesenheitsmitteilungen per E-Mail oder Anrufbeantworter, auf das notwendige Mindestmaß zu beschränken (z. B. keine Abwesenheitsdauern oder Benennung von Vertreterregelungen in öffentlichen Abwesenheitsmitteilungen, keine Organigramme auf der Homepage des AUFTRAGNEHMERS) sowie
– weitere Maßnahmen zur Erkennung von Versuchen der Informationsgewinnung durch Dritte zu ergreifen, insbesondere Awareness-Schulungen, Maßnahmen zur Erkennung von und Schutz vor Innentätern, Vorgaben für den Umgang mit externen Personen an den Standorten des AUFTRAGNEHMERS, Auswertung der Vorgehensweise erfolgter Angriffe.

Grundsätzlich sind alle Informationen zu schützen, welche vertrauliche Informationen sind, sowie alle weiteren Informationen, welche dazu geeignet sind, Rückschlüsse auf Informationen des jeweiligen Kunden zu erlangen, insbesondere

– Hinweise auf oder Darstellungen von Aufbau- und Ablauf-Organisationsstrukturen,
– Unternehmenskultur,
– Kommunikationsschemata,
– Sprachbesonderheiten (z. B. bestimmte Begriffe oder intern genutzte Abkürzungen),
– persönliche Eigenschaften von Nutzern und
– nicht der Öffentlichkeit bekannte Ereignisse / Termine (z. B. Urlaubszeiträume)

.

Dies gilt auch für Informationen, die für sich genommen nicht die vorgenannten Kriterien erfüllen, jedoch in Korrelation zu einer ungewollten Offenlegung der vorgenannten Informationen führen können.

Bezug: EN ISO/IEC 27001:2022 A.6.3, A. 5.10, A.7.7, A.8.1, A.5.14, A.6.6

33 SCHWACHSTELLENMANAGEMENT

Diese Ziffer findet für Cloudleistungen insoweit Anwendung, dass der Cloud-Anbieter den Verfahren gemäß ISO/IEC 27001 folgt.

33.1 Umfang

Die Verantwortung für die Steuerung von technischen Informationssicherheitsschwachstellen der durch ihn betriebenen Systeme und Technologien liegt bei dem AUFTRAGNEHMER. Diese hat in geeigneter Weise kontinuierlich

– Informationen zu Informationssicherheitsschwachstellen zu sammeln und zu beschaffen (mindestens der Hersteller und des CERT-Bund),
– Informationssicherheitsschwachstellen und Sicherheitsempfehlungen für die bereitgestellten und betriebenen Technologien zu identifizieren, insbesondere in Form regelmäßiger (mind monatlicher) Schwachstellenscans und jährlicher Penetrationstests der gesamten vertragsgegenständlichen Infrastruktur,

– die funktionalen und sicherheitsrelevanten Auswirkungen, Risiken und Kritikalität der Schwachstellen unverzüglich zu beurteilen und zu klassifizieren,
– entsprechende Abhilfe- und Beseitigungsmaßnahmen unverzüglich zu entwickeln und
– entsprechende Abhilfe- und Beseitigungsmaßnahmen unverzüglich zu ergreifen sowie
– Reports und Berichte zur Wirksamkeit des Schwachstellenmanagements zu erstellen und dem AUFTRAGGEBER zu übermitteln.

Im Falle von Unklarheiten oder technischen Herausforderungen erfolgt eine Abstimmung mit dem AUFTRAGGEBER.

Bezug: EN ISO/IEC 27001:2022 A.8.8, A.6.8

33.2 Informations- und Abstimmungspflichten

Erkannte Schwachstellen und Abhilfemaßnahmen sind durch den AUFTRAGNEHMER zu dokumentieren und dem AUFTRAGGEBER zu melden sowie stets vor Implementierung mit dem Ansprechpartner des AUFTRAGGEBERS abzustimmen

Bezug: EN ISO/IEC 27001:2022 A.8.8, A.6.8

33.3 Kritikalität

Für die Bewertung der Kritikalität sind analog die Vorgaben und Kriterien der Ziff. 8.6 anzuwenden.

Ausgehend von der Kritikalität gelten folgende Anforderungen an die Lösung und Neutralisierung der Schwachstelle, beginnend vom Zeitpunkt der Kenntnisnahme durch den AUFTRAGNEHMER

Kritikalität	Beschreibung	Finale Lösungszeit	Zeit zur Neutralisierung
niedrig	Als geringfügig eingestufte Schwachstellen ermöglichen das Sammeln von Informationen (offene Ports, Dienste, Fingerprinting etc.) über das Zielsystem. Diese können als Vorbereitung für weitere Angriffe genutzt werden.	6 Monate	30 Kalendertage
weniger kritisch	Eine derartig klassifizierte Schwachstelle erlaubt das Auslesen von Informationen des Zielsystems. So können durch das Auslesen der auf dem System installierten Software weitere Angriffe auf bekannte Schwachstellen vorbereitet werden.	3 Monate	7 Kalendertage
kritisch	(Potenzielle) Angreifer können durch diese Schwachstelle teilweisen Zugriff auf im System gespeicherte oder verarbeitete Daten, dazu gehören auch die Sicherheitseinstellungen des Systems, erhalten und eine missbräuchliche Nutzung des Zielsystems herbeiführen. Die Vertraulichkeit der auf dem System gespeicherten Daten ist gefährdet. Beispiele hierfür sind: Auslesen einzelner Dateien und Verzeichnisse des Systems, Angriffe auf die Verfügbarkeit, unberechtigte Nutzung von Diensten.	2 Monate	48 Stunden
hochkritisch	Die Schwachstelle ermöglicht (potenziellen) Angreifern das einfache und schnelle Erlangen von unberechtigten und weitreichenden Zugriffen auf das Zielsystem. Hierzu gehören unter anderem Lese- und Schreibzugriffe auf das Dateisystem, die unberechtigte Ausführung von Programmcode sowie das Vorhandensein von Backdoors.	1 Monat	8 Stunden

Bezug: EN ISO/IEC 27001:2022 A.8.8, A.6.8

34 AUDITS

34.1 Der AUFTRAGNEHMER führt mindestens einmal jährlich eigene Informationssicherheitsaudits seiner Organisation, insbesondere seiner Serviceorganisation, seiner Kontrollorganisation, seines ISMS und seiner Sicherheitssysteme durch. Der AUFTRAGNEHMER wird bei den Audits dem AUFTRAGGEBER den Aufbau und Ablauf seiner Kontrollorganisation erläutern. Darüber hinaus wird der AUFTRAGNEHMER die Ergebnisse seiner regelmäßigen Sicherheitsuntersuchungen dem AUFTRAGGEBER unverzüglich zugänglich machen und in Kopie übermitteln. Im Hinblick auf Cloudleistungen Dritter bietet der Cloudanbieter standardisierte Verfahren gemäß ISO/IEC 27001 an und stellt jeweils aktuelle Nachweise in Form eines Zertifizierungsnachweises gemäß ISO/IEC 27001 zur Verfügung.

34.2 Im Interesse einer dauerhaften Schutzwirkung der Sicherheitsmaßnahmen werden diese regelmäßigen Überprüfungen unterzogen. Im Rahmen dieser Überprüfungen werden die jeweils gültigen Mechanismen und Regelungen daraufhin untersucht, ob sie

1. die notwendige und beabsichtigte Schutzwirkung aufweisen
2. in der täglichen Handhabung korrekt angewandt werden
3. allen betroffenen Personen bekannt und in den Betriebsablauf integriert sind und
4. im Einsatz praktikabel sind.

Darüber hinaus werden die jeweils gültigen Mechanismen und Regelungen daraufhin untersucht, ob

1. seit der letzten Prüfung das angestrebte Sicherheitsniveau jederzeit gewährleistet war und
2. der Schutz auch bei eventuellen neuen Bedrohungen und Gefährdungen gewährleistet ist.

35 PENETRATIONSTESTS

Diese Ziffer findet für Cloudleistungen Anwendung. Der Cloudanbieter folgt dem standardisierten Verfahren gemäß ISO/IEC 27001 und stellt auf Anforderung abhängige Auditnachweise zur Verfügung.

35.1 Der AUFTRAGNEHMER stellt sicher, dass mindestens jährliche Penetrationstests der vertragsgegenständlichen Infrastruktur durchgeführt werden. Weiterhin gewährt der AUFTRAGNEHMER dem AUFTRAGGEBER in abgestimmten Zeitfenstern die Durchführung von Penetrationstests durch von dem AUFTRAGGEBER beauftragte Dritte.

35.2 Die Kosten von AUFTRAGGEBER-initiierten Penetrationstests trägt der AUFTRAGGEBER; die Kosten von AUFTRAGNEHMER-seitigen Penetrationstests trägt der AUFTRAGNEHMER.

35.3 Sofern bei einem Penetrationstest hochkritische Schwachstellen oder Sicherheitslücken der Kritikalität „hochkritisch“ entdeckt werden, für die bereits vertragsgegenständliche Regelungen getroffen wurden, gehen die Kosten zur Schließung der Sicherheitslücken zu Lasten des AUFTRAGNEHMERS.

35.4 Sofern, unabhängig von der Art der Ermittlung, ein vertragswidriges Verhalten des AUFTRAGNEHMERS festgestellt wird, ist der AUFTRAGGEBER berechtigt, dem AUFTRAGNEHMER eine angemessene Frist zur Beseitigung des vertragswidrigen Zustandes und Wiederherstellung des vertragsgemäßen Zustandes zu setzen. Sofern Umstände bekannt werden, für welche eine vertragliche Regelung bisher nicht getroffen wurde, werden die Vertragsparteien einvernehmlich festlegen, welche Konsequenzen und Maßnahmen aus den Audits in welcher Priorität bei dem AUFTRAGNEHMER implementiert werden.

35.5 Audits und Penetrationstests sind so zu planen und durchzuführen, dass diese den Geschäftsbetrieb des AUFTRAGGEBERS in einem geringstmöglichen Maße beeinflussen.

Bezug: EN ISO/IEC 27001:2022 Kapitel 9.2, Kapitel10.1, A.8.34, A.5.35, A.5.36

36 BEWEISSICHERUNG / FORENSISCHE UNTERSTÜTZUNG

Durch den AUFTRAGNEHMER sind

– für Informationen mit dem höchsten Schutzbedarf dauerhaft und

– bei Informationssicherheitsvorfällen mit dem Verdacht auf dolose oder vorsätzliche Handlungen unverzüglich nach Bekanntwerden durch den AUFTRAGNEHMER

Maßnahmen zur Unterstützung von forensischen Untersuchungen durchzuführen. Diese erfolgen auf Basis eines mit AUFTRAGGEBER abgestimmten Konzeptes und Prozesses. Dabei sind insbesondere Maßnahmen in Bezug auf

1. die Datenzusammenstellung / Beweissicherung, insbesondere
   - die Isolierung der betroffenen Systeme,
   - die Verhinderung einer Abschaltung der Systeme vor Beginn der Beweissicherung,
   - die Ermöglichung von forensisch verwertbaren Kopien und
   - eine revisions- und veränderungssichere Aufbewahrung von Logs und Protokolldateien

und

2. die Analyse, insbesondere
   - die Bereitstellung von entsprechend geeigneten Räumlichkeiten,
   - die Bereitstellung von Informationen, Auskünften und Dokumentationen zu ausgenutzten Schwachstellen und
   - die Bereitstellung von Informationen, Auskünften und Dokumentationen zu Abläufen und Zeitpunkten

zu treffen.

Für Cloudleistungen Dritter gilt, dass der Cloudanbieter auf Basis standardisierter Verfahren gemäß ISO/IEC 27001 auf Anforderung forensischer Daten mit Bezug zum AUFTRAGGEBER betreffende Vorfälle zur Verfügung stellt.

Bezug: EN ISO/IEC 27001:2022 A.5.28

37 DOKUMENTATIONEN

In Bezug auf Cloudleistungen folgt der Cloudanbieter standardisierten internen Verfahren gemäß ISO/IEC 27001 und stellt Dokumentationen des Cloudsystems/Anwendung/Service zur Verfügung.

Alle Tätigkeiten aus den o. g. Vorgaben sind durch den AUFTRAGNEHMER zu dokumentieren und zu bewerten und einmal jährlich und bei jeder Änderung unverzüglich dem AUFTRAGGEBER vorzulegen. Diese Dokumentation der Sicherheitsmaßnahmen, der Prozesse und des Betriebs ist gemäß den Anforderungen des Vertrages und der EN ISO/IEC 27001 in der jeweils gültigen Fassung, insbesondere Anhang A, zu erstellen und zu aktualisieren.

Die Anforderungen an die Dokumentation richten sich im Übrigen nach der Anlage 1 Dokumentation und Reporting der SAIT ZVB-IT. Der AUFTRAGNEHMER überprüft die Dokumentationen in angemessenen Abständen und aktualisiert diese entsprechend.

Teile der Dokumentationen, die nicht direkt oder indirekt den jeweilligen Kunden betreffen, können vom Zugang und der Übermittlung ausgeschlossen werden. Dokumentationen, die auch den AUFTRAGNEHMER oder andere Kunden betreffen, sind so aufzubauen, dass der AUFTRAGGEBER diese zumindest auszugsweise zur Verfügung gestellt bekommt.

Für Änderungen der Dokumentationen gelten die Regelungen des Vertrages entsprechend.

Bezug: EN ISO/IEC 27001:2022 A.5.1, A.5.2, A.6.4, A.6.5, A.5.9, A.5.10, A.5.15, A.8.24, A.7.7, A.8.13, A.8.15, A.5.14, A.6.6, A.5.8, A.8.26, A.8.27, A.5.21, A.5.26, A.5.29, A.5.31, A.5.33

38 PRÜFUNG DER MAßNAHMENUMSETZUNG

Der AUFTRAGNEHMER implementiert und betreibt ein System zur Bewertung in Bezug auf die Wirksamkeit und Leistungsfähigkeit des ISMS und der getroffenen Maßnahmen.

Der AUFTRAGNEHMER überprüft und berichtet dem AUFTRAGGEBER in angemessenen, regelmäßigen Abständen, jedoch mindestens jährlich und nach jedem Informationssicherheitsvorfall nach Maßgabe der Ziff. 8.6, die Umsetzung der in diesem Dokument definierten Anforderungen und die Einhaltung der Maßnahmen und technischen Vorgaben.

Der AUFTRAGNEHMER verbessert und passt die durch ihn getroffenen Maßnahmen kontinuierlich entsprechend der gewonnenen Erkenntnisse an.

Für Cloudleistungen Dritter gilt, dass der Cloudanbieter auf Anfrage Überprüfungen und Berichte in standardisierten internen Verfahren gemäß ISO/IEC 27001 bereitstellt.

Bezug: EN ISO/IEC 27001:2022 Kapitel 9.1, 9.3, 10.2, A.5.36/A.8.8

39 MONITORING, BERICHTSWESEN

Die Funktionsfähigkeit des ISMS und der Informationssicherheitsmaßnahmen ist durch den AUFTRAGNEHMER mittels eines geeigneten Monitorings zu überwachen.

Bezug: EN ISO/IEC 27001:2022 Kapitel 5.3

40 BEENDIGUNG DES VERTRAGSVERHÄLTNISSES

Bei Beendigung des Vertragsverhältnisses gelten die Regelungen zum Ablauf des Exit-Prozesses wie in Anlage 2 Exit Management der SAIT ZVB-IT vereinbart.

Bezug: EN ISO/IEC 27001:2022 A.7.14, A.5.34

41 AHNDUNG VON VERSTÖßEN

Der AUFTRAGNEHMER haftet für jede schuldhafte Verletzung der Regelungen dieses Dokumentes. Eine Umkehr der Beweislast ist hiermit nicht verbunden.

Der AUFTRAGNEHMER wird den jeweiligen Kunden von allen Schäden freistellen und schadlos halten, die aus der Verletzung von Verpflichtungen des AUFTRAGNEHMERS und / oder seiner Erfüllungsgehilfen resultieren, insbesondere, aber nicht ausschließlich, von Schäden durch Buß- und Strafgelder.

Schuldhafte Verstöße der von dem AUFTRAGNEHMER eingesetzten Personen gegen Regelungen dieses Dokumentes sind durch den AUFTRAGNEHMER entsprechend den internen Regelungen der AUFTRAGNEHMERS zu ahnden.

Bezug: EN ISO/IEC 27001:2022 A.6.4

42 SCHLUSSBESTIMMUNGEN

Die Kosten des AUFTRAGNEHMERS der Umsetzung der Vorgaben dieses Dokumentes trägt der AUFTRAGNEHMER. Der AUFTRAGNEHMER stellt sicher, zur Erfüllung der vereinbarten Vorgaben genügend und ausreichend qualifiziertes Fachpersonal für den AUFTRAGGEBER vorzuhalten.

Abweichungen von den vereinbarten Vorgaben sind nur in begründeten Fällen zulässig und bedürfen der vorhergehenden Zustimmung des AUFTRAGGEBERS.

APPENDIX A – Verpflichtungserklärung

Diese Verpflichtungserklärung zu Geheimhaltung, Datenschutz und Datensicherheit wird zwischen

……..

……...

– nachfolgend **AUFTRAGNEHMER** genannt –

und

«Name», «Vorname»

– nachfolgend **Externer Mitarbeiter** genannt –

geschlossen.

Der Externe Mitarbeiter wird über die bei dem AUFTRAGNEHMER erlangten vertraulichen Informationen gegenüber jedermann Verschwiegenheit bewahren, soweit dies das Geschäftsinteresse des AUFTRAGNEHMERS, der SITA Airport IT GmbH („AUFTRAGGEBER“) und/oder deren Kunden, wie z.B. der Flughafen Düsseldorf GmbH („FDG“) und / oder der mit der FDG verbundenen Unternehmen erfordert.

Es ist dem externen Mitarbeiter gemäß Art. 28 Abs. 3 Bstb. b DS-GVO untersagt, geschützte personen- und sachbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonstwie zu nutzen.

Die Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung der Tätigkeit für den AUFTRAGNEHMER fort.

Alle Schriftstücke, Zeichnungen, Aufzeichnungen, Bücher und Gegenstände aller Art, die der externe Mitarbeiter im Rahmen seiner Tätigkeit bei dem AUFTRAGNEHMER erhalten oder angefertigt hat, sind mit Abschluss der Erbringung der Leistungen durch den externen Mitarbeiter dem AUFTRAGNEHMER zurückzugeben, sofern im Einzelfall keine anderslautende Abmachung getroffen wird.

[Ort], [Datum]

Unterschrift des Externen Mitarbeiters