

Vertragsanhang

IT- und Informationssicherheitsanforderungen

Zusammenfassung

Dieses Dokument definiert grundsätzliche Sicherheitsanforderungen (Mindestkriterien) an Lieferanten von Produkten und Dienstleistungen der Stromnetz-Berlin (SNB).

Inhalt

1	Allgemeine Vertragsbestimmungen	4
1.1	Vertragsparteien	4
1.2	Vertragsgegenstand	4
1.3	Anwendungsbereich	4
1.4	Kontaktperson für die IT- und Informationssicherheit	5
1.5	Erreichbarkeiten und Meldepflichten	5
2	Einstufung der Sicherheitsanforderungen	6
3	Anforderungen an die Informationssicherheit	7
3.1	Allgemeine Verantwortlichkeiten des Auftragnehmers	7
3.1.1	Aufrechterhaltung der vertraglichen IT- und Informationssicherheitsanforderungen	7
3.1.2	Einsatz von Unterauftragnehmern	7
3.1.3	Nachweisverpflichtung/Vor-Ort-Kontrolle	7
3.2	Organisatorische Anforderungen	9
3.2.1	Betrieb eines Informationssicherheitsmanagementsystems (ISMS)	9
3.2.2	Informationsklassifizierung und -handhabung	9
3.2.3	Asset-Management	9
3.2.4	Zugriffsschutz und Berechtigungsvergabe	9
3.2.5	Nutzung von Cloud-Diensten	10
3.3	Personelle Anforderungen	11
3.3.1	Informationssicherheits-Organisation	11
3.3.2	Personalsicherheit	11
3.3.3	Informationssicherheit bei Remote-Arbeit	11
3.4	Physische Anforderungen	12
3.4.1	Standort- und Datensicherheit	12
3.4.2	Zugangskontrolle und -beschränkungen	12
3.4.3	Versand von Speichermedien	12
3.5	Technologische Anforderungen	13
3.5.1	Sicherheit der Endgeräte	13
3.5.2	Sichere Authentifizierung und Autorisierung	13
3.5.3	Schutz vor Schadsoftware	13
3.5.4	Schwachstellenmanagement	13
3.5.5	Löschung von Auftraggeberinformationen	14
3.5.6	Datensicherung und -archivierung	14
3.5.7	Protokollierung und Überwachung (Angriffserkennung)	14
3.5.8	Systemhärtung	14
3.5.9	IT-Sicherheitsarchitektur	14
3.5.10	Nutzung von kryptographischen Verfahren	15
4	Kenntnisnahme/Bestätigung	15
5	Anhang	16

5.1	Anhang I: Glossar	16
5.2	Anhang II: Berichte zur Informationssicherheit	17

1 Allgemeine Vertragsbestimmungen

1.1 Vertragsparteien

Dieses Dokument regelt die künftige Zusammenarbeit im Themenfeld „IT- und Informationssicherheit“ zwischen

dem Auftraggeber,

Stromnetz Berlin GmbH

und dem Auftragnehmer,

[Name des zukünftigen Auftragnehmers]

für den Einsatz im bzw. die Anwendung durch den Auftraggeber zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus.

1.2 Vertragsgegenstand

Dieser Vertragsanhang regelt die Umsetzung von IT- und Informationssicherheitsanforderungen durch den Auftragnehmer. Der Vertragsanhang bezieht sich auf den Leistungsvertrag mit folgenden Hauptkomponenten:

- Kreative Full-Service-Agenturen für die Stromnetz Berlin GmbH

Im Rahmen dieses Vertrags erhält der Auftragnehmer Zugang zu wichtigen, für die IT- und Informationssicherheit relevanten geschäftlichen Informationen des Auftraggebers, an denen ein Geheimhaltungsinteresse besteht. Diese Liste ist nicht abschließend. Diese Informationen werden nachfolgend als "Auftraggeberinformationen" bezeichnet. Im Einzelnen umfasst dies folgende Informationen: Inhalts- und Kommunikationsdaten, Kampagneninhalte, unternehmensinterne Informationen (beispielsweise Hintergrundinformationen, personenbezogene Daten je nach Kontext, Bilddaten, Mediendaten, Vertrags- und Abrechnungsdaten, Zugangsdaten, Präsentationen und Konzepte

Die Verpflichtung des Auftragnehmers zum Schutz der Auftraggeberinformationen bestehen unabhängig davon, wer diese Informationen erstellt hat und unabhängig von der Form der Übermittlung.

1.3 Anwendungsbereich

Sofern nicht nachfolgend abweichend geregelt, gelten sämtliche Regelungen dieser IT- und Informationssicherheitsanforderungen nur für jene Assets (siehe Anhang I: Glossar), die im Rahmen der Leistungserbringung relevant sind.

1.4 Kontaktperson für die IT- und Informationssicherheit

Der Auftragnehmer und Auftraggeber benennen jeweils eine Person als Kontaktperson für die IT- und Informationssicherheit. Diese Rolle darf auch mit anderen Rollen (z. B. Serviceverantwortliche, Accountmanager) kombiniert werden. Sie dient als Erstkontakt im Falle eines sicherheitsrelevanten Ereignisses und bei generellen Fragen zur IT- und Informationssicherheit.

Kontaktperson beim Auftraggeber:

Randy Glaß, randy.glass@stromnetz-berlin.de

Kontaktperson beim Auftragnehmer:

Herr/Frau Mustermann, E-Mail

1.5 Erreichbarkeiten und Meldepflichten

Der Auftragnehmer verpflichtet sich, den Auftraggeber über alle sicherheitsrelevanten Ereignisse (SRE) und Sicherheitsvorfälle (siehe Anhang I: Glossar) zu informieren, die im Umfeld des Auftragnehmers auftreten oder Auswirkungen auf seine unmittelbare Leistungserbringung haben. Die Meldung hat, sofern der Sicherheitsvorfall relevant für die Auftraggeberinformationen ist, unverzüglich zu erfolgen.

	Schutzbedarf	
	Normal	Hoch/sehr hoch
Meldung eines Sicherheitsvorfalls	unverzüglich	unverzüglich
Meldung eines sicherheitsrelevanten Ereignisses (SRE)	72 Stunden nach Entdeckung des Vorfalls	24 Stunden nach Entdeckung des Vorfalls
Schwachstellenmeldung	72 Stunden nach Entdeckung	24 Stunden nach Entdeckung

Tabelle 1: Erreichbarkeiten und Meldepflichten

Der Auftragnehmer verpflichtet sich, alle Informationen, die zur Bewältigung des Vorfalls beitragen können, zur Verfügung zu stellen. Als zentrale Meldestelle für sicherheitsrelevante Ereignisse und Sicherheitsvorfälle gilt das

Security Operation Center (SOC) der SNB

E-Mail: soc@stromnetz-berlin.de

Notrufnummer: +49 30 49202-4444

Der Auftragnehmer hat in solchen Fällen neben Zwischeninformationen einen finalen Abschlussbericht zu erstellen. Der Auftraggeber verpflichtet sich, alle bereitgestellten Informationen und Berichte über Sicherheitsereignisse und -vorfälle vertraulich zu behandeln.

2 Einstufung der Sicherheitsanforderungen

Im Rahmen der Zusammenarbeit zwischen dem Auftragnehmer und Auftraggeber wird folgende Leistung erbracht. Unter anderen werden folgende Informations- und Datenkategorien¹ verarbeitet:

Kriterium	Beschreibung
Beschreibung der Leistung	<ul style="list-style-type: none"> Bereitstellung von Kommunikationsagenturleistungen
Verarbeitete Daten	<ul style="list-style-type: none"> Kommunikationsdaten Personenbezogene Daten je nach Kontext Bild-, Video- und Mediendaten (Texte, Fotos, Grafiken, Layouts)

Tabelle 2: Leistungsbeschreibung und Datenkategorien

Die Sicherheitsanforderungen betreffen die Bereiche Vertraulichkeit, Integrität und Verfügbarkeit und können mit „normal“, „hoch“ und „sehr hoch“ bewertet werden. Für die im Vertragsgegenstand definierte Leistung werden folgende Schutzbedarfe festgelegt:

Schutzziel	Schutzbedarf
Vertraulichkeit	<ul style="list-style-type: none"> Hoch
Verfügbarkeit¹	<ul style="list-style-type: none"> Normal
Integrität²	<ul style="list-style-type: none"> Hoch

Tabelle 3: Schutzbedarfsfeststellung

- 1 Verfügbarkeit bedeutet, dass jederzeit zuverlässig auf Dateien zugegriffen werden kann, wenn sie benötigt werden.
- 2 Integrität bedeutet, dass Daten unverändert, vollständig und korrekt bleiben und nicht unbefugt manipuliert werden. Wenn die Integrität gestört ist, können Daten unbemerkt verändert werden, sodass zum Beispiel ein manipuliertes Protokoll falsche Entscheidungen auslöst.

¹ Die Auflistung der voraussichtlich verarbeiteten Daten erhebt keinen Anspruch auf Vollständigkeit.

3 Anforderungen an die Informationssicherheit

Die folgenden Sicherheitsanforderungen konkretisieren die vertraglichen Rechte und Pflichten zwischen dem Auftragnehmer und dem Auftraggeber im Rahmen der Leistungserbringung des Auftragnehmers. Sie konkretisieren Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik für das ISMS der SNB.²

3.1 Allgemeine Verantwortlichkeiten des Auftragnehmers

3.1.1 Aufrechterhaltung der vertraglichen IT- und Informationssicherheitsanforderungen

- (1) Der Auftragnehmer verpflichtet sich, die durch den Auftraggeber definierten Anforderungen an die IT- und Informationssicherheit einzuhalten.
- (2) Der Auftragnehmer ist dafür verantwortlich, während des gesamten Vertragszeitraums ein angemessenes Schutzniveau für die Auftraggeberinformationen aufrechtzuerhalten. Dies beinhaltet insbesondere, dass die Informationen:
 - nur verwendet werden, wenn und soweit dies zur Leistungserbringung erforderlich ist,
 - nur Personen zugänglich gemacht werden dürfen, die zur Einhaltung der Vertraulichkeit verpflichtet sind und die die Informationen im Rahmen der Leistungserbringung benötigen (berechtigte Personen),
 - nicht länger als erforderlich aufbewahrt werden,
 - durch Informationssicherheitsmaßnahmen vor Offenlegung/Zugänglichmachung durch unberechtigte Personen geschützt werden.
- (3) Der Auftragnehmer hat dem Auftraggeber Änderungen seiner Assets, die geeignet sind, die Erfüllbarkeit der vorliegenden IT- und Informationssicherheitsanforderungen zu beeinträchtigen, unverzüglich mitzuteilen und die Vereinbarkeit mit den Anforderungen dieses Vertragsanhangs zu erläutern und ggf. nachzuweisen.

3.1.2 Einsatz von Unterauftragnehmern

- (1) Im Falle des Einsatzes von Unterauftragnehmern hat der Auftragnehmer dafür zu sorgen, dass die für den jeweiligen Leistungsbestandteil relevanten Verpflichtungen dieser IT- und Informationssicherheitsanforderungen eingehalten werden.
- (2) Der Auftragnehmer hat die Einhaltung der Verpflichtungen schriftlich mit jedem Unterauftragnehmer zu vereinbaren und deren Einhaltung zu überwachen. Ungeachtet dessen bleibt der Auftragnehmer gegenüber dem Auftraggeber vollumfänglich zur Leistungserbringung verpflichtet. Er steht gegenüber dem Auftraggeber allein für die ordnungsgemäße Erbringung der geschuldeten Leistungen ein.
- (3) Eine Übertragung von Leistungsbestandteilen auf Unterauftragnehmer ohne Zustimmung des Auftraggebers ist unzulässig.

3.1.3 Nachweisverpflichtung/Vor-Ort-Kontrolle

- (1) Der Auftragnehmer ist verpflichtet, die Einhaltung der in diesem Vertragsanhang festgelegten Anforderungen gegenüber dem Auftraggeber nachzuweisen. Der Auftraggeber ist zu diesem Zweck berechtigt, eine strukturierte Vor-Ort-Kontrolle von Informationen,

² Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen (Version 3.0, Stand November 2021)

Prozessen, Systemen, Kontroll- und Sicherheitsmaßnahmen oder Organisationsstrukturen bei dem Auftragnehmer durchzuführen (z. B. im Rahmen eines Audits/Assessments) bzw. durch einen akkreditierten ISO27001 Auditor durchführen zu lassen. Der Auftragnehmer ist verpflichtet, bei der Durchführung der Kontrolle zu unterstützen, insbesondere durch Vorlage bzw. Zugänglichmachung der erforderlichen Informationen und Nachweise.

- (4) Der Auftraggeber wird einen Bericht über die Ergebnisse der Vor-Ort-Kontrolle verfassen. Sofern hierfür Nachweise und oder Befunde erforderlich sind, ist der Auftragnehmer verpflichtet, diese innerhalb von vier Wochen nach Aufforderung an den Auftraggeber zu übermitteln.
- (5) Falls während der Überprüfung ein Verstoß gegen eine in diesem Vertragsanhang festgelegte Anforderung festgestellt wird, hat der Auftragnehmer unverzüglich Maßnahmen zur Beseitigung des Verstoßes zu ergreifen. Sofern der Verstoß schwerwiegend ist, darf der Auftraggeber Vorgaben zur Beseitigung machen, die der Auftragnehmer umzusetzen hat, sofern dies für ihn nicht unzumutbar ist; der Auftraggeber wird sich vor der Festlegung einer Vorgabe mit dem Auftragnehmer abstimmen.

3.2 Organisatorische Anforderungen

3.2.1 Informationsklassifizierung und -handhabung

- (1) Auftraggeberinformationen, die beim Auftragnehmer gespeichert sind, müssen im Besitz des Auftragnehmers verbleiben. Die Weitergabe von Auftraggeberinformationen darf nur nach dokumentierter Freigabe (Datenfreigabeformular) durch den Auftraggeber erfolgen.
- (2) Der Auftragnehmer verpflichtet sich, die Vorgaben der Informationsklassifizierung (siehe Anhang III: Mitgeltende Dokumente) zu beachten und die Auftraggeberinformationen nach diesem Klassifizierungsschema zu behandeln.

3.2.2 Asset-Management

- (1) Der Auftragnehmer verpflichtet sich, Assets (siehe Anhang I: Glossar), die für die Leistungserbringung relevant sind, zu identifizieren und zu dokumentieren; die Dokumentation ist fortlaufend zu aktualisieren
- (2) Der Auftragnehmer ist verpflichtet, unter Berücksichtigung von Risiken des unbefugten Zugriffs, Beschädigung oder Verlusts, angemessene Schutzmaßnahmen für die Assets mit dem Ziel zu implementieren, den Eintritt der Risiken zu verhindern. Die Schutzmaßnahmen sind über den gesamten Zeitraum aufrechtzuerhalten und fortlaufend zu überprüfen und ggf. zu aktualisieren.

3.2.3 Zugriffsschutz und Berechtigungsvergabe

- (1) Der Auftragnehmer ist verpflichtet, dokumentierte Prozesse und Kontrollen zum Zugriffsschutz und zur Berechtigungsvergabe (inkl. Freigabeprozesse für Berechtigungen auf Systemen und Informationen, Verfahren zur zeitnahen Löschung von Zugriffsrechten bei Austritt oder Abteilungswechsel) zu implementieren.
- (2) Der Auftragnehmer ist verpflichtet, den Zugriffsschutz nachfolgenden Grundsätzen zu gestalten:
 - Need-to-know: Zugriffe dürfen nur auf Basis der betrieblichen Notwendigkeit vergeben werden.
 - Least Privilege: Benutzer dürfen nur die minimalen Zugriffsrechte (z. B. lesen, ändern, löschen) erhalten, die für die Ausführung der betrieblichen Aufgaben erforderlich sind.
 - Segregation of duties: Kritische Aufgaben (z. B. administrative Berechtigungen) müssen so verteilt werden, dass keine Einzelperson die volle Kontrolle über alle Aktionen eines Prozesses erhält.
- (3) Der Auftragnehmer ist verpflichtet, für kritische Systeme³ (z. B. Systeme mit hohem Schutzbedarf; Systeme, die im Internet exponiert sind) eine Mehr-Faktor-Authentifizierung (MFA) zu implementieren. Nicht mehr benötigte Zugriffsrechte sind unverzüglich zu entziehen.
- (4) Der Auftragnehmer verpflichtet sich, auf Anfrage des Auftraggebers eine aktuelle Liste des Personals zur Verfügung zu stellen, das Zugriff auf Auftraggeberinformationen hat.

³ Eine Begriffsdefinition befindet sich im Glossar.

3.2.4 Nutzung von Cloud-Diensten

- (1) Sofern der Auftragnehmer im Rahmen der Leistungserbringung eine Cloud-Lösung einsetzt, stellt er sicher, dass die Lösung einem allgemein bekannten Cloud-Sicherheitsstandard (z. B. Kriterienkatalog Cloud Computing C5, Cloud Controls Matrix des CSA) entspricht. Die Verpflichtung des Satz 1 gilt ebenfalls, sofern der Auftragnehmer die Cloud-Lösung eines Dritten (Cloud-Dienstleister) im Rahmen der Leistungserbringung nutzt.
- (2) Der Auftragnehmer verpflichtet sich ferner, für den Fall, dass im Rahmen der Leistungserbringung die Cloud-Lösung eines Dritten von ihm genutzt wird, die Einhaltung der in diesem Dokument festgelegten Informationssicherheitsanforderungen mit dem Dritten zu vereinbaren.

3.3 Personelle Anforderungen

3.3.1 Informationssicherheits-Organisation

- (1) Der Auftragnehmer verpflichtet sich, dass innerhalb der Organisation eine Funktionstrennung (z. B. zwischen Administration und Revision) eingehalten wird, um mögliche Interessenskonflikte zu vermeiden.

3.3.2 Personalsicherheit

- (1) Der Auftragnehmer ist verpflichtet, neue Mitarbeiter im Zuge des Einstellungsprozesses zur Einhaltung geltender Regelwerke⁴ der Informationssicherheit zu verpflichten.
- (2) Für die Mitarbeiter des Auftragnehmers werden periodisch Security-Awareness-Trainings durchgeführt. Die Security-Awareness-Trainings sollen mindestens folgendes umfassen:
 - a. Erkennung relevanter Bedrohungen wie Phishing und Malware
 - b. Verhaltensweisen bei Sicherheitsvorfällen und Meldungen
 - c. Sichere Arbeitspraktiken und Passwortmanagement

Die Inhalte der Schulungen werden entsprechend den aktuellen Bedrohungslagen und Angriffsvektoren aktualisiert.

- (3) Der Auftragnehmer verpflichtet sich, eine geeignete Meldestelle bzw. einen Meldeweg zur Meldung von Informationssicherheitsereignissen für das Personal einzurichten.

3.3.3 Informationssicherheit bei Remote-Arbeit

- (1) Der Auftragnehmer verpflichtet sich, dass die Informationssicherheit auch bei Remote-Arbeit (z. B. bei Arbeit im Home-Office) gewährleistet ist. Hierzu werden entsprechende Sicherheitsvorgaben für die Remote-Arbeit erstellt und an die betroffenen Mitarbeiter kommuniziert. Die Vorgaben an die Remote-Arbeit sollten folgende Mindestinhalte aufweisen:
 - a. Zugangsbeschränkungen und Authentifizierungsmaßnahmen für den Zugang auf das Unternehmensnetzwerk des Auftragnehmers,
 - b. Verfahren zum Umgang mit sensiblen Informationen außerhalb des Unternehmensnetzwerks (inkl. sicherer Dateübertragung),
 - c. Sicherheitsbewusstsein bei der Remote-Arbeit
- (2) Der Auftragnehmer gewährleistet, dass Remote-Arbeit nur über verschlüsselte Verbindungen (z. B. Virtuelle Private Netzwerke) mit den internen Systemen erfolgt.
- (3) Der Auftragnehmer verpflichtet sich, eine starke Authentifizierung, einschließlich Multi-Faktor-Authentifizierung für Mitarbeiter bei Remote-Arbeit umzusetzen.
- (4) Der Auftragnehmer legt Mindestsicherheitsanforderungen für die Geräte fest, die zur Durchführung von Remote-Arbeit verwendet werden dürfen. Diese Anforderungen müssen mindestens die Anforderungen des Abschnitts 3.5.1 berücksichtigen.

⁴ Interne Richtlinien des Auftragnehmers sowie auf diesen Vertrag anwendbare gesetzliche und vertragliche Verpflichtungen

3.4 Physische Anforderungen

3.4.1 Standort- und Datensicherheit

- (1) Eine Verarbeitung von Auftraggeberinformationen (einschließlich Speicherung von Daten; Zugriff auf Daten) durch den Auftragnehmer ist örtlich nur zulässig, (i) in einem Mitgliedstaat der Europäischen Union bzw. in einem Mitgliedstaat des Europäischen Wirtschaftsraums oder (ii) in einem Drittland, dass der Auftraggeber zur Verarbeitung von Daten vorher schriftlich freigegeben hat.
- (2) Der Auftragnehmer verpflichtet sich, eine Übersicht über alle Standorte, an denen Auftraggeberinformationen verarbeitet oder gespeichert werden, zu erstellen, fortlaufend zu aktualisieren und auf Anforderung an den Auftraggeber zu übermitteln. Diese Standorte umfassen insbesondere Rechenzentren, Standorte mit Zugriff auf oder Kopien von Auftraggeberinformationen sowie Wartungsbereiche. Geplante und ungeplante Änderungen der Standorte sind dem Auftraggeber unverzüglich mitzuteilen.

3.4.2 Zugangskontrolle und -beschränkungen

- (1) Der Auftragnehmer verpflichtet sich, den Zugang zu schutzbedürftigen Gebäudeteilen und Räumen zu regeln und zu kontrollieren. Die Regelungen zur Zugangskontrolle werden durch den Auftragnehmer in einem Konzept definiert. Alle erteilten Berechtigungen müssen auf ein Mindestmaß reduziert und dokumentiert werden.

3.4.3 Versand von Speichermedien

- (1) Der Auftragnehmer verpflichtet sich zu einem sicheren Versand aller Speichermedien, die Auftraggeberinformationen enthalten. Folgende Sicherheitsmaßnahmen sind beim Versand von Speichermedien nach Satz 1 (einschließlich solcher in Geräten) mindestens anzuwenden (kumulativ):
 - a. Die Speichermedien und/oder Geräte dürfen während des Versands nicht unverschlüsselt oder ungeschützt zugänglich sein.
 - b. Die Speichermedien und/oder Geräte müssen in verschlossenen und versiegelten Behältern versandt werden.
 - c. Der Transport muss anhand von Protokollen und Trackingverfahren lückenlos dokumentiert werden.
- (2) Bei Verlust oder Diebstahl von Speichermedien während des Versands hat der Auftragnehmer dies unverzüglich dem Auftraggeber zu melden und Maßnahmen zur Aufklärung des Vorfalls einzuleiten.
- (3) Sofern der Auftragnehmer gegen die Vorgaben des Abs. 1 verstößt, ist er dazu verpflichtet, dem Auftraggeber die Kosten einer forensischen Untersuchung des Speichermediums und/oder Gerätes zu erstatten, die der Aufklärung dient, ob Dritte Zugriff auf das Gerät und/oder das Speichergerät hatten. Lässt sich ein möglicher Zugriff von Dritten nicht mit hinreichender Wahrscheinlichkeit ausschließen, hat der Auftragnehmer überdies die Kosten für die Beschaffung eines vergleichbaren Speichermediums und/oder Neugerätes zu tragen einschließlich aller damit zusammenhängenden Kosten.

3.5 Technologische Anforderungen

3.5.1 Sicherheit der Endgeräte

- (1) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung von Auftraggeberinformationen auf eigenen Endgeräten folgende Sicherheitsanforderungen umzusetzen:
 - a. die Konfiguration und Härtung der betroffenen Endgeräte erfolgt anhand eines im Bereich IT-Sicherheit allgemein bekannten Standards (z. B. Härtungsempfehlungen des Herstellers, IT-Grundschutz-Standards, CIS-Benchmarks),
 - b. die Sicherheitseinstellungen werden regelmäßig überprüft und
 - c. die Endgeräte sind mit Sicherheitslösungen zum Schutz vor Schadsoftware (z. B. Antivirensoftware, Endpoint-Protection) ausgestattet und werden regelmäßig auf Schadsoftware überprüft.

3.5.2 Sichere Authentifizierung und Autorisierung

- (1) Der Auftragnehmer verpflichtet sich, administrative Zugänge oder Netzwerk-Ports, die aus externen bzw. öffentlichen Netzwerken erreichbar sind, entweder zu deaktivieren oder angemessen abzusichern (z. B. durch die Implementierung von Multi-Faktor-Authentifizierung). Netzwerkverbindungen, Systemzugriffe und administrative Tätigkeiten werden zur Nachvollziehbarkeit von Angriffen oder Fehlbedienungen protokolliert.
- (2) Die vom Auftragnehmer bereitgestellten Dienste und/oder Schnittstellen müssen die Einhaltung der geltenden Mindestanforderungen des BSI an die Passwortkomplexität durch eine konfigurierbare Passwortrichtlinie sicherstellen.⁵
- (3) Der Auftragnehmer sorgt dafür, dass Passwörter und sonstige Authentifizierungsgeheimnisse nicht unverschlüsselt gespeichert oder übertragen werden.

3.5.3 Schutz vor Schadsoftware

- (1) Der Auftragnehmer stellt sicher, dass alle Endpunkte eines Netzwerks (Geräte, die sich am Ende eines Kommunikationskanals mit dem Netzwerk befinden und dazu geeignet sind, Daten mit dem Netzwerk auszutauschen, insbesondere Clients, Server und mobile Geräte) mit aktuellen Antivirus- und Anti-Malware-Lösungen ausgestattet sind.
- (2) Der Auftragnehmer sorgt dafür, dass die Mitarbeiter des Auftragnehmers sensibilisiert werden, um Phishing-Angriffe zu erkennen und zu vermeiden.
- (3) Der Auftragnehmer stellt sicher, dass alle eingehenden Dateien und E-Mails auf Schadsoftware zu scannen, bevor sie in das Netzwerk oder auf Endgeräte gelangen.

3.5.4 Schwachstellenmanagement

- (1) Der Auftragnehmer verpflichtet sich, regelmäßig Empfehlungen zur IT-Sicherheit aus verschiedenen Quellen wie z. B. Hersteller-Bulletins und BSI-Lageberichten zu prüfen und diese in Bezug auf die genutzten IT-Systeme zu bewerten. Sollte ein IT-System ganz oder teilweise von einer Sicherheitslücke betroffen sein, hat der Auftragnehmer unverzüglich eine Risikobewertung vorzunehmen.

⁵ Siehe <https://www.bsi.bund.de/dok/6596574>

3.5.5 Löschung von Auftraggeberinformationen

- (1) Der Auftragnehmer sichert zu – sofern keine abweichenden vertraglichen Anforderungen bezüglich der Aufbewahrung von Auftraggeberinformationen vereinbart sind oder gesetzliche Aufbewahrungspflichten entgegenstehen –, nach Vertragsende alle Auftraggeberinformationen vollständig und sicher zu löschen und/oder zu vernichten.
- (2) Der Auftragnehmer verpflichtet sich, ein geeignetes, dem aktuellen Stand der Technik entsprechendes Verfahren zur sicheren Löschung und Vernichtung von Auftraggeberinformationen anzuwenden. Das Verfahren muss mindestens enthalten:
 - a. nachvollziehbare Dokumentation von Löschvorgängen,
 - b. Kontaktierung des Auftraggebers vor der Löschung der Auftraggeberinformationen,
 - c. Verfahren zur vollständigen und sicheren Löschung von physischen Datenträgern und Speichermedien
- (3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber nach Aufforderung Nachweise über die Vernichtung bzw. Löschung von Auftraggeberinformationen vorzulegen.

3.5.6 Datensicherung und -archivierung

- (1) Der Auftragnehmer verpflichtet sich, regelmäßig Datensicherungen von allen Daten, die für die Leistungserbringung benötigt werden, durchzuführen.
- (2) Der Auftragnehmer verpflichtet sich, regelmäßig die Wirksamkeit und Funktionalität aller Datensicherungs- und Archivierungssysteme zu überprüfen. Nachweise über durchgeführte Überprüfungen werden dem Auftraggeber nach Aufforderung bereitgestellt.

3.5.7 Protokollierung und Überwachung (Angriffserkennung)

- (1) Der Auftragnehmer verpflichtet sich, Prozesse und Mechanismen zur Identifikation und Behandlung von sicherheitsrelevanten Ereignissen (SRE)⁶ zu etablieren.

3.5.8 Systemhärtung

- (1) Der Auftragnehmer verpflichtet sich, jene Systeme, die im Zusammenhang mit der Leistungserbringung relevant sind, entsprechend allgemeiner Konfigurationsstandards und Sicherheitsvorschriften (z. B. CIS-Benchmarks, BSI-IT-Grundschutzbausteinen, Herstellerempfehlung) zu härten.
- (2) Sofern für IT-Leistungen Standardpasswörter vorgegeben sind, stellt der Auftragnehmer sicher, dass sie vom Auftraggeber geändert werden können.

3.5.9 IT-Sicherheitsarchitektur

- (1) Der Auftragnehmer verpflichtet sich zur Etablierung einer IT-Sicherheitsarchitektur zur Sicherstellung eines angemessenen Schutzniveaus für alle Informationsdienste, die im Zusammenhang mit der Leistungserbringung stehen. Diese hat folgende Grundsätze zu erfüllen:
 - Informationssicherheit ist als integraler Bestandteil des Systemdesigns zu betrachten,

⁶ Siehe Glossar.

- Informationsdienste sind grundsätzlich als unsicher anzusehen,
- miteinander verbundene Systeme oder Komponenten sind als nicht vertrauenswürdig zu betrachten. Es muss verhindert werden, dass Angreifer nach der Übernahme der Kontrolle über ein Informationsdienst auf weitere Informationsdienste zugreifen können.
- Die IT-Sicherheitsarchitektur muss mehrschichtig aufgebaut und betrieben werden (z. B. Firewall, Authentifizierung, Isolierung, Härtung, Protokollierung, Schadsoftwareschutz etc.).
- Unterschiedliche Informationsdienste sind in Abhängigkeit der Kritikalität zu trennen und abzusichern.

3.5.10 Nutzung von kryptographischen Verfahren

- (1) Sofern der Auftragnehmer kryptographische Verfahren einsetzt, verpflichtet er sich, Konfigurationen und Schlüssellängen einzusetzen, die dem aktuellen Stand der Technik entsprechen. Um sicherzustellen, dass keine veralteten bzw. unsicheren kryptographischen Lösungen eingesetzt werden, verpflichtet der Auftragnehmer sich, eine Richtlinie für den Umgang mit kryptographischen Verfahren zu definieren.

3.5.1.1. Änderungs- und Patchmanagement

- (1) Der Auftragnehmer verpflichtet sich, einen Prozess zu etablieren, um die nach Veröffentlichung zeitnahe Implementierung von Patches und Updates für alle IT-Systeme, die im Zusammenhang mit der Verarbeitung von Auftraggeberinformationen stehen, zu etablieren. Patches- und Updates mit Auswirkungen auf die Leistungserbringung sollen in der Regel außerhalb der Hauptnutzungszeit eingespielt werden, sofern nicht aus Gründen der IT-Sicherheit ein unverzügliches Handeln geboten ist.

4 Kenntnisnahme/Bestätigung

Der Auftragnehmer bestätigt hiermit die Zustimmung zu den im vorliegenden Vertragsanhang:

- Vertragsanhang IT- und Informationssicherheitsanforderungen

enthaltenen Anforderungen und erklärt sich zur Einhaltung der Maßnahmen bereit.

Name	Unternehmen/Rolle	(Digitale) Unterschrift/Signatur
Vorname, Nachname		
Vorname, Nachname		
Vorname, Nachname		

Tabelle 4: Kenntnisnahme und Bestätigung

5 Anhang

5.1 Anhang I: Glossar

#	Begriff	Definition
1	CVSS	Common Vulnerability Scoring System (CVSS) - Internationaler Industriestandard zur Bewertung des Schweregrads von möglichen oder tatsächlichen Sicherheitslücken in IT-Systemen.
2	Kritische IT-Systeme	Diejenigen IT-Systeme, deren Ausfall oder Beeinträchtigung schwerwiegende Folgen hat. Diese Systeme können beispielsweise sensible Daten speichern, wichtige IT-gestützte Prozesse steuern oder eine besonders exponierte Stellung im Netzwerk haben.
3	Schwachstelle	Sicherheitslücke, die es einem Angreifer ermöglicht mithilfe eines sog. Exploits (Software zur Ausnutzung einer Schwachstelle) einen erfolgreichen Angriff auf ein IT-System durchzuführen.
4	Schutzbedürftige Gebäudeteile	Bereiche innerhalb eines Gebäudes, in denen sich sensible Informationen, Anlagen oder Ausrüstungen befinden, die einen besonderen Schutz vor unbefugten Zugriff oder anderen physischen Bedrohungen erfordern.
5	Sicherheitsrelevantes Ereignis (SRE)	Detektierte Aktion innerhalb eines Systems, die eine potenzielle Auswirkung auf die Informationssicherheit haben könnte.
6	Sicherheitsvorfall (Qualifiziertes SRE)	Unerwünschtes – tatsächlich eingetretenes – Ereignis, dass die Informationssicherheit beeinträchtigt und erhebliche Schäden verursachen kann.
7	Assets	Bezeichnet sämtliche materiellen oder immateriellen Güter, die im Rahmen der Leistungserbringung relevant sind. Es kann sich dabei um physische Objekte, Informationen, Systeme, Dienstleistungen, Ressourcen oder Prozesse handeln, wie zum Beispiel: <ul style="list-style-type: none"> • Physische Assets: Gebäude, Maschinen, Datenträger • Information Assets: Geschäftsdaten, Finanzdaten, Mitarbeiterdaten • System Assets: IT-Systeme, Netzwerkkomponenten • Personelle-Assets: Internes Personal, Dienstleister
8	IT-System	Gesamtheit der im Rahmen der Leistungserbringung relevanten Hard- und Software

Tabelle 5: Begriffsdefinitionen dieses Dokuments

5.2 Anhang II: Berichte zur Informationssicherheit

Der Auftragnehmer verpflichtet sich, regelmäßig Berichte gemäß der nachstehenden Tabelle über die vereinbarten Dienstleistungen bereitzustellen. Die erwarteten Inhalte und die Häufigkeit jedes Berichts werden in der folgenden Tabelle beschrieben.

#	Bericht	Inhalt	Häufigkeit
1	Sicherheitsvorfall	<ul style="list-style-type: none"> Detailbericht zu kritischen Sicherheitsvorfällen und -ereignissen inklusive Status, Schadensauswirkungen, Ursache und ergriffenen Maßnahmen. 	Ad-Hoc im Falle eines kritischen Sicherheitsvorfalls
2	Zugriffsberechtigtes Auftragnehmerpersonal	<ul style="list-style-type: none"> Liste des Personals des Auftragnehmers mit Zugriff auf Auftraggeberinformationen 	auf Anfrage des Auftraggebers
3	Prozessbeschreibungen	<ul style="list-style-type: none"> Vorgabe- und Nachweisdokumente zu den im Rahmen dieses Dokuments geforderten Betriebsprozessen 	auf Anfrage des Auftraggebers, ggf. im Rahmen eines Audits
4	Cloud-Security-Anforderungen	<ul style="list-style-type: none"> Auflistung, welche Sicherheitsmaßnahmen vom Cloud-Diensteanbieter und welche vom Auftragnehmer erfüllt werden müssen. 	auf Anfrage des Auftraggebers

Tabelle 6: Berichte zur Informationssicherheit