Vorgaben zur Informationssicherheit in Lieferantenbeziehungen

Hinweis zur sprachlichen Gleichbehandlung:
Dieses Dokument richtet sich an alle Personen im definierten Geltungsbereich, unabhängig von Geschlecht, Herkunft oder sonstigen persönlichen Merkmalen. Aus Gründen der Lesbarkeit und Einheitlichkeit wird im Dokument der generische Maskulin verwendet. Diese Formulierung schließt alle Geschlechter gleichermaßen ein.

Dokumenteingenschaften

Dokumenten-ID	Vorgaben_InfoSec_Lieferantenbeziehungen.docx
Dokumenten-Eigentümer (Ersteller)	Tony Hentschel, Stadtreinigung Dresden GmbH
Dokumenten-Prüfer (Prüfer)	Kerstin Sachse, Technische Werke Dresden GmbH
Dokumenten-Freigeber (Freigeber)	Paul Timmermann, Stadtreinigung Dresden GmbH
Dokumentenart	ISMS Stufe 2 - Richtlinie
Klassifizierung	S2: intern
Geltungsbereich	externe IT-Dienstleister
Aktuelle Version	1.0

Dokumentenstatus und Freigabe

Status	Version	Datum	Name und Abteilung /Firma
Review	1.0	17.03.2026	Tony Hentschel, IT/Sicherheit, Stadtreinigung Dresden GmbH
Änderung			
Übernahme des Inhaltes in SRD-Vorlage, überarbeiten der Darstellung/Layout			
Wählen Sie ein Element aus.	0.0	Klicken oder tippen Sie, um ein Datum einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
Änderung			
Klicken oder tippen Sie hier, um Text einzugeben.			
Wählen Sie ein Element aus.	0.0	Klicken oder tippen Sie, um ein Datum einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
Änderung			
Klicken oder tippen Sie hier, um Text einzugeben.			
Wählen Sie ein Element aus.	0.0	Klicken oder tippen Sie, um ein Datum einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
Änderung			
Klicken oder tippen Sie hier, um Text einzugeben.			

1. Geltungsbereich, Ziele, Verantwortlichkeiten 4
2. Verantwortlichkeiten 5
3. Informationssicherheitsmanagement 6
4. Meldung von Informationssicherheitsvorfällen 9
5. Eingesetztes Personal und Nachauftragnehmer 11
6. IT-Infrastruktur, Zugriffe und Verschlüsselung 13
7. Künstliche Intelligenz 17
8. Schwachstellenmanagement und Softwareentwicklung 18
9. Zusammenarbeit 20
10. Beendigung der Leistung 23
11. Kontaktdaten 25
12. Glossar 26

1. Geltungsbereich, Ziele, Verantwortlichkeiten

Diese Anlage legt die verbindlichen Mindestanforderungen an die Informationssicherheit in der Leistungsbeziehung zwischen Auftraggeber und Auftragnehmer fest. Sie dient der Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der damit verbundenen Systeme, Anwendungen und Prozesse. Der Auftragnehmer verpflichtet sich, die definierten Vorgaben einzuhalten. Auftragnehmer sind definiert als jeder Dritte, der Leistungen für die Stadtreinigung Dresden auf Basis vertraglicher Beziehungen erbringt. Diese Anlage richtet sich an die Geschäftsleitung der Lieferanten, deren Mitarbeiter sowie deren Erfüllungs- oder Verrichtungsgehilfen. Der Auftraggeber behält sich das Recht vor, die Einhaltung insgesamt, mittels Stichproben oder anhand übergebener Dokumentationen zu überprüfen.

Im Rahmen der Leistungserbringung werden die Lieferanten hinsichtlich der Informationssicherheit in drei grundlegende Lieferantenkategorien eingeordnet. Aus diesem Grund enthält diese Anlage Regelungen für drei Katego-rien von IT-Lieferanten (Allgemein, Integriert, Kritisch). Die Einordnung des Auftragnehmers in eine der Lieferantenkategorien erfolgt im jeweiligen Einzelvertrag. Soweit nicht gekennzeichnet, gelten alle Regelungen für alle drei Lieferantenkategorien. Regelungen, die zusätzlich nur für die Lieferantenkategorien „Integriert“ und/oder „Kritisch“ gelten, sind besonders gekennzeichnet.

1.1. Motivation, Ziele und Rahmen

Die betrieblichen Abläufe der Stadtreinigung Dresden sind von sicheren und funktionierenden informationstechnischen Systemen und Komponenten abhängig. Sie sind wesentlicher Bestandteil verschiedener Kernprozesse zur Erreichung der Unternehmensziele und damit Grundlage für den Erfolg unserer Unternehmen. Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung.

Als systemkritischer Energieversorger betreibt die Stadtreinigung Dresden, unter Verwendung von informationstechnischen Systemen und Komponenten, kritische Infrastrukturen, die für das Funktionieren des Gemeinwesens von hoher Bedeutung sind. Die Stadtreinigung Dresden ist sich bewusst, dass ihr Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit oder die betroffene Bevölkerung bedeuten könnte.

Der Vorstand der Stadtreinigung Dresden AG hat nachfolgende Ziele der Informationssicherheit festgelegt:

- Vermeidung von Störungen der Vertraulichkeit, Verfügbarkeit, Integrität sowie erforderlichenfalls Authentizität informationstechnischer Systeme, Komponenten oder Prozesse,
- Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, ein-schließlich Minimierung des Ausmaßes potenzieller Schäden,
- Aufrechterhaltung der Versorgungssicherheit, insbesondere kritischer Infrastrukturen, in den jeweiligen Versorgungsgebieten, einschließlich übernommener Betriebsführungen,
- Einhaltung von gesetzlichen Vorgaben und Regularien sowie Einhaltung von Verträgen,
- Vermeidung von monetären Schäden durch Vorfälle und Erhalt des Firmenimages.

2. Verantwortlichkeiten

2.1. Der Auftragnehmer hat dafür zu sorgen, dass die Leistungserbringung den hier folgenden Vorgaben folgt.

2.2. Der Auftragnehmer hat jederzeit sicher zu stellen, dass sein Handeln, das Handeln seiner Beschäftigten und seiner Erfüllungs-/Verrichtungsgehilfen nicht die Verfügbarkeit, Vertraulichkeit oder Integrität bzw. Authentizität der Assets der Stadtreinigung Dresden beeinträchtigt.

2.3. Mitarbeiter oder Erfüllungs-/Verrichtungsgehilfen des Auftragnehmers müssen vom Auftragnehmer auf die Anforderungen im Sinne dieser Vereinbarung verpflichtet werden. Dem Auftraggeber ist jederzeit Einsicht in diese Verpflichtungen zu gewähren.

2.4. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die ordnungsgemäße Erfüllung der Einhaltung der vereinbarten Sicherheitsanforderungen durch Mitarbeiter oder Erfüllungs-/Verrichtungsgehilfen (einschließlich Subunternehmer) verantwortlich und haftet für deren Handlungen und Unterlassungen wie für eigenes Verhalten gemäß § 278 BGB sowie für die Einhaltung der datenschutzrechtlichen Vorgaben nach Art. 28 und Art. 32 DSGVO.

3. Informationssicherheitsmanagement

3.1. Der Auftragnehmer hat grundlegende Sicherheitsrichtlinien für die Nutzung und den Betrieb der IT-Infrastruktur definiert und in seinem Unternehmen etabliert. Dies umfasst insbesondere aber nicht ausschließlich die folgenden Themenkomplexe:

- Klassifizierung und Kennzeichnung von vertraulichen bzw. schützenswerten Informationen
- Rechte- und Rollenkonzept für den Zugriff auf Informationen
- Meldung und Behandlung von Informationssicherheitsvorfällen
- Regeln und Verfahren für die sichere Nutzung von Passwörtern
- Absicherung der IT-Infrastruktur (z.B. Härtung, Schwachstellenmanagement, Malware-Schutz)
- Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken

3.2. Die Mitarbeiter des Aufragnehmers werden regelmäßig (mindestens jährlich) zum Thema Informationssicherheit geschult.

3.3. Ist die Leistungserbringung den Lieferantenkategorien „Integriert“ oder „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

3.3.1. Der Auftragnehmer hat sich bei der Organisation seiner IT-Prozesse eines anerkannten Rahmenwerks (z.B. ITIL, COBIT) für das Management und die Steuerung der IT zu bedienen.

3.3.2. Zur Etablierung und Aufrechterhaltung eines angemessenen Schutzes aller Informationen soll der Auftragnehmer sein Informationssicherheitsmanagementsystem (ISMS) nach einem anerkannten Standard (z.B. nach ISO/IEC 27001, BSI IT-Grundschutz) ausrichten und unterhalten.

3.3.3. Der Auftragnehmer hat geeignete Maßnahmen zu etablieren, die die Sicherheit der Lieferkette einschließlich sicherheitsrelevanter Aspekte der Beziehungen zu unmittelbaren Lieferanten und Dienstleistern gewährleisten. Ebenso sind Sicherheitsvorkehrungen für die Beschaffung, Entwicklung und Wartung informationstechnischer Systeme, Komponenten und Prozesse umzusetzen.

3.3.4. Der Auftragnehmer ist verpflichtet, seine Mitarbeiter regelmäßig, anlassbezogen, mindestens jedoch einmal jährlich, in Bezug auf die Sicherstellung der Informationssicherheit zu sensibilisieren und zu schulen und dies dem Auftraggeber in geeigneter Weise nachzuweisen. Inhalte dieser Schulungen müssen gemäß aktuellen Erkenntnissen angepasst werden.

3.3.5. Der Auftragnehmer ist verpflichtet, den Auftraggeber auf Verlangen über Sicherheitsmaßnahmen, Änderungen im IT-Sicherheitsmanagement, Sicherheitsvorfälle und die Ergebnisse durchgeführter IS-Revisionen und Penetrationstests in einer mit dem Auftraggeber abgestimmten Form zu informieren, insofern sie in Bezug zu den zu erbringenden Leistungen stehen.

3.3.6. Der Auftragnehmer ist verpflichtet sicherzustellen, dass zu jeder Zeit handlungsfähiges und entsprechend geschultes Personal bereitsteht, um bei IT-sicherheitsrelevanten Vorfällen, Systembeeinträchtigungen und/oder -ausfällen (Security Incident Handling und Troubleshooting) zeitnahe Abhilfe zu schaffen.

3.3.7. Der Auftragnehmer ist verpflichtet, mit geeigneten Notfallvorsorgemaßnahmen seine Leistungsfähigkeit kontinuierlich aufrecht zu erhalten. Dabei sollte er sich an anerkannten Standards (beispielsweise ISO 22301, oder BSI-Standard 200-4) orientieren.

3.3.8. Der Auftragnehmer muss ein geeignetes Konzept zur Fortführung der kontinuierlichen Erbringung der Leistung vorlegen. Das Konzept soll im Fall von unvorhersehbaren Schadensereignissen vor schwerwiegenden Betriebsunterbrechungen wie z.B. Naturereignisse, Versorgungsunterbrechungen, Informationssicherheitsvorfälle durch Dritte schützen und den Schaden begrenzen.

3.4. Ist die Leistungserbringung der Lieferantenkategorie „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

3.4.1. Der Auftragnehmer ist verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) nach einem anerkannten Standard (z.B. nach ISO/IEC 27001, BSI IT-Grundschutz) zur Etablierung und Aufrechter-haltung eines angemessenen Schutzes aller Informationen zu implementieren und zu unterhalten. Der Geltungsbereich der Zertifizierung muss mindestens den Bereich der vereinbarten Leistungen abdecken.

3.4.2. Der Auftragnehmer weist dem Auftraggeber kontinuierlich die Einhaltung der in Ziffer 3.4.1 aufgeführten Pflichten durch Übermittlung eines jeweils gültigen Zertifikates einer anerkannten Zertifizierungsstelle (einer unter www.dakks.de gelisteten Zertifizierungsstelle) nach.

3.4.3. Um die Wirksamkeit von Maßnahmen im Bereich des Notfallmanagements zu gewährleisten, müssen durch den Auftragnehmer regelmäßig Tests und Notfallübungen (z.B. in Form eines inszenierten Ausfalls eines Standorts des Auftragnehmers) durchgeführt werden. Die wesentlichen Ziele sind dabei, Inkonsistenzen in den Notfallplänen oder Mängel in der Planung und Umsetzung von Notfallmaßnahmen aufzudecken, sowie effektive und reibungslose Abläufe in einem Notfall zu trainieren. Der Auftragnehmer verpflichtet sich, die Notfallübungen zu dokumentieren und auf Anfrage durch den Auftraggeber bereitzustellen.

3.4.4. Soweit Gegenstand der Vertragsleistung Cloud-Services sind, ist der Auftragnehmer verpflichtet, ein Business Continuity Management System (BCMS) nach einem anerkannten Standard (z.B. ISO/IEC 22301, BSI-Standard 200-4) zur Etablierung und Aufrechterhaltung der notwendigen Prozesse zur Leistungser-bringung zu implementieren und zu unterhalten.

3.4.5. Der Auftragnehmer muss dem Auftraggeber die Priorisierung des Wiederanlaufs für die angebotenen Dienste transparent und in geeigneter Weise darstellen.

4. Meldung von Informationssicherheitsvorfällen

4.1. Ist die Leistungserbringung den Lieferantenkategorien „Integriert“ oder “Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

4.1.1. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei Kenntnisnahme über Sicherheitsvorfälle, die den Auftraggeber betreffen oder betreffen könnten, unverzüglich zu informieren. Dies bezieht sich insbeson-dere auf Vorfälle, welche die Vertraulichkeit, Verfügbarkeit oder Integrität der Informationen des Auftrag-gebers betreffen könnten.

4.1.2. Sicherheitsvorfälle sind insbesondere (nicht abschließend):

- Der Verlust von Hardware des Auftragnehmers mit Daten des Auftraggebers, zur Verfügung gestellte Geräte des Auftraggebers, physische Identifikations- und Zutrittsmittel (inkl. Geräte für eine Multi-Faktor-Authentifizierung) oder sonstige Assets des Auftraggebers
- die Kompromittierung von Zugangsdaten/Passwörtern für Systeme des Auftraggebers sowie schwerwiegende Software-Fehler oder Zero-Day-Schwachstellen in der an die Stadtreinigung Dresden bereitgestellte/gelieferte Software.
- Informationssicherheitsereignisse (z.B. auftretende Störungen, Verstöße gegen diese Vereinbarung), welche Daten oder Systeme des Auftraggebers in Bezug auf Vertraulichkeit, Integrität oder Verfügbarkeit negativ beeinflussen bzw. negativ beeinflussen können;

4.1.3. Sicherheitsvorfälle oder Informationssicherheitsereignisse beim Auftragnehmer mit laufenden Untersuchungen und Behebungen sind spätestens nach 12 Stunden der internen Entdeckung zu melden, sofern potenzielle Auswirkungen auf die Stadtreinigung Dresden bzw. den verbundenen Unternehmen bis zu diesem Zeitpunkt nicht ausgeschlossen werden können. Dazu zählen unter anderem der Verlust von Hardware und Identifikationsmitteln des Auftragnehmers mit potenziellem Zugriff auf Daten des Auftraggebers, Angriffe/Infiltration/Malware mit unklarer Auswirkung, Datenverlust, identifizierte Zero-Day-Schwach-stellen in der Infrastruktur des Auftragnehmers.

4.1.4. Die Meldung muss mindestens die folgenden Informationen erhalten, soweit zutreffend

- Zeitpunkt des Vorfalles, Zeitpunkt der Feststellung
- Art des Vorfalles/Ursache
- Schweregrad/Kritikalität
- betroffene Daten/Software/Geräte/Identifikationsmittel
- (soweit aktuell bekannt)
- aktuelles Lagebild und Wirksamkeit der bislang umgesetzten Maßnahmen

4.1.5. Im Falle eines Informationssicherheitsvorfalles muss der Auftragnehmer dem Auftraggeber alle Informationen, die für die Analyse und/oder interne Bearbeitung des Informationssicherheitsvorfalles notwendig sind, in einem zur Weiterverarbeitung geeigneten, gängigen Datenformat zur Verfügung stellen.

4.1.6. Der Auftragnehmer ist verpflichtet, mit den für den Auftraggeber zuständigen Aufsichtsbehörden zusam-menzuarbeiten, Kontrollen der Behörden vor Ort zu ermöglichen und den Auftraggeber bei behördlichen Kontrollmaßnahmen umfassend zu unterstützen. Dies umfasst insbesondere, aber nicht ausschließlich:

- Regulatorisch vorgeschriebene Audits (z.B. durch vom BSI bestellte Auditoren)
- Audits durch die Stadtreinigung Dresden oder durch sie ernannte und bevollmächtigte Auditoren, die sich aus dem individuellen Risiko der Leistungserbringung ergeben
- Datenschutzbehörden/ BSI nach einem Sicherheitsvorfall/Datenpanne

5. Eingesetztes Personal und Nachauftragnehmer

5.1. Der Auftragnehmer ist verpflichtet, die Mitarbeiter, die er im Rahmen der Erfüllung seiner vertraglichen Pflichten gegenüber dem Auftraggeber einsetzt, vor ihrem Einsatz auf die vertraglichen Anforderungen zur Sicherstellung der Informationssicherheit und der Vertraulichkeitsverpflichtung im Hinblick auf den Umgang mit Daten und Systemen des Auftraggebers hinzuweisen und dies in geeigneter Form zu doku-mentieren.

5.2. Der Auftragnehmer ist verpflichtet, den Auftraggeber vor Vertragsschluss schriftlich über alle Subunter-nehmer zu informieren, die er plant bei der Erbringung der Leistung für den Auftraggeber einzusetzen.

5.3. Der Auftragnehmer ist verpflichtet, den Auftraggeber anlassbezogen über Änderungen in der Leistungs-erbringung sowie den Einsatz neuer oder den Austausch bestehender Subunternehmer schriftlich zu unterrichten.

5.4. Wenn und soweit der Auftragnehmer Teile der nach diesem Vertrag oder dieser Anlage geschuldeten Leistung für den Auftraggeber an Subunternehmer auslagert, ist der Auftragnehmer verpflichtet, die Sicherheitsanforderungen, die der Auftraggeber und der Auftragnehmer vereinbart haben, entsprechend mit diesen Subunternehmern zu vereinbaren. Die Sicherheitsanforderungen an Subunternehmer müssen insbesondere so definiert werden, dass die Sicherheitsstandards für die Daten des Auftraggebers und Leistungen für den Auftraggeber in jedem Fall eingehalten werden können und dass der Auftragnehmer in der Lage ist, eigene Verpflichtungen zur Sicherheit gegenüber dem Auftraggeber vollumfassend zu erfül-len. Der Auftragnehmer ist verpflichtet, dem Auftraggeber die Erfüllung dieser Pflicht in geeigneter Weise nachzuweisen.

5.5. Ist die Leistungserbringung den Lieferantenkategorien „Integriert“ oder „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

5.5.1. Der Auftraggeber ist berechtigt, aus wichtigem Grund die Auswechslung von Personal des Auftragnehmers zu verlangen. Dies gilt insbesondere dann, wenn berechtigte Zweifel an der notwendigen Erfahrung oder Qualifikation bestehen bzw. Arbeitssicherheits-, IT-Sicherheits- und Umweltschutzbestimmungen oder vertragliche Pflichten nicht beachtet werden. Auf Wunsch des Auftraggebers sind entsprechende aktuelle Nachweise vorzulegen. Der Auftragnehmer verpflichtet sich, in diesen Fällen unverzüglich für qualifizierten Ersatz zu sorgen. Die vereinbarten Termine und Fristen bleiben hiervon unberührt.

5.6. Ist die Leistungserbringung der Lieferantenkategorie „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

5.6.1. Sofern Mitarbeiter des Auftragnehmers besonders kritische Tätigkeiten für den Auftraggeber erbringen oder Zugriff auf geschäftskritische Systeme erhalten, umfasst die Überprüfung dieser Personen insbe-sondere weitergehende Prüfungen, die rechtlich oder aus Sicht des Auftraggebers erforderlich sind, etwa die Einholung eines polizeilichen Führungszeugnisses zur Prüfung auf Vorstrafen; diese Maßnahmen dienen der Minimierung von Sicherheits- und Betriebsrisiken und sind vor Aufnahme der Tätigkeit abzuschließen.

5.6.2. Sofern für die Leistungserbringung gegenüber dem Auftraggeber Dritte durch den Auftragnehmer genutzt werden, stellt der Auftragnehmer sicher, dass auch der Dritte sein Einverständnis zur Durchführung der Audits und Sicherheitsüberprüfungen durch den Auftraggeber erteilt.

6. IT-Infrastruktur, Zugriffe und Verschlüsselung

6.1. Der Auftragnehmer muss innerhalb seiner eigenen IT-Systeme einen angemessenen Schutz vor Schad-software implementieren und aktuell halten. Dies umfasst insbesondere den Einsatz von zeitgemäßen Lösungen zur Erkennung und Abwehr von Malware (einschließlich Viren, Trojanern, Ransomware und vergleichbaren Bedrohungen) sowie ergänzende Sicherheitsmaßnahmen wie Spam- und Phishing-Schutz. Die eingesetzten Systeme müssen dem Stand der Technik entsprechen und regelmäßig aktualisiert sowie überwacht werden.

6.2. Der Auftragnehmer ist verpflichtet, seine IT-Systeme und IT-Dienste zu überwachen und die ihm vor-liegenden Informationen hinsichtlich Verfügbarkeit, Kapazität und Sicherheit auszuwerten.

6.3. Bei Systemen, die nicht nur für den Auftraggeber betrieben werden (gemischt betriebene Systeme), verpflichtet sich der Auftragnehmer, ein geeignetes Berechtigungsmanagement zur Verfügung zu stellen, in dem gewährleistet ist, dass Zugriffsrechte für den Auftraggeber und andere Nutzer granular und getrennt vergeben werden können. (z.B. Attribute-Based Access Control).

6.4. Ergänzend zu Ziffer 6.3 sind durch den Auftragnehmer technische Backend-Accounts und Zugangsdaten (z. B. für Datenbanken, Systemintegrationen oder Service-APIs) so zu gestalten, dass eine Kompro-mittierung bei einem Auftraggeber (Kunden) nicht zu einer Gefährdung anderer Auftraggeber (Kunden) führt. Insbesondere dürfen keine globalen oder hardcodierten Zugangsdaten verwendet werden, die für mehrere Auftraggeber (Kunden) identisch sind.

6.5. Ist die Leistungserbringung den Lieferantenkategorien „Integriert“ oder „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

6.5.1. Der Auftragnehmer hat sicherzustellen, dass die im Rahmen der Leistungserbringung eingesetzten Mitar-beitenden des Auftragnehmers die ihnen zum Zwecke der Leistungserbringung überlassenen Authentisierungsinformationen sorgfältig behandeln. Dies beinhaltet insbesondere, dass Authentisierungsinformationen nicht weitergegeben werden und dass bei Verdacht von Kompromittierung diese umgehend erneuert werden müssen.

6.5.2. Die Nutzung von Sammelkonten („shared accounts“), für interaktive Anmeldungen an Systemen des Auf-traggebers oder an Systemen, die dessen Daten verarbeiten, ist nur nach expliziter Freigabe durch den Auftraggeber gestattet. Ist ein Sammelkonto notwendig, so ist dies nur zulässig, wenn die Verwendung dieses Sammelkontos im Nachgang einer real handelnden Person zugeordnet werden kann. Hierfür ist der Einsatz von vor- oder nachgelagerten Authentifizierungsmethoden (z.B. Sprungserver), Dokumentation in Schichtplänen, Ticketsystemen oder anderen geeigneten Methoden beim Auftragnehmer vorzusehen bzw. zu implementieren. Diese Daten sind mind. 12 Monate aufzubewahren. Der Auftraggeber behält sich das Recht vor, anlassbezogen die Identität der handelnden Person(en) abzufragen.

6.5.3. Der Auftragnehmer hat sicherzustellen, dass Nutzer und Administratoren ausschließlich die Zugriffsrechte erhalten, die sie zur Erfüllung der vertraglichen Pflichten des Auftragnehmers benötigen. Der Auftragneh-mer ist verpflichtet, die Zugriffsrechte für Systemdateien restriktiv, d.h. nur im erforderlichen Umfang, zu vergeben.

6.5.4. Der Auftragnehmer hat sicherzustellen, dass sämtliche Zugriffsrechte entsprechend einem klaren, vordefinierten Rollenkonzept vergeben werden, welches fortlaufend überprüft und aktualisiert wird. Der Auftragnehmer hat ferner sicherzustellen, dass Zugriffsrechte im Falle der Veränderung des Rollenkonzeptes oder der Beendigung dieser Vereinbarung unverzüglich entzogen werden.

6.5.5. Der Auftragnehmer trägt dafür Sorge, dass Mitarbeiter des Auftragnehmers sowie von ihm beauftragte Dritte mit Administratorenrechten für Systeme und Anwendungen, die durch den Auftragnehmer für den Auftraggeber betrieben werden, nur im Wege der Zwei-Faktor-Authentisierung zugreifen.

6.5.6. Der Auftragnehmer verpflichtet sich, alle Informationen des Auftraggebers so zu isolieren, dass Daten und Ausführungsbereiche nicht mit denen anderer Kunden vermischt werden (z. B. eigene Instanzen, durch Mandanten-Isolation oder Container-Technologien).

6.5.7. Der Auftragnehmer hat regelmäßige Datensicherungen, durchzuführen. Umfang, Speicherintervalle, Spei-cherzeitpunkte und Speicherdauer sind an der Leistung auszurichten und nachvollziehbar zu dokumentie-ren.

6.5.8. Der Auftragnehmer hat für eine sichere Grundkonfiguration von Serversystemen zu sorgen, beispielsweise durch den Einsatz gehärteter Betriebssysteme und die Deaktivierung nicht benötigter Funktionen.

6.5.9. Der Auftragnehmer hat dem Auftraggeber unter Angabe des Landes und der Region offenzulegen, an welchen Standorten die Daten des Auftraggebers gespeichert werden.

6.5.10. Der Auftragnehmer hat wirksame Sicherheitsmaßnahmen gegen netzbasierte Angriffe, einschließlich Distributed Denial of Service (DDoS), zu implementieren. Dies umfasst insbesondere den Einsatz geeigneter Technologien wie Firewalls, IPS/IDS-Systeme, Application Layer Gateways sowie Mechanismen zur Über-wachung der Verfügbarkeit und zur Sperrung oder Filterung von schädlichem Netzwerkverkehr.

6.5.11. Der Auftragnehmer muss sicherstellen, dass Daten sowohl ‚in transfer' als auch ‚at rest' verschlüsselt übertragen und/oder gespeichert werden. Dies gilt insbesondere aber nicht ausschließlich für Daten mit hohem Schutzbedarf (z. B. Steuerungsdaten einer kritischen Anlage oder vertrauliche Geschäftsdaten), die über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

6.5.12. Der Auftragnehmer hat eine angemessene und geeignete Netzsegmentierung sicherzustellen. Netzwerk-segmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen müssen durch den Auftragnehmer (z.B. durch Firewalls) voneinander getrennt werden.

6.5.13. Physische Bereiche mit schützenswerten Informationen oder Systemen des Auftraggebers sind ange-messen vor unautorisierten Zutritten zu schützen. Die Bereiche sind fortlaufend zu überwachen, beispielsweise durch Zutrittskontrollsysteme, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal oder Alarmsysteme.

6.6. Ist die Leistungserbringung der Lieferantenkategorie „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

6.6.1. Der Auftragnehmer ist verpflichtet, seine relevanten IT-Systeme so zu organisieren, dass ein beherrschbares Schadensereignis nicht gleichzeitig alle genutzten IT-Systeme beeinträchtigt. Ein beherrschbares Schadensereignis ist z.B. Feuer, Explosion, Unfälle im Straßen-, Schienen-, Wasser- oder Luftverkehr oder Naturkatastrophen mit begrenzter Breitenwirkung, wie beispielsweise ein Flusshochwasser.

6.6.2. Der Auftragnehmer hat für Admin- und Power-User-Zugänge auf Systeme des Auftraggebers im Zusammenhang mit der Erbringung der vertragsgegenständlichen Leistungen vor Vergabe von privilegierten Zu-gangsrechten, die im Rahmen der Auftragserbringung verwendet werden, die schriftliche Zustimmung des Auftraggebers einzuholen. Die Anforderung hat mindestens die einzurichtenden Nutzer, die Systeme, den Berechtigungsumfang der Zugänge, den Gültigkeitszeitraum sowie den Grund zu benennen.

6.6.3. Die nach Ziffer 6.6.2 eingerichteten Zugänge sind regelmäßig auf deren Notwendigkeit zu überprüfen. Die privilegierten Accounts haben eine Gültigkeit von bis zu 24 Monaten und einen Prüfzyklus von je 12 Mo-naten. Jede positive Prüfung verlängert die Gültigkeit um bis zu weitere 24 Monate.

6.6.4. Der Auftragnehmer ist verpflichtet, für Power-User und Administratoren ein Account-Recording einzurichten und die Aufzeichnungen unveränderbar an ein sicheres, getrenntes System weiterzuleiten. Die Aufzeichnungen sind sicher (Vertraulichkeit, Integrität und Verfügbarkeit, Authentizität) für mindestens 12 Monate aufzubewahren.

6.6.5. Der Auftragnehmer ist verpflichtet, die Dateizugriffsrechte auf Systemdateien nach dem Prinzip der minimalen Rechte zu konfigurieren, sodass nur für den Betrieb erforderliche Berechtigungen bestehen.

6.6.6. Um sicherzustellen, dass keine veralteten und als unsicher bekannte Kryptographielösungen in den Produkten verwendet werden, die der Auftragnehmer dem Auftraggeber bereitstellt oder verkauft oder die sonst bei dem Auftraggeber zum Einsatz kommen, muss der Auftragnehmer eine schriftliche Richtlinie etablieren, egelmäßig aktualisieren und dem Auftraggeber auf Anfrage bereitstellen. Diese Richtlinie soll sich an anerkannten Standards orientieren (z. B. BSI TR 02102 in der jeweils aktuellen Version).

6.6.7. Sobald eine angewandte Kryptographielösung in der Industrie als nicht mehr sicher bekannt wird, müssen sowohl die Richtlinie als auch die Umsetzung derselben angepasst werden. Wenn eine solche Kryptogra-phielösung in dem bereits beim Auftraggeber eingesetzten Produkt verwendet wird, muss der Auftrag-nehmer sie im Rahmen vom Vulnerability-Management-Prozess als Schwachstelle bewerten und mel-den. Der Auftragnehmer hat Vorschläge zur Behebung der Schwachstelle zu unterbreiten.

6.6.8. Der Auftragnehmer wird dem Auftraggeber auf Verlangen eine aktuelle Übersicht über die verwendeten kryptographischen Absicherungen für IT-Systeme des Auftraggebers oder für Systeme, die Daten des Auftraggebers verarbeiten zur Verfügung stellen.

6.6.9. Der Auftragnehmer muss sicherstellen, dass administrative Aufgaben nach dem Prinzip der Funktionstrennung (Segregation of Duties, SoD) durchgeführt werden. Dabei ist insbesondere auf eine Trennung zwischen ausführenden und kontrollierenden/genehmigenden Funktionen zu achten, wie z.B. Beantragung, Genehmigung und Zuweisung von Zugriffsrechten.

7. Künstliche Intelligenz

7.1. Der Auftragnehmer hat zu Beginn der Leistungserbringung in Textform anzugeben, ob und in welchem Umfang Künstliche Intelligenz (KI) im Sinne des EU AI Act eingesetzt wird. Er stuft die eingesetzte KI nach dem EU AI Act ein und begründet seine Einstufung.

7.2. Der Auftragnehmer beschriebt in Textform die folgenden Themenkomplexe

a) konkreten KI-Funktionen (z. B. Prognosen, Textanalyse, Entscheidungsunterstützung),
b) verwendete KI-Technologie (z. B. LLM, Machine Learning, regelbasierte Systeme) und
c) Beschreibung der betrieblichen Zielsetzung
d) Eigenentwicklung oder Einbindung externer Dienste (Bei Nutzung externer Dienste sind Anbieter, Produktbezeichnung und Hosting-Standort anzugeben)
e) Trainingsverfahren, die verwendeten Datentypen und die Datenquellen
f) Verfahren zur Sicherstellung von Fairness und/oder Bias

7.3. Soweit vertraglich nicht anders vereinbart, trifft der Auftragnehmer technische Maßnahmen, die sicher-stellen, dass keine Daten des Auftraggebers in Trainingsdaten Dritter oder in unkontrollierbare Ausgaben einfließen. Dies umfasst mindestens aber nicht ausschließlich die Themen Datenisolation, Verschlüssel-ung, Zugriffskontrolle, Auditierbarkeit).

7.4. Inhaltliche Änderungen im Rahmen der Leistungserbringung mit Bezug zu den Ziffern 7.1und 7.2 sind dem Auftraggeber unverzüglich schriftlich mitzuteilen. Auftraggeber und Auftragnehmer bewerten diese Änderungen gemeinsam mit Blick auf die Leistungserbringung und vereinbaren Maßnahmen zum Umgang mit diesen Maßnahmen.

8. Schwachstellenmanagement und Softwareentwicklung

8.1. Der Auftragnehmer verpflichtet sich auf die Einhaltung allgemein anerkannter Standards für die Sicherheit des Software Development Life Cycle-Prozesses (z.B. von NIST, OWASP etc.). Dies gilt insbesondere für die Entwicklung von Standardsoftware, Individualsoftware oder auch die Bereitstellung von Cloud-Service, soweit anwendbar.

8.2. Der Auftragnehmer hat sicherzustellen, dass nur mit der Entwicklung betraute Mitarbeiter des Auftragnehmers Zugriff zum Quellcode erhalten.

8.3. Sofern der Auftragnehmer Software oder Komponenten Dritter (z.B. kommerziell, frei, Open Source, Closed-Source), in die ausgelieferten Softwareprodukte integriert oder diese im Rahmen der Leistungserbringung nutzt, muss er diese vollständig dokumentieren. Der Auftragnehmer ist verpflichtet, die Lizenz-Compliance sicherzustellen und alle Drittkomponenten in sein Schwachstellenmanagement einzubeziehen.

8.4. Der Auftragnehmer ist verpflichtet, alle von ihm bereitgestellten, betriebenen oder verantworteten Komponenten einschließlich Betriebssystem und Software regelmäßig auf bekannte Schwachstellen (z. B. CVEs) zu prüfen, diese nach einer einheitlichen und transparenten Bewertungsmethodik (z. B. CVSS) zu klassifizieren und eigenständig zu beheben. Die Behebung hat nach einem verbindlichen Zeitplan zu erfolgen, der sich an der Kritikalität der Schwachstelle orientiert. Liegt die Installation von Patches in der Verantwortung des Auftraggebers, muss der Auftragnehmer diesen unverzüglich informieren und die erforderlichen Updates bereitstellen.

8.5. Der Auftragnehmer ist verpflichtet, den Auftraggeber über erkannte Schwachstellen in bereitgestellten Produkten, die den Auftraggeber betreffen oder betreffen könnten, unverzüglich zu informieren. Hierbei sind die Schwachstellen nach einer transparenten Risikoklassifizierung einzuordnen.

8.6. Vor Bereitstellung an den Auftraggeber hat der Auftragnehmer sicherzustellen, dass die Software frei von Schadsoftware wie z.B. Viren, Würmer, Spionagesoftware ist. Die bereitgestellten Versionen sind vor Übergabe ausführlich zu testen. Es darf nur funktionsfähige und fehlerfreie Software als Aktualisierung zur Verfügung gestellt werden.

8.7. Ist die Leistungserbringung den Lieferantenkategorien „Integriert“ oder „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

8.7.1. Sofern und soweit der Auftragnehmer Testdaten für die Entwicklung von Anwendungen und Systemen verwendet, müssen diese sorgfältig und nachvollziehbar ausgewählt, geschützt und kontrolliert werden, d.h. es sollen anonymisierte bzw. pseudonymisierte Daten verwendet werden. Werden Echtdaten ver-wendet, bedarf dies einer vorherigen Zustimmung des Auftraggebers. Ferner müssen die Testsysteme denselben Sicherheitsanforderungen genügen wie die Produktivsysteme.

8.7.2. Um sicherzustellen, dass die Patches, Updates und Service Packs im Wirkbetrieb rückwirkungsfrei funktionieren, hat sie der Auftragnehmer vor Auslieferung auf Testsystemen einer Überprüfung zu unterziehen.

8.7.3. Der Auftragnehmer wird insbesondere alle technisch möglichen und im konkreten Fall zumutbaren Vorkehrungen (z.B. Pentests & Härtung) treffen, um die vertragsgegenständliche Software oder den Cloud-Service gegen bekannte Angriffstechniken (u.a. SQL-Injection, Cross-Site Scripting, Denial of Services Attacken, Brute-Force-Angriffe, Man-in-the-Middle-Attacken) zu schützen.

8.7.4. Der Auftragnehmer ist damit einverstanden, dass der Auftraggeber oder ein von ihm beauftragter Dritter regelmäßig Sicherheitsüberprüfungen, sogenannte Penetrationstests wie z.B. Scan- oder Intrusion Tests, in Bezug auf die IT-Systeme des Auftragnehmers durchführt die für die Leistungserbringung gegenüber dem Auftraggeber genutzt werden. Die Kosten für eine Sicherheitsüberprüfung trägt jede Partei für sich.

8.7.5. Der Auftragnehmer hat für ein reibungsloses Patch- und Änderungsmanagement zu sorgen, welches das zügige Einspielen von Patches, Updates und Service Packs ermöglicht. Daneben hat der Auftragnehmer ein Release Management zu etablieren und mit dem Auftraggeber abzustimmen.

8.8. Ist die Leistungserbringung der Lieferantenkategorie „Kritisch“ zuzuordnen, gelten die folgenden Regelungen zusätzlich:

8.8.1. Der Auftragnehmer verpflichtet sich, durch geeignete Maßnahmen (z.B. durch Hinterlegung des Source Codes sowie notwendiger, regelmäßig aktualisierter Daten/Informationen/Dokumentationen) unter Be-rücksichtigung der Vertraulichkeitsvereinbarungen und Datenschutzanforderungen nach diesem Vertrag sicherzustellen, dass der Betrieb des Auftraggebers im Falle einer Insolvenz des Auftragnehmers nicht wesentlich gestört wird und die vertragsgegenständlichen Leistungen durch den Auftraggeber selbst oder einen Dritten nahtlos weiter erbracht werden können.

9. Zusammenarbeit

9.1. Der Auftragnehmer muss sicherstellen, dass das eigene Netzwerk keinen unkontrollierten Zugriff Dritter auf das Netzwerk des Auftraggebers ermöglicht.

9.2. IT-Geräte des Auftragsnehmers, auf denen Daten des Auftraggebers gespeichert sind oder verarbeitet werden, müssen geeignet gegen Schadsoftware, Datenverlust, Datenverfälschung und Zugriff Dritter gesichert sein. Die direkte Verbindung von IT-Geräten des Auftragnehmers mit dem internen Netzwerk des Auftraggebers ist untersagt.

9.3. Mobile Datenträger (z.B. USB-Sticks und Festplatten) sowie mobile IT-Geräte mit Informationen oder Daten des Auftraggebers müssen verschlüsselt werden. In Kombination mit IT-Geräten des Auftraggebers dürfen nur mobile Datenträger verwendet werden, die auf Schadprogramme geprüft und durch den Auftraggeber freigegeben wurden.

9.4. Für den Remotezugriff auf Systeme des Auftraggebers muss der von dem Auftraggeber bereitgestellte Zugang genutzt werden.

9.5. Mitarbeiter des Auftragnehmers müssen sich bei ihrem Ansprechpartner vor Aufnahme der Aufgaben oder Tätigkeiten anmelden.

9.6. Die Einräumung des Remotezugriffs erfolgt ausschließlich zur Erfüllung der Vertragsleistungen des Auftragnehmers (insbesondere Wartung, Pflege, etc.) und ausschließlich zu den vertraglich konkretisierten Zwecken.

9.7. Erteilte Weisungen zu Art, Umfang und Ablauf der Nutzung der Zugriffsberechtigung sind durch den Auftragnehmer jederzeit einzuhalten.

9.8. Der Auftraggeber behält sich das Recht vor, sämtliche im Rahmen der vertraglich vereinbarten Tätigkeiten durch den Aufragnehmer erfolgenden Zugriffe – einschließlich, aber nicht beschränkt auf Fernwartungs-zugriffe, privilegierte Zugriffe über Privileged Access Management (PAM), Zugriffe im Rahmen von Client- oder Citrix-Umgebungen sowie systemseitige Erfassungen durch Sicherheits- und Monitoringlösungen (z. B. SIEM, Microsoft Defender oder vergleichbare Systeme) – aufzuzeichnen und zum Zwecke der IT-Sicherheit zu überwachen.

9.9. Die Auswertung der gemäß Ziffer 9.8 anfallenden Daten erfolgt ausschließlich zu folgenden Zwecken:

- Erkennung und Abwehr von Cyberangriffen,
- Nachvollziehbarkeit von administrativen Tätigkeiten, insbesondere im Rahmen von Fernwartung,
- Beweissicherung bei sicherheitsrelevanten Vorfällen (z. B. im Rahmen forensischer Analysen)

9.10. Die gemäß Ziffer 9.8 aufgezeichneten personenbezogenen Daten werden ausschließlich im Einklang mit den jeweils geltenden datenschutzrechtlichen Vorschriften, insbesondere der Datenschutz-Grundver-ordnung (DSGVO), verarbeitet.

9.11. Der Auftragnehmer muss die Vorgaben zur Klassifizierung von Informationen des Auftraggebers einhalten und seine Mitarbeiter dahingehend nachweislich unterweisen.

9.12. Alle Informationen des Auftraggebers sind entsprechend ihrer Vertraulichkeitsklasse zu schützen. Der Auftraggeber hat die nachfolgenden Vertraulichkeitsklassen festgelegt:

a) ÖFFENTLICH - nicht schutzwürdig
b) INTERN (Standard) - allgemeine dienstliche Informationen
c) VERTRAULICH - sensible Informationen
d) STRENG VERTRAULICH - besonders sensible Informationen

9.13. Alle Informationen des Auftraggebers sind bei Erstellung durch den Auftragnehmer in eine Vertraulichkeitsklasse einzuordnen und zu kennzeichnen. Die Informationsklassifizierung richtet sich dabei nach dem möglichen Einfluss auf die Geschäftsprozesse des Auftraggebers, der sich aus einer vorsätzlichen oder nicht beabsichtigten Bekanntgabe der Informationen ergeben kann.

9.14. Alle Informationen und Daten des Auftraggebers ab Vertraulichkeitsklasse „Intern“ dürfen nur nach Freigabe des Auftraggebers an berechtigte Dritte weitergegeben werden. Der gleichwertige Schutz bei allen Empfängern muss durch den Auftragnehmer sichergestellt werden.

9.15. Vertrauliche bzw. streng vertrauliche Informationen des Auftraggebers dürfen nur nach Freigabe des Auftraggebers an einen eingeschränkten Personenkreis (wenn „Kenntnis notwendig“) und unter weitergehenden Schutzmaßnahmen (u.a. Vertraulichkeitsvereinbarung, Verschlüsselung, Festlegung von befugten Empfängern, Regelung der Zulässigkeit der Herstellung von Kopien) an berechtigte Dritte weitergegeben werden.

9.16. Für den Umgang mit vertraulichen Informationen gelten die folgenden Rahmenbedingungen

- Kennzeichnung mit Vermerk „VERTRAULICH“ auch bei mündlicher Übertragung oder bei Ausdrucken
- Verschlossene Aufbewahrung und Weitergabe mit geeigneter Rechtevergabe

9.17. Für den Umgang mit streng vertraulichen Informationen gelten zusätzlich zu Ziffer 8.14 die folgenden Rahmenbedingungen:

- Vor der Weitergabe müssen die Empfänger der Information eine persönliche Erklärung über die Wahrung der Vertraulichkeit in angemessener Form abgeben.

9.18. Alle Informationen und Daten des Auftraggebers ab Vertraulichkeitsklasse „Intern“, sind bei der Übertragung über öffentliche Netze oder bei der Nutzung von mobilen Datenträgern zu verschlüsseln.

9.19. Sofern es durch den Auftraggeber nicht explizit beauftragt oder nachträglich genehmigt wurde, ist die Anfertigung von Foto-/Audio-/Videoaufnahmen ausgeschlossen. Dies betrifft vor allem aber nicht ausschließlich die folgenden Themenkomplexe:

a) physische Sicherheit:
   - Zutrittssteuerung und Sicherheitszonierungen der Anlagen und Gebäude, Lage- und Gebäudepläne
   - Sicherheitstechnik und Überwachungssysteme

b) Verfahrenstechnik:
   - Anlagentechnik
   - Schaltanlagen, Transformatoren, Frequenzumrichter, Netzersatzaggregate oder USV-Anlagen (Unterbrechungsfreie Stromversorgung) des Auftraggebers (sämtliche Anlagen der Strom- oder Notstromversorgung)
   - Messcontainer/Online-Überwachungen/Sensoren/Aktoren/Analyse-Equipment etc. des Auftraggebers (sämtliche Anlagen für Messungen/Analysen etc.)
   - Informationen zu Automatisierungsvorgängen

c) Assets und Dokumentationen:
   - Herstellerangaben, Produktangaben, Softwareversionen
   - Visualisierungen, technische Zeichnungen, Schaltbilder, Netzwerk-, Architektur- und Infrastrukturpläne, Handbücher und Anleitungen

d) Mitarbeitende:
   - Videokonferenzen, Bildschirmmitschnitte, Fotos oder sonstige Aufzeichnungen von Mitarbeitern des Auftraggebers und weiteren Lieferanten

9.20. Das Erstellen von Aufnahmen innerhalb von Videokonferenzen ist ausschließlich zulässig, wenn:

- dies vorab ausdrücklich vom Auftraggeber genehmigt wurde, und
- alle beteiligten Teilnehmenden vor Beginn der Aufzeichnung eindeutig informiert wurden und ihr Ein-verständnis erklärt haben.

9.21. Soweit Mitarbeiter des Auftragnehmers Zutrittsberechtigungen erhalten, sind diese nur im Rahmen der vereinbarten Aufgaben oder Tätigkeiten persönlich zu verwenden. Die Berechtigung darf nicht übertragen werden. Mitarbeiter des Auftragnehmers müssen sich bei ihrem Ansprechpartner bei Aufnahme der Aufgaben oder Tätigkeiten anmelden. Der Zutritt darf ausschließlich zu den durch den Auftraggeber freigegebenen Bereichen erfolgen. Der Auftraggeber behält sich das Recht vor, die Tätigkeiten des Auftragnehmers Vor-Ort, insbesondere in sensiblen Bereichen, durch eigene Mitarbeiter zu überwachen.

10. Beendigung der Leistung

10.1. Im Falle der Beendigung der Leistung, sind Informationen und Unterlagen, die auf Wunsch des Auftrag-gebers nicht an den Auftraggeber ausgehändigt werden, vorbehaltlich gesetzlicher Aufbewahrungsfristen abschließend zu löschen bzw. zu vernichten. Eine schriftliche Bestätigung der Löschung/ der Vernichtung ist dem Auftraggeber auf dessen Nachfrage auszuhändigen.

10.2. Der Auftragnehmer sorgt ferner dafür, dass sämtliche Kenntnisse und Informationen, die im Rahmen der Vertragserfüllung wichtig für den laufenden Geschäftsbetrieb des Auftraggebers sind, dokumentiert und in einer mit dem Auftraggeber abgestimmten Form an diesen übergeben werden. Die Übergabe hat kontinuierlich innerhalb der Leistungsbeziehung sowie abschließend mit Beendigung der Leistung zu erfolgen.

10.3. Sobald ein Mitarbeiter des Auftragnehmers nicht mehr zum Zwecke der Erbringung von Leistungen für den Auftraggeber eingesetzt wird oder die Zusammenarbeit insgesamt abgeschlossen ist, hat der Auf-tragnehmer dafür Sorge zu tragen, dass alle relevanten Zugänge und Berechtigungen entzogen werden und dass der jeweilige Mitarbeiter alle im Rahmen und für Zwecke der Leistungserbringung erhaltenen Gegenstände, Informationen, Unterlagen oder ähnlichen Werte („Assets“) des Auftraggebers ordnungsgemäß an diesen zurückzugibt. Dies sind unter anderem:

- Organisationseigene Geräte (Computer, Mobiltelefon, Tablet),
- Dokumente des Auftraggebers,
- Firmenausweis, Zugangskarten,
- Software und Softwarehandbücher,
- auf elektronischen Medien gespeicherte Informationen,
- sonstige Informationen, an denen kein Zurückbehaltungsrecht besteht,
- sonstige übergebene Unternehmenswerte.

10.4. Ist die Leistungserbringung den Lieferantenkategorien „Integriert“ oder „Kritisch“ zuzuordnen, gelten folgende Regelungen ergänzend:

10.4.1. Spätestens drei Monate vor Ende der Leistungserbringung beginnt die beidseitige Abstimmung der bevor-stehenden Transition der Systeme und Leistungen. Im Rahmen der Abstimmung werden mindestens die folgenden Themen betrachtet und schriftlich vereinbart:

- Vorgehen der Transition inkl. Terminplanung, Kommunikationsplanung und Stakeholderbetrachtung
- Hauptansprechpartner auf Auftraggeber- und Auftragnehmerseite
- Beteiligte inkl. deren Aufgaben
- Datenformate für die Übergabe der Daten (nicht-proprietär, weiterverwendbar)
- Datenformate der sonstigen Dokumente und Dokumentationen
- Zeitpunkt der Unzugänglichmachung der Daten
- Ggf. gesetzlich Aufbewahrungsfrist und/oder Löschung inkl. Nachweis
- Verantwortlichkeiten und Mitwirkungspflichten im Rahmen der Datenbereitstellung
- Datentransferwege / Technologien

- Vorgehen des KnowHow-Transfers
- ggf. Planung eines Cut-Over, falls erforderlich (Modell, Zeitpunkte, Betriebsübergang)
- ggf. Lizenz- und Rechteübertragung für Software und Dokumentationen

10.4.2. Nach Festlegung, Detaillierung und Planung der genannten Inhalte erfolgt die Transition. Die Beteiligten stimmen sich innerhalb der Transition regelmäßig über den Status und die Aktivitäten ab.

10.4.3. Der Auftragnehmer verpflichtet sich zur zielführenden und kooperativen Zusammenarbeit mit dem Auftraggeber und einem eventuellen neuen Dienstleister. Alle Beteiligten stellen für den Übergabeprozess entsprechend qualifiziertes Personal bereit, um einen stabilen, sicheren und geordneten Betriebsüber-gang und Weiterbetrieb zu gewährleisten.

11. Kontaktdaten

Folgenden Parteien sind im Falle sind im Falle relevanter Ereignisse zu kontaktieren. Zusätzlich dient auch der innerhalb der Beauftragung festgelegte fachliche Ansprechpartner als Kontakt.

Informationssicherheitskoordinator	Datenschutzbeauftragter
Pfotenhauerstraße 46, 01307 Dresden Telefon: +49 351 4455 265 E-Mail: t.b.d.	TÜV SÜD Akademie GmbH E-Mail: datenschutz@twd-dresden.de

12. Glossar

Begriff	Erläuterung
Vertragsleistung	Bezeichnet im Rahmen dieses Dokumentes die gemäß Vertrag durch den Lieferanten (Auftragnehmer) zu erbringenden Leistungen. Sie umfasst Art, Umfang, Qualität, Zeitrahmen sowie besondere Anforderungen der Leistungserbringung.
Warenklassen	Bezeichnet im Rahmen dieses Dokumentes die Zusammenfassung der unterschiedlichen Vertrags-leistungen zu bekannten Klassen wie bspw. Software, Hardware, Dienstleistung und Cloud-Services.
Software	Software bezeichnet im Rahmen dieses Dokumentes alle Computerprogramme die auf einem Computer, Server, einer VM oder einem anderen Gerät mit elektronischen Bestandteilen ausgeführt werden können sowie die dazu gehörenden Dokumentationen.
Individualsoftware	Individualsoftware bezeichnet im Rahmen dieses Dokumentes Software, die speziell für den Auftraggeber, mit dem Auftraggeber oder vom Auftraggeber selbst programmiert, entwickelt oder angepasst wurde.
Standardsoftware	Standardsoftware bezeichnet im Rahmen dieses Dokumentes Software, die nicht speziell für den Auftraggeber entwickelt, aber eventuell im Einzelfall in Teilen im Quelltext oder mittels Customizings für den Auftraggeber angepasst wurde.
Hardware	Hardware bezeichnet im Rahmen dieses Dokumentes die physischen Komponenten (die elektronischen und mechanischen Bestandteile) eines datenverarbeitenden Systems.
Dienstleistung	Dienstleistung bezeichnet im Rahmen dieses Dokumentes Leistungen, die die Planung, Bereitstellung, Wartung und Unterstützung von IT-Systemen und -Infrastrukturen betreffen. Dies umfasst insbesondere die Beratung, Softwareentwicklung oder auch die Unterstützung im laufenden Betrieb sowie den Support. Dabei ist die Abrechnungsart unerheblich (z.B. Pauschalpreis oder Abrechnung nach Aufwand).
Cloud-Service	Bezeichnet im Rahmen dieses Dokuments einen durch einen externen Anbieter bereitgestellten IT-Dienst (z. B. SaaS, PaaS oder IaaS), der nicht im eigenen Rechenzentrum betrieben wird und dessen Nutzung typischerweise über netzwerkbasierte Zugänge erfolgt. Dies kann über das öffentliche Internet oder über gesicherte Verbindungen (z. B. VPN, MPLS) geschehen.
Lieferantenkategorie Allgemein	Lieferung von Hard- und Software sowie Cloud-Services Wartungs- oder Supportverträge nur auf Basis von Beistellung/Lieferung/Austausch keine Systembindung, Installation oder Support Leistungen ohne Systemzugriff aber mit Zugang zu geringkritischen personenbezogenen Daten (z.B. Name, Kontakt) Informationen Klassifizierung „Öffentlich"
Lieferantenkategorie Integriert	Leistungen der Lieferantenkategorie "Allgemein" UND Wartungs- oder Support mit Zugriff auf Informationen ab der Klassifizierung "INTERN" Erbringung von Leistungen mit Zugriff auf Systeme/RZ-Hardware und auf Informationen ab der Klassifizierung "INTERN"
Lieferantenkategorie Kritisch	Leistungen der Kategorie "Integriert" UND

	direkte oder indirekte Unterstützung von geschäfts- und/oder erfolgskritischen Prozessen

Mitgeltende Dokumente

Entsprechend der ISMS-Dokumentenpyramide müssen nachfolgende Dokumente nach ISO 27001:2022 beigebracht werden:

Dokument	Ablageort
Leitlinie	Klicken oder tippen Sie hier, um Text einzugeben.
Konzept/Richtlinie	Klicken oder tippen Sie hier, um Text einzugeben.
Arbeitsanweisungen	Klicken oder tippen Sie hier, um Text einzugeben.
Dokumentationen	Klicken oder tippen Sie hier, um Text einzugeben.

Diese Dokumente müssen der Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen des BSI entsprechen.

Anhänge

Lfd. Nr.	Dokument	Ablageort
1		Klicken oder tippen Sie hier, um Text einzugeben.
2		Klicken oder tippen Sie hier, um Text einzugeben.
3		Klicken oder tippen Sie hier, um Text einzugeben.
4		Klicken oder tippen Sie hier, um Text einzugeben.

Freigabeerklärung - Unterschriftenblatt

Dokumententitel: Vorgaben zur Informationssicherheit in Lieferantenbeziehungen

Dokumenten-ID: Dokument4 Version: 1.0 **Ersetzt Version:** _____

Status: ☐ Neuaufnahme ☐ Änderung ☐ Außer Kraft gesetzt

Freigabeerklärung:
Mit ihrer Unterschrift bestätigen die nachfolgend genannten Rollen, dass das Dokument inhaltlich geprüft, abgestimmt und zur verbindlichen Nutzung freigegeben wurde. Das Dokument tritt zum im Dokument angegebenen Datum in Kraft.

Hinweis zur Verwendung (intern):
Dieses Blatt dient der formalen Dokumentenlenkung nach ISO-27001-Best-Practice. Unterschriften können händisch erfolgen oder im digitalen Freigabeworkflow (z. B. mit **qeS - qualifizierter elektronischer Signatur**).

Rolle/Funktion	Name	Abteilung	Datum	Unterschrift
Wählen Sie ein Element aus.	Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie, um ein Datum einzugeben.	