Anhang [XX] – Sicherheitsanforderungen an Auftragnehmer der BT

Inhaltsverzeichnis

TEIL 1: EINLEITUNG

1 EINLEITUNG

1.1 Dieses Dokument enthält die Sicherheitsanforderungen von BT.

1.2 In den vorliegenden Sicherheitsanforderungen kommen die Definitionen aus Teil 5 mit der Überschrift "**Definitionen**" zur Anwendung, im Übrigen sind die Bestimmungen des Vertrags anwendbar und alle Begriffe und Ausdrücke in den Sicherheitsanforderungen haben die gleiche Bedeutung wie im Vertrag.

1.3 Die Sicherheitsanforderungen gelten zusätzlich und unbeschadet weiterer im Vertrag festgelegter Pflichten des Auftragnehmers (einschließlich, jedoch ohne Beschränkung hierauf, der Pflichten wie sie in den Bestimmungen mit den Überschriften "**Vertraulichkeit**", "**Schutz personenbezogener Daten**" und "**Compliance**" genannt sind).

TEIL 2: VORAUSSETZUNGEN BEI EINGESCHRÄNKTEM ZUGANG

2 VORAUSSETZUNGEN BEI EINGESCHRÄNKTEM ZUGANG

Dieser Abschnitt bezieht sich auf Fälle, in denen der Auftragnehmer Leistungen ausführt oder Lieferungen erbringt, die einen eingeschränkten Zugang zu Daten von BT oder Kunden von BT erfordern oder für die eine Zugangsberechtigungsstufe für Verwaltungssysteme von BT vergeben wird. Für Auftragnehmer, die zu dieser Kategorie gehören, gelten die übrigen Bestimmungen dieses Dokuments nicht.

2.1 Der Auftragnehmer muss, unbeschadet von Verschwiegenheitsverpflichtungen in Fällen, in denen der Auftragnehmer oder Mitarbeiter Zugang zu BT-Daten haben:

2.2 Dafür sorgen, dass BT-Daten nicht an Mitarbeiter mitgeteilt werden oder diesen zugänglich gemacht werden, es sei denn, dies ist für die Auftragserfüllung erforderlich; und

2.3 Sämtliche Systeme und Verfahren einrichten (sowohl technischer als auch organisatorischer Art) in Übereinstimmung mit den Anforderungen der Guten Industriepraxis für Sicherheit zum Schutz und zur Geheimhaltung von BT-Daten und -Systemen.

TEIL 3: ALLGEMEINE SICHERHEITSANFORDERUNGEN

Zwingend zu beachten, wenn die in Teil 2 genannten Anforderungen bei eingeschränktem Zugang nicht anwendbar sind.

3 ALLGEMEINE DATENSICHERHEIT

Allgemeine Datensicherheit

3.1 Der Auftragnehmer hat Systeme und Verfahren einzurichten (sowohl technischer als auch organisatorischer Art), um:

3.1.1 Sicherheit und Vertraulichkeit von BT-Daten und -Systemen nach den Vorgaben der Sicherheitsanforderungen zu schützen; und

3.1.2 die Verfügbarkeit, Qualität, Vollständigkeit und angemessene Kapazität zur Erbringung der Leistungen ohne Unterbrechung sicherzustellen, wie nach den Anforderungen der Guten Industriepraxis für Sicherheit.

3.2 Der Auftragnehmer hat ein dokumentiertes Verfahren für Veränderungen im IT-Management einzurichten, um sicherzustellen, dass sämtliche Veränderungen auf Verfahren und Systeme des Auftragnehmers weiterhin in Übereinstimmung mit vorliegenden Sicherheitsanforderungen eintreten.

3.3 Der Auftragnehmer hat auf schriftliches Verlangen von BT dieser Kopien sämtlicher Sicherheitszertifikate und Übereinstimmungserklärungen zu überlassen, die für die Leistungen erheblich sind, um die Erfüllung mit vorliegenden Sicherheitsanforderungen nachzuweisen.

3.4 Der Auftragnehmer hat alle zumutbaren Schritte zu unternehmen, um geeignete Personen als Kontaktpersonen für Sicherheitsrisiken, Störfallmanagement und Compliance Management zu benennen. Der Auftragnehmer hat dem BT-Sicherheitskontakt alle Einzelheiten zu Kontaktdaten der Person und jegliche Änderungen mitzuteilen. Einzelheiten zu den Kontaktdaten sind:-

Name, Zuständigkeit, Funktion und firmeninterne E-Mail-Adresse und/oder Telefonnummer

3.5 Der Auftragnehmer erkennt an und stimmt zu, dass BT berechtigt ist, von Zeit zu Zeit zumutbare Änderungen der BT-Sicherheitsanforderungen vorzunehmen, bei:

3.5.1 Wechsel des Eigentümers oder Kontrollorgans des Auftraggebers infolge von Fusion, Übernahme oder wesentlichen Veränderungen;

3.5.2 Änderungen der Technologie- oder Industriestandards für Sicherheit; oder

3.5.3 Wesentlichen Änderungen bei Lieferungen und Leistungen oder der Art der Auftragserfüllung,

(jeweils als "**Veränderte Sicherheitsanforderung**" bezeichnet).

Nach Erhalt der schriftlichen Mitteilung von BT über das Erfordernis einer Änderung bei den Sicherheitsanforderungen hat der Auftragnehmer unverzüglich, in jedem Fall jedoch innerhalb einer zumutbaren Frist, die Änderung zu beachten (wobei die Zumutbarkeit sich nach der Art der Änderung und dem Risiko für BT richtet).

3.6 Der Auftragnehmer hat mindestens einmal jährlich oder bei wesentlichen Änderungen der Lieferungen oder der Art der Lieferungen die Sicherheitsanforderungen zu überprüfen, um deren Übereinstimmung mit allen anderen Sicherheitsanforderungen zu gewährleisten.

3.7 Erfüllt der Auftragnehmer Vertragspflichten mit Hilfe von Subunternehmern, hat der Auftragnehmer dafür zu sorgen, dass alle Verträge mit wichtigen Subunternehmern eine schriftliche Vereinbarung enthalten, durch die sich der Subunternehmer zur Einhaltung der jeweils maßgeblichen BT Sicherheitsanforderungen verpflichtet. Diese Vereinbarungen zwischen dem Auftragnehmer und seinen Subunternehmern müssen vorliegen, bevor der Subunternehmer oder dessen Personal Zugriff auf die BT-Systeme oder -Daten erhalten.

Nutzung von BT-Daten

3.8 Der Auftragnehmer ist nicht berechtigt, BT-Daten für andere als die vereinbarten Zwecke und über das zur Vertragserfüllung erforderliche Maß hinaus zu benutzen. Verarbeitet der Auftragnehmer personenbezogene Daten, ist er nicht berechtigt, solche Daten, die Teil der BT-Daten sind, zu anderen als zu den im Anhang für Datenverarbeitung speziell genannten Zwecken zu nutzen.

3.9 BT-Daten dürfen so lange gespeichert werden wie es für die Vertragserfüllung erforderlich ist und nach Vertragsende bis zu zwei Jahren, es sei denn, BT und der Auftragnehmer vereinbaren eine andere Speicherzeit oder eine solche ergibt sich aus gesetzlichen Vorschriften. Zur Vermeidung von Unklarheiten darüber, wann der Auftragnehmer personenbezogene Daten verarbeitet, ist er nicht berechtigt, personenbezogene Daten, die Teil der BT-Daten sind, länger als die im Anhang für Datenverarbeitung oder im Kapitel "**Schutz von personenbezogenen Daten**" speziell genannten Zeiträume zu speichern.

3.10 Der Auftragnehmer hat nachfolgend genannte Richtlinien und Standards zu befolgen:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

3.11 Bei direkter Lieferung für einen Vertrag mit der Regierung von Großbritannien hat der Auftragnehmer die aktuelle Version des Förderprogramms Cyber Essentials Plus einzuhalten.

Informationsverarbeitung

3.12 Der Auftragnehmer ist verpflichtet, Verfahren zur Informationsverarbeitung vor- und einzuhalten, die mit der Einstufung von Daten Dritter und Handhabungsbeschreibung übereinstimmen und mindestens sicherstellen, dass der Auftragnehmer:

3.12.1 geeignete Verfahren einrichtet, um die unbefugte Verbreitung von BT-Daten in jeder Form zu vermeiden, einschließlich E-Mail, Fax, soziale Netzwerke, Druckerzeugnisse oder Postsendungen (zum Beispiel: sicherstellen, dass die Saubere-Tisch- und Bildschirm-Politik umgesetzt wird und streng vertrauliche Daten nicht per Fax oder E-Mail verschickt werden);

3.12.2 in Besprechungen nicht über BT-Daten spricht, es sei denn, alle Teilnehmer: (i) sind berechtigt, an der Besprechung teilzunehmen; (ii) benötigen die besprochenen Daten; und (iii) kennen und beachten ihre Verschwiegenheitsverpflichtungen;

3.12.3 keine BT-Daten speichert:

3.12.3.1 in der Cloud oder mittels Internetdiensten, einschließlich, jedoch nicht beschränkt auf Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin oder Facebook, es sei denn, es besteht eine schriftliche Vereinbarung hierzu mit BT;

3.12.3.2 auf einem Laptop oder sonstigen Gerät, es sei denn, diese sind mit einer umfassenden Festplattenverschlüsselung ausgestattet (wie z.B. BitLocker), die den in Absatz 3.15 genannten Standards entspricht; oder

3.12.3.3 BT-Daten auf sichere Weise löscht oder unbrauchbar macht.

Zugangskontrolle

3.13 Der Auftragnehmer hat je nach Umgebung und Art der Lieferung an BT Zugangskontrollen bei eigenen Systemen zu unterhalten und gegebenenfalls dafür zu sorgen, dass:

3.13.1 alle Nutzer, einschließlich Nutzer auf Administratorebene über eigene ID verfügen;

3.13.2 regelmäßige Änderungen der Passwörter (mindestens alle 90 Tage) durchgeführt werden;

3.13.3 geeignete Schutzmechanismen eingerichtet werden nach erfolglosen Login-Versuchen zur Vermeidung von Brute-Force-Angriffen;

3.13.4 ungenutzte Konten automatisch gesperrt werden;

3.13.5 Passwörter einer bestimmten Länge benutzt werden (mindestens 8 Zeichen, davon müssen drei den folgenden Kategorien entstammen: (i) Großbuchstabe; (ii) Kleinbuchstabe; (iii) Ziffer; und (iv) Sonderzeichen) und der Passwortverlauf durchgesetzt wird, um die Verwendung früherer Passwörter innerhalb von 12 Monaten zu unterbinden;

3.13.6 rollenbasierter Zugriff auf Systeme des Auftragnehmers nach strengeren Anforderungen bei der Zugangskontrolle für Administratoren eingerichtet wird; und

3.13.7 regelmäßige Kontrollen und Überprüfungen von Benutzerzugriffen durchgeführt werden.

Remote-Zugriff

3.14 Der Auftragnehmer ist nicht berechtigt, Mitarbeitern Remote-Zugriff auf Daten zu gestatten, die als streng vertraulich eingestuft sind, es sei denn, es liegt eine schriftliche Vereinbarung hierzu mit BT vor. Wird Remote-Zugriff zugelassen, hat der Auftragnehmer dafür zu sorgen, dass geeignete Sicherheitskontrollen innerhalb seiner Organisation durchgeführt werden, einschließlich, jedoch nicht beschränkt auf das Erfordernis der Zwei-Faktor-Authentifizierung von Nutzern bei Remote-Zugriffen. Erfolgt ein Remote-Zugriff über ein öffentliches Netz zur Unterstützung, wird die Verbindung gemäß den Bestimmungen in Absatz 3.15 verschlüsselt.

Datenübertragung

3.15 Die routinemäßige Übertragung von Massenaufzeichnungen von BT-Daten hat über PGP oder eine zugelassene Transferplattform zu erfolgen.

Verschlüsselung

3.16 Der Auftragnehmer hat dafür zu sorgen, dass vertrauliche und streng vertrauliche BT-Daten sowohl im Ruhezustand als auch während Übertragungen nach den Bestimmungen für Gute Praxis zur Sicherheit verschlüsselt werden, um zu gewährleisten, dass keine Standards verwendet werden, die von der Branche abgelehnt werden. Aktuelle Verschlüsselungsstandards, die von BT zum Vertragsbeginn genehmigt werden und die in Absatz 3.15 genannten Anforderungen erfüllen, sind in den Bestimmungen zur Informationsklassifikation Dritter und Behandlungsbeschreibung genannt.

Fehlerkorrekturen

3.17 Der Auftragnehmer hat ein dokumentiertes Verfahren zur Fehlerkorrektur vorzuhalten und dieses einzuhalten. Das Verfahren hat mindestens sicherzustellen, dass der Auftragnehmer:

3.17.1 Fehlerkorrekturen (Patches) in folgenden zeitlichen Rahmen durchführt:

Art des Patches	Beschreibung	Zeitplan
Kritische Patches	Patches zur Korrektur von Zero-Day-Schwachstellen	So schnell wie möglich einsetzen und immer innerhalb von 14 Tagen nach Verfügbarkeit des Patches
Wichtige Patches	Schwachstellen, die als hoch, 7.0 - 8.9 auf der Skala für die Bewertung der Schwere von Schwachstellen nach den Standards des CVSS, eingestuft werden	Innerhalb von 30 Tagen nach Verfügbarkeit des Patches

Sonstige Patches	Alle übrigen Patches, die weder kritische noch wichtige Patches sind	Innerhalb von 8 Wochen nach Verfügbarkeit des Patches

3.17.2 alle möglichen Vertreiber für Patches beobachtet;

3.17.3 Patches verwendet, die direkt von Vertreibern für eigene Systeme erworben werden und Patches, die entweder (i) über eine digitale Unterschrift verfügen oder (ii) über eine Hash-Funktion des Vertreibers (MD5-Hashes sind nicht zu verwenden) für das Update-Paket, damit die Herkunft des Patchs als von einem seriösen Anbieter für Open-Source-Software festgestellt werden kann;

3.17.4 alle Patches auf Systemen testet, die genau den Einstellungen auf den Zielsystemen entsprechen vor deren Anwendung auf den Zielsystemen und die korrekte Patchleistung nach jeder Patchaktivität prüft; und

3.17.5 Systeme des Auftragnehmers wartet und aktualisiert um sicherzustellen, dass die neuesten Patches des Vertreibers verwendet werden können.

3.18 Ist die Fehlerkorrektur durch den Auftragnehmer nicht möglich, hat dieser BT schriftlich darüber zu informieren. Nach Erhalt einer derartigen Mitteilung hat BT das Risiko für BT und BT-Daten in Zusammenhang mit der weiteren Nutzung durch den Auftragnehmer zu prüfen. BT ist berechtigt, zumutbare Maßnahmen seitens des Auftragnehmers zu verlangen, derartige Risiken zu beheben (auf Kosten des Auftragnehmers).

Schwachstellen-Management

3.19 Der Auftragnehmer hat ein Verfahren zum Schwachstellen-Management vor- und einzuhalten. Das Verfahren hat mindestens sicherzustellen, dass der Auftraggeber:

3.19.1 geeignete Maßnahmen unternimmt, die Schwachstellen zu erkennen (zum Beispiel durch Scanning);

3.19.2 regelmäßige eigene Penetrationstests durchführt und Testberichte anfertigt; und

3.19.3 auf jede Nachricht über Schwachstellen reagiert und Aktionspläne einführt, bekannte Schwachstellen zu entschärfen gemäß der Absätze 3.22 bis 3.27.

Penetrationstests

3.20 Der Auftragnehmer ist verpflichtet:

3.20.1 BT (oder von BT befugten Subunternehmern) die Durchführung zumutbarer Penetrationstests nach angemessener Vorankündigung zu gestatten; und

3.20.2 BT den Zugriff auf vorhandene Penetrationstestberichte des Auftragnehmers in Bezug auf Lieferungen zu ermöglichen.

Audit und Protokollierung

3.21 Der Auftragnehmer hat ein Audit- und Protokollierungsverfahren vor- und einzuhalten, wobei sicherzustellen ist, dass der Auftragnehmer mindestens (soweit angezeigt) folgende Vorkommnisse aufzeichnet:

3.21.1 Beginn und Ende der protokollierten Verfahren;

3.21.2 Veränderungen in der Art der aufgezeichneten Vorkommnisse wie im Prüfprotokoll gefordert (zum Beispiel Startparameter und deren Veränderungen);

3.21.3 Ein- und Abschalten des Systems beim Auftragnehmer;

3.21.4 erfolgreich durchgeführte Anmeldungen;

3.21.5 misslungene Anmeldeversuche (zum Beispiel falsche Nutzer-ID oder falsches Passwort);

3.21.6 alle Vorgänge, die von berechtigten Nutzern durchgeführt werden (zum Beispiel Nutzer mit Zugang zu Systemprogrammen oder Anwendungen);

3.21.7 erfolgreiche und misslungene Privilegieneskalation;

3.21.8 sämtliche Zugriffe durch den Auftragnehmer oder dessen Mitarbeiter auf streng vertrauliche Daten und Eingriffe in diese; und

3.21.9 Einrichtung, Veränderung und Löschen von Benutzerkonten.

3.22 Zu jedem prüffähigen Ereignis hat der Auftragnehmer ein manipulationssicheres Prüfprotokoll vorzuhalten, das die Rekonstruktion derartiger Ereignisse ermöglicht.

3.23 Im Hinblick auf die Anfälligkeit von Komponenten/Daten hat der Auftragnehmer Prüfprotokolle regelmäßig zu kontrollieren und zu analysieren um verdächtige oder abweichende Vorkommnisse festzustellen und entsprechende Maßnahmen zu ergreifen und/oder einen Alarm auszulösen.

3.24 Sämtliche Alarmsituationen müssen schriftlich festgehalten werden und innerhalb eines Zeitrahmens bearbeitet werden, der sich nach der Alarmstufe richtet.

3.25 Der Auftragnehmer verpflichtet sich, die Protokolle 3 Monate aufzubewahren (es sei denn, in den Bedingungen mit der Überschrift "**Schutz von personenbezogenen Daten**" wird ein anderer Zeitrahmen aufgestellt) und Kopien anzufertigen oder nach Aufforderung durch BT Zugriff auf die Protokolldateien zu gewähren in einem von beiden Parteien zu vereinbarenden Format.

Threat Management und Umgang mit Sicherheitsvorfällen

3.26 Der Auftragnehmer hat ein formelles Verfahren zur Behandlung von Sicherheitsvorfällen vor- und einzuhalten, in dem Zuständigkeiten bei sicherheitsrelevanten Vorfällen genau festlegt sind. Sämtliche Informationen in Bezug auf sicherheitsrelevante Vorfälle sind als "**vertraulich**" zu behandeln.

3.27 Der Auftragnehmer hat den BT-Sicherheitskontakt und den kaufmännischen Ansprechpartner von BT innerhalb einer zumutbaren Frist nach Kenntnis eines sicherheitsrelevanten Vorfalls zu informieren, in jedem Fall innerhalb von maximal zwölf (12) Stunden.

3.28 Der Auftragnehmer hat geeignete und zeitgerechte Maßnahmen zu ergreifen, um die Risiken und Folgen eines sicherheitsrelevanten Vorfalls abzumildern und die Stärke und Dauer des Vorfalls zu verringern.

3.29 Der Auftragnehmer verpflichtet sich, alle Informationen, die BT in Bezug auf den sicherheitsrelevanten Vorfall verlangt, mitzuteilen, einschließlich, jedoch nicht beschränkt auf:

3.29.1 Datum und Uhrzeit;

3.29.2 Ort;

3.29.3 Art des Vorfalls;

3.29.4 Auswirkung;

3.29.5 Einstufung der betroffenen Daten;

3.29.6 Status und

3.29.7 Ergebnis (einschließlich Empfehlungen oder durchgeführte Maßnahmen zur Problemlösung).

3.30 Der Auftragnehmer hat dafür zu sorgen, dass erkannte Risiken in Bezug auf Vertraulichkeit, Vollständigkeit oder Verfügbarkeit von BT-Daten in Verfahren oder Systemen des Auftragnehmers unverzüglich beseitigt werden.

3.31 Stellt ein sicherheitsrelevanter Vorfall auch eine Verletzung von personenbezogenen Daten dar, hat der Auftragnehmer zusätzlich zu den Bestimmungen dieser Sicherheitsanforderungen auch die Bestimmungen im Abschnitt mit der Überschrift "**Schutz personenbezogener Daten**" zu beachten. Zur Vermeidung von Unklarheiten hat der Auftragnehmer ebenfalls die Bestimmungen im Abschnitt mit der Überschrift "**Schutz von personenbezogenen Daten**" in Bezug auf sämtliche Verletzungen personenbezogener Daten zu beachten, unabhängig davon, ob der Verstoß als sicherheitsrelevanter Vorfall zu betrachten ist.

4 SICHERHEIT DER MITARBEITER

4.1 Mitarbeiter dürfen erst dann Zugang erhalten, wenn sie das Training für Informationssicherheit von BT absolviert haben, das über https://workingwithbt.extra.bt.com aufgerufen werden kann oder über das BT-Lernsystem, bei dem Mitarbeitern eine BT-Identifikationsnummer zugeteilt wird. Das Training für Informationssicherheit von BT ist von Zeit zu Zeit zu aktualisieren, die Einzelheiten hierzu enthält https://workingwithbt.extra.bt.com. Der Auftragnehmer hat die Aufzeichnungen zu durchgeführten Trainingseinheiten für Prüfungen durch BT aufzubewahren.

4.2 Der Auftragnehmer hat dafür zu sorgen, dass alle Mitarbeiter Vertraulichkeitserklärungen unterzeichnen, die ähnliche Verpflichtungen enthalten wie für den Auftragnehmer in Teil 2, bevor sie in Gebäuden oder an Systemen von BT arbeiten oder Zugang zu BT-Daten bekommen. Der Auftragnehmer hat die Vertraulichkeitserklärungen aufzubewahren und BT zur Prüfung zur Verfügung zu stellen.

4.3 Der Auftragnehmer hat Verstöße gegen die eigenen Sicherheitsbestimmungen- und Verfahren und die von BT mit einem formellen Verfahren zu ahnden, einschließlich eines Disziplinarverfahrens, durch das den Mitarbeitern:

4.3.1 der Zugriff auf BT-Systeme und BT-Daten oder

4.3.2 die Ausführung von Arbeiten in Zusammenhang mit der Auftragserfüllung untersagt wird.

Darüber hinaus hat der Auftragnehmer sicherzustellen, dass Mitarbeiter, die in o.g. Fällen von der Ausübung ihrer Aufgaben entfernt werden, im Anschluss daran keinen Zugang zu BT-Systemen oder BT-Daten erhalten oder Arbeiten in Zusammenhang mit Lieferungen ausführen.

4.4 Der Auftragnehmer hat innerhalb des gesetzlich zulässigen Rahmens eine vertrauliche Hotline vorzuhalten, die von allen Mitarbeitern genutzt werden kann, wenn sie ein mit diesen Sicherheitsanforderungen unvereinbares Verhalten oder eine Verletzung der Sicherheitsanforderungen feststellen. Der Auftragnehmer hat dem BT-Sicherheitskontakt diesbezüglich Bericht zu erstatten.

4.5 Führt ein Mitarbeiter keine Leistungen zur Auftragserfüllung mehr aus, hat der Auftraggeber dafür zu sorgen, dass:

4.5.1 der Zugriff auf BT-Daten widerrufen wird und

4.5.2 auf Anforderung durch Sachwerte oder Daten von BT, die sich in Besitz des Mitarbeiters befinden, entweder:

4.5.2.1 dem zuständigen BT-Team zurückgegeben werden oder

4.5.2.2 nach der aktuell gültigen Version zur Einstufung von Daten Dritter und Handhabungsbeschreibung vernichtet werden.

4.6 Soweit keine anders lautende schriftliche Vereinbarung mit dem BT-Sicherheitskontakt getroffen wurde, hat der Auftragnehmer ein geprüftes Austrittsverfahren für Mitarbeiter einzuführen, das die schriftliche Anfrage an den BT-Sicherheitskontakt einschließt, den Zugang zu BT-Systemen und BT-Daten und sämtliche sonstigen Zugriffe und Zugänge zu löschen. Mitarbeiter sind darauf hinzuweisen, dass ihre Vertraulichkeitserklärungen in Kraft bleiben und BT-Daten, die sie während ihrer Tätigkeit im Rahmen der Vertragserfüllung erfahren, nicht weitergegeben werden dürfen.

4.7 Im Rahmen der Zugangsbewilligung hat der Auftragnehmer Aufzeichnungen zu sämtlichen Mitarbeitern vorzuhalten und mitzuteilen, die eine Zugangsbewilligung beantragen oder mit der Auftragserfüllung gegenüber BT beschäftigt sind, einschließlich Name, Einsatzort, unternehmenseigene E-Mail-Adresse, Telefondirektwahl und Anschlussnummer am Arbeitsplatz (falls anwendbar) und/oder Mobiltelefonnummer, Datum des Antrags auf Zuteilung einer Nutzer-Identifikationsnummer (UIN) (falls vorhanden), Datum für den Beginn der Tätigkeit im Rahmen der Auftragserfüllung an BT, Datum des Abschlusses der Pflichtausbildung, Datum des Endes der Tätigkeit im Rahmen der Auftragserfüllung an BT und Erklärung zur Zuverlässigkeitsprüfung. Der Sicherheitskontakt des Auftragnehmers haftet stets dafür, dass nur Mitarbeiter eine Genehmigung erhalten.

4.8 Der Auftragnehmer hat Bestimmungen und Verfahren vorzuhalten, um sicherzustellen, dass Mitarbeiter keine sozialen Netzwerke benutzen, um online Erklärungen, Kommentare, Inhalte oder Bilder zu versenden, die

4.8.1 vernünftigerweise als Standpunkte von BT verstanden werden können,

4.8.2 vertrauliche BT-Daten oder Daten, die als ‘Vertraulich’ oder ‘Streng Vertraulich’ eingestuft sind, veröffentlichen und

4.8.3 BT diffamieren und der Marke und dem Ansehen von BT Schaden zufügen können.

5 AUDIT & SICHERHEITSÜBERPRÜFUNGEN

5.1 Unbeschadet sonstiger Rechte von BT zur Durchführung von Kontrollen behält sich BT und deren benannte Vertreter vor, zur Feststellung der Einhaltung vorliegender Sicherheitsanforderungen und gegebenenfalls der Bestimmungen zu “**Schutz von personenbezogenen Daten**”, gelegentlich Sicherheitsaudits durchzuführen zu ausgewählten oder allen Aspekten der Bestimmungen, Verfahren und Systeme des Auftragnehmers mittels einer dokumentgestützten Sicherheitsüberprüfung sowohl an der Betriebsstätte des Auftragnehmers als auch an Betriebsstätten von Subunternehmern, die mit der Erbringung von Leistungen oder Lieferungen zur Vertragserfüllung betraut sind.

5.2 Der Auftragnehmer ermöglicht BT oder deren Vertreter Zugang und leistet diesen Unterstützung soweit erforderlich und angemessen bei dokumentgestützten Sicherheitsüberprüfungen oder Audits in Betriebsstätten. Der Auftragnehmer erhält 30 Tage im Voraus die Benachrichtigung für ein routinemäßiges Audit in der Betriebsstätte, jedoch ist BT im Falle einer festgestellten oder vermuteten Verletzung von personenbezogenen Daten oder sicherheitsrelevanten Verstößen nicht zur Vorankündigung verpflichtet.

5.3 Der Auftragnehmer ist verpflichtet, mit BT zusammenzuarbeiten und auf eigene Kosten innerhalb von 30 Tagen oder einer entsprechend vereinbarten Frist nach Aufforderung durch BT vereinbarte Empfehlungen umzusetzen und Korrekturen vorzunehmen, die BT für erforderlich erachtet und sich aus einer dokumentgestützten Sicherheitsüberprüfung oder infolge eines Audits in der Betriebsstätte ergeben.

5.4 Wird BT gezwungen, ein unabhängiges Audit des Auftragnehmers durchzuführen und wird dabei festgestellt, dass der Auftragnehmer die Bestimmungen und Praktiken der ISO/IEC 27001:2013 nicht einhält, hat dieser auf eigene Kosten die zur Erfüllung erforderlichen Handlungen durchzuführen und BT deren Kosten für das Audit vollumfänglich zu erstatten.

6 ERMITTLUNGEN

6.1 Hat BT einen Verdacht auf das Vorliegen

6.1.1 einer Verletzung personenbezogener Daten,

6.1.2 eines sicherheitsrelevanten Verstoßes

6.1.3 oder eines Verstoßes gegen vorliegende Sicherheitsanforderungen,

informiert BT den Sicherheitsbeauftragten des Auftragnehmers und dieser verpflichtet sich, auf eigene Kosten:

6.1.4 unverzüglich Maßnahmen einzuleiten, den vermuteten Verstoß aufzudecken, einen solchen zu verhindern und dafür zu sorgen, Folgen eines Verstoßes abzuwenden; und

6.1.5 alles zu unternehmen, den ordnungsgemäßen Zustand wieder herzustellen und den Verstoß zu beheben.

6.1.6 auf Verlangen von BT Berichte zu Ermittlungsergebnissen und Maßnahmen zur Abwendung des Verstoßes BT zur Verfügung zu stellen,

Im Fall eines schweren Verstoßes ist der Auftragnehmer verpflichtet, vollumfänglich mit BT zusammenzuarbeiten bei sämtlichen Ermittlungen oder Audits durch BT oder Regulierungsbehörden und/oder Strafverfolgungsbehörden, die auch den Zugang zu BT-Daten einschließen, die in den Betriebsstätten des Auftragnehmers oder auf dessen Systemen vorhanden sind.

Während der Ermittlungen ist der Auftragnehmer verpflichtet, mit BT zusammenzuarbeiten und die für die Ermittlungen eines Verstoßes erforderlichen und geeigneten Zugänge zu ermöglichen und Unterstützung zu leisten. BT ist berechtigt, den Auftragnehmer aufzufordern, dessen materielle oder immaterielle Vermögenswerte in Quarantäne zu stellen, wenn dies den Ermittlungen dienlich ist. Der Auftragnehmer ist nicht berechtigt, sich einer solchen Aufforderung unbillig zu widersetzen oder dieser verzögert nachzukommen.

TEIL 4: BESONDERE SICHERHEITSANFORDERUNGEN

7 ALLGEMEINE SICHERHEITSANFORDERUNGEN & BESTIMMUNGEN

7.1 Der Auftragnehmer garantiert, dass Systeme, Lieferungen, Nebenleistungen, Verfahren und Orte stets die Standards der ISO/IEC 27001:2013 und aller zukünftig geltenden Versionen der Standards erfüllen. Die Einhaltung mit den Standards ist nach Ermessen von BT wie folgt nachzuweisen:

7.1.1 durch Zertifizierung des Informationssicherheits-Managementsystems ISMS des Auftragnehmers durch eine zum britischen Akkreditierungsservice UKAS gehörende Stelle oder einer internationalen anerkannten Zertifizierungsstelle, dessen Rahmen und Erklärung zur Anwendbarkeit von BT bestätigt wurde oder

7.1.2 durch ein von BT bestimmtes bilaterales Audit- und Testverfahren.

7.2 Der Auftragnehmer hat zu Beginn des Vertrags ein gültiges ISO/IEC 27001 Zertifikat vorzulegen und nachfolgende erneuerte Zertifikate.

7.3 Bei Änderung von Rahmen und Erklärung zur Anwendbarkeit der Zertifizierung hat der Auftragnehmer diese Änderungen unter Einhaltung des Kontrollverfahrens für Änderungen neu zertifizieren zu lassen (oder, falls ein Kontrollverfahren für Änderungen nicht vorliegt, mittels eines Änderungsverfahrens). Der Auftragnehmer hat BT innerhalb von 2 Werktagen über größere Abweichungen zu informieren, die durch die Zertifizierungsstelle oder den Auftragnehmer selbst festgestellt werden.

8 PHYSISCHE SICHERHEIT – BETRIEBSSTÄTTEN VON BT

Dieser Abschnitt ist zu beachten, wenn der Auftragnehmer Leistungen in Betriebsstätten von BT erbringt.

8.1 Mitarbeiter, die in Betriebsstätten von BT eingesetzt werden, haben zum Nachweis ihrer Zugangsberechtigung einen Ausweis des Auftraggebers oder von BT bei sich zu führen und sichtbar zu tragen ("**Zugangsberechtigungsausweis**"). Der Zugangsberechtigungsausweis enthält ein Lichtbild, das den Mitarbeiter eindeutig erkennen lässt. Mitarbeiter erhalten je nach örtlichen Sicherheitsanordnungen ebenfalls einen elektronischen Zugangsausweis und/oder einen zeitlich begrenzt gültigen Besucherausweis.

8.2 Der Auftragnehmer hat BT unverzüglich, spätestens innerhalb von 5 Werktagen zu informieren, wenn Mitarbeiter, die über einen BT-Zugangsberechtigungsausweis verfügen, keinen Zugang mehr zu BT-Betriebsstätten benötigen.

8.3 Es dürfen nur zugelassene von BT erstellte Server, Webtop PCs und sichere Endgeräte direkt an BT-Domains angeschlossen werden (über LAN-Anschluss oder Wireless-Verbindung). Auftragnehmer (und gegebenenfalls dessen

Mitarbeiter) dürfen Geräte, die keine Zulassung von BT haben, nur nach vorheriger schriftlicher Genehmigung des BT-Sicherheitsbeauftragten an BT-Domains anschließen. Der BT-Sicherheitskontakt erteilt die schriftliche Genehmigung erst nach Durchführung des BT-internen Sicherheitsprüfungsverfahrens. Der Auftragnehmer hat in jedem Fall dafür zu sorgen, dass keine persönlichen Geräte der Mitarbeiter und sonstiger Beschäftigter (einschließlich Auftragnehmer, überlassene Arbeitnehmer und Leiharbeiter) benutzt werden, um BT-Daten zu speichern, einzusehen oder zu verarbeiten.

8.4 BT-Daten dürfen aus Betriebsstätten von BT nur nach vorheriger Genehmigung durch BT entfernt werden und ebenfalls dürfen Geräte oder Software nur nach vorheriger Genehmigung durch BT aus Betriebsstätten von BT entfernt oder in diesen installiert werden.

8.5 Maßnahmen und Richtlinien zum Gesundheitsschutz und zu Arbeiten in den Betriebsstätten von BT sind zu beachten, einschließlich, aber nicht beschränkt auf begleitende Mitarbeiter und die Übernahme von geeigneten Arbeitsmethoden in Sicherheitsbereichen.

8.6 Ist der Auftragnehmer befugt, seinen Mitarbeitern von außen Zugang zu Bereichen in Liegenschaften von BT zu gestatten, sind die von BT autorisierten Mitarbeiter verpflichtet, die Bestimmungen über "**Zugang des Auftragnehmers zu Betriebseinrichtungen und Gebäuden von BT**" einzuhalten https://groupextranet.bt.com/selling2bt/working/third_party_access/default.htm. Zusätzlich haben Mitarbeiter ohne Zugangsberechtigung von BT mindestens eine L2-Zuverlässigkeitsüberprüfung vorzuweisen https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

9 PHYSISCHE SICHERHEIT – BETRIEBSSTÄTTEN DES AUFTRAGNEHMERS

Dieser Abschnitt ist zu beachten, wenn der Auftragnehmer Leistungen außerhalb von BT-Betriebsstätten erbringt. (Z.B. Betriebsstätten des Auftragnehmers oder Dritter.)

9.1 Der Zugang zu BT-fremden Betriebsstätten (Standorte, Gebäude oder interne Bereiche), in denen Leistungen erbracht werden oder BT-Daten gespeichert oder verarbeitet werden, ist nur unter Verwendung einer Ausweiskarte für zugangsberechtigte Auftragnehmer gestattet. Der Ausweis dient jederzeit der Identitätsprüfung in den jeweiligen Betriebsstätten, wobei das auf dem Ausweis enthaltene Lichtbild eindeutig den Inhaber erkennen lassen muss. Zugangsberechtigte Personen können ebenfalls einen elektronischen Zugangsausweis oder Zugang über eine Sicherheitstastatur erhalten. Der Auftragnehmer hat Verfahren vorzuhalten für: Genehmigungen, Änderungen von Zugangscodes (mindestens monatlich) und ad-hoc Codeänderungen.

9.2 Der Auftragnehmer muss dafür sorgen, dass der Zugang zu BT-fremden Betriebsstätten, in denen Leistungen für BT erbracht werden oder BT-Daten gespeichert oder verarbeitet werden, mit Genehmigung erfolgt und Sicherheitsverfahren dafür vorliegen und die entsprechenden Kontrollen und Überprüfungen von Mitarbeitern, Besuchern und sonstigen Personen, einschließlich Dritter mit Zugang zu diesen Bereichen (z.B. Im Rahmen von Umweltkontrollen, Sicherheits- oder Reinigungsdiensten) durchgeführt werden.

9.3 Auf Verlangen von BT hat der Auftragnehmer dafür zu sorgen, dass Mitarbeiter sicher von anderem Personal des Auftragnehmers getrennt werden. Darüber hinaus hat der Auftragnehmer dafür zu sorgen, dass Systeme und Infrastrukturen zur Erfüllung der Auftragsleistungen in einem besonders dafür bereitgestellten Netzwerk enthalten sind. Dieses Netzwerk darf nur aus Systemen bestehen, die der Bereitstellung einer sicheren Datenverarbeitungseinrichtung dienen.

9.4 Sicherheitsbereiche in Betriebsstätten des Auftragnehmers (z.B. Netzwerkkommunikationsräume) sind von anderen Räumen abzutrennen und mit geeigneten Zugangskontrollen zu schützen, um sicherzustellen, dass nur befugte Mitarbeiter Zugang haben. Zugänge zu diesen Bereichen durch Mitarbeiter sind mindestens einmal im Monat zu überprüfen und mindestens einmal im Jahr sind die Zugangsberechtigungen neu zu vergeben.

Der Auftragnehmer hat auf Verlangen von BT Nachweise über die Risikoanalyse vorzulegen. Wird der Aufforderung von BT nicht entsprochen, kann BT nach eigenem Ermessen selbst oder durch einen beauftragten Vertreter vor Beginn der Leistungen zur Auftragserfüllung eine Risikoanalyse der Umgebung, vornehmen, in der Leistungen erbracht werden sollen (z.B. Datenzentren, Datenverarbeitungsbereiche, Computerräume). Darüber hinaus ist BT vor Ausführung von erheblichen Arbeiten in Betriebsstätten, die die Sicherheit von BT-Daten beeinträchtigen können, zu informieren.

9.5 Sicherheits-Videoüberwachungssysteme (CCTV) und damit verbundene Aufzeichnungsmedien sind vom Auftragnehmer entweder als Reaktion auf Sicherheitsvorfälle oder als Instrument der Sicherheitskontrolle oder zur Abschreckung oder als Hilfsmittel zur Ergreifung von auf frischer Tat ertappter Straftäter einzusetzen. Aufnahmen aus Videoüberwachung (auf Band oder digital) sind mindestens 20 Tage zu speichern. Diese Frist kann in folgenden Fällen verlängert werden:

9.5.1 wenn der CCTV-Videobeweis für Ermittlungen zu sicherheitsrelevanten Vorfällen oder strafrechtlichen Ermittlungen aufbewahrt werden muss; oder

9.5.2 wenn dies zur Einhaltung von gesetzlichen Bestimmungen erforderlich ist.

9.5.3 Sämtliche Videoaufnahmen sind in einem abgeschlossenen Schrank aufzubewahren, dessen Schlüssel sicher aufzubewahren und kontrollieren sind. Der Zugriff zum Schrank ist nur befugten Personen gestattet.

9.6 Sämtliche Videoaufzeichnungsgeräte sind an einem sicheren Ort aufzustellen, um Veränderungen oder Zerstörung zu vermeiden, ebenso wie die Möglichkeit der „zufälligen“ Übertragung auf angeschlossene Videobildschirme, nach den Richtlinien zur Benutzung von Videoüberwachungen unter

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

9.7 Der Auftragnehmer hat alle Bereiche seiner Betriebsstätten, die zur Auftragserfüllung benutzt werden, mindestens einmal im Monat auf Gefahren und Bedrohungen zu überprüfen. Der Auftragnehmer hat alle geeigneten Maßnahmen zum Schutz der körperlichen Unversehrtheit zu beachten und durchzuführen im Hinblick auf:

9.7.1 Kenntnis von Bedrohungen am Standort, einschließlich, aber nicht beschränkt auf mögliche Bedrohungen von Industriebetrieben am Ort und von in der Nähe gelagerter gefährlicher Materialien; und

9.7.2 Naturkatastrophen, einschließlich, aber nicht beschränkt auf Risiken wie Hochwasser, Erdrutsche oder extreme Wetterlagen.

9.8 Elektrische und Telekommunikationsleitungen in den Betriebsstätten des Auftragnehmers, die Daten enthalten oder Informationsdienste unterstützen oder Radio-/Satellitenleistungen, die zur Leistungserbringung verwendet werden, sind vom Auftragnehmer so sicher einzurichten, dass die Unterbrechung der Geschäftstätigkeit verhindert wird. Physische Sicherheitsmaßnahmen im Einklang mit dem Risikograd der Geschäftstätigkeiten, für die sie vorgesehen sind, sind wie folgt auszuführen:

9.8.1 Geschäftskritische Fahrbahnen, Kabelschirme oder Schächte mit geschäftskritischen Kabeln sind zu schützen;

9.8.2 Der Zugang zu Kabelschächten oder Steigleitungskästen darf nur mit elektronischer Zugangskontrolle oder einem Effective-Key-Management erfolgen;

9.8.3 Computerkommunikationsverbindungen und Kommunikationsanlagen in Computern sind geschützt und umweltgeschützt einzurichten; und

9.8.4 Radio- und Satellitenkommunikationsverbindungen und Kommunikationsanlagen sind sachgerecht zu sichern.

9.9 BT verlangt, sofern keine anders lautende Vereinbarung zwischen dem Auftragnehmer und dem BT-Sicherheitsbeauftragten besteht, dass der Auftragnehmer einen Sicherheitsdienst einrichtet zur Ergänzung der elektronischen und physischen Sicherheitsmaßnahmen in den Betriebsstätten des Auftragnehmers, wenn:

9.9.1 Stellen entscheidende Bedeutung für den Geschäftsbetrieb haben (z.B. Kontaktzentren, Rechenzentren, Schlüsselstandorte für Netzwerke etc.)

9.9.2 Verarbeitete BT-Daten Marken und Ansehen von BT beeinträchtigt werden können oder einen Nachteil erleiden können

9.9.3 große BT-Datenmengen verarbeitet werden (z.B. Auslagerung von Geschäftsprozessen)

9.9.4 Vertragsverpflichtungen mit Kunden bestehen

9.9.5 besondere Risiken/Bedrohungen an der Betriebsstätte vorliegen

9.9.6 Der Auftragnehmer hoch sensible BT-Daten besitzt.

9.10 Um BT-Anlagen (wie z.B. Server oder BT-Schalter) in den Betriebsstätten des Auftragnehmers vor Umweltschäden oder -gefahren zu schützen und vor der Gefahr unbefugter Zugriffe, sind BT-Anlagen in einem geschützten Bereich und getrennt von Anlagen, die von Systemen BT-fremder Organisationen benutzt werden, aufzustellen. Die Trennung hat so zu erfolgen, dass die Sicherheit der BT-Anlagen weder vorsätzlich noch zufällig gefährdet wird infolge von Zugriffen BT-fremder Organisationen. Die Trennung kann zum Beispiel durch Einziehen von Sicherheitswänden, Einrichtung von abschließbaren Schränken oder Metallkäfigen erfolgen.

9.11 Der Auftragnehmer hat geeignete Maßnahmen durchzuführen, um physische Sicherheit zu garantieren im Hinblick auf:

9.11.1 Brandschutzmaßnahmen einschließlich, jedoch nicht beschränkt auf Alarm-, Brandmelde- und Brandbekämpfungsanlagen;

9.11.2 Witterungsverhältnisse hinsichtlich Temperatur, Feuchtigkeit, statische Elektrizität und damit zusammenhängendes Management, Überwachung und Reaktionen auf extreme Bedingungen (wie zum Beispiel automatische Abschaltungen, Alarme);

9.11.3 Kontrollanlagen einschließlich, aber nicht beschränkt auf Klimaanlagen und Wassermelder;

9.11.4 Lage von Wasserspeichern, Leitungen etc. innerhalb der Betriebsstätten;

9.11.5 überprüfbaren Zugang - wenn der Zugang zu Systemen durch Personen überprüfbar sein muss und

9.11.6 Überwachung von Mitarbeitern, die üblicherweise nicht mit dem BT-Systemmanagement oder -zugang in Verbindung stehen.

9.12 Sicherheitszonen (Barrieren wie Wände, Zäune, Eingangstore mit Ausweiskontrolle oder personalbesetzte Rezeptionen) sind zum Schutz von Bereichen einzurichten mit sensiblen BT-Daten oder Daten von BT-Kunden (einschließlich personenbezogene Daten) und damit verbundenen Einrichtungen.

9.13 Zugangsstellen wie Liefer- und Ladezonen und sonstige Stellen, an denen unbefugte Personen in die Betriebsstätten gelangen können, sind zu überwachen und, falls möglich, von den datenverarbeitenden Einrichtungen zu trennen, um unbefugten Zugang oder vorsätzliche Angriffe zu verhindern.

9.14 Der Auftragnehmer hat dafür zu sorgen, dass der Zugang zu Bereichen, in denen Zugriff auf BT-Daten oder Daten von BT-Kunden (einschließlich personenbezogene Daten) möglich ist, mit Chip- oder Transponderkarten erfolgt (oder gleichwertiger Sicherheitssysteme) und er hat zwecks Einhaltung dieser Bestimmungen monatliche interne Audits durchzuführen.

9.15 Der Auftragnehmer hat dafür zu sorgen, dass das Fotografieren und/oder die Aufnahme von Bildern von BT-Daten oder Daten von BT-Kunden (einschließlich personenbezogene Daten) untersagt wird. In Ausnahmefällen, in denen die Aufnahme solcher Bilder aus geschäftlichen Gründen erforderlich ist, ist eine befristete Ausnahme dieser Bestimmung zu beantragen und schriftlich durch den BT-Sicherheitsbeauftragten zu erteilen.

9.16 Der Auftragnehmer hat zum Schutz von BT-Daten die Standards zum sauberen Schreibtisch und zum sauberen Bildschirm einzuhalten.

10 LIEFERUNG BEI HOSTING-AUSSTATTUNG

Dieser Abschnitt ist zu beachten wenn der Auftragnehmer ein Hosting-Umfeld für BT-Anlagen oder Anlagen von BT-Kunden liefert.

10.1 Stellt der Auftragnehmer an seiner Betriebsstätte einen sicheren Zugangsbereich zur Verfügung für das Hosting von BT-Anlagen oder Anlagen von BT-Kunden ("**Betriebsstätte des Auftragnehmers**"), hat er

10.1.1 dafür zu sorgen, dass alle Mitarbeiter mit Zugang zu den Betriebsstätten über eine Ausweiskarte oder eine elektronische Ausweiskarte verfügen. Diese Karte dient der Identitätskontrolle in den Betriebsstätten des Auftragnehmers und hat ein Lichtbild des Mitarbeiters zu enthalten, das diesen eindeutig erkennen lässt; und

10.1.2 Verfahren einzurichten für den Umgang mit Sicherheitsgefahren für BT-Anlagen oder Anlagen von BT-Kunden oder gegen Dritte, die für BT tätig sind, um BT-Daten und Daten von BT-Kunden in Betriebsstätten des Auftragnehmers zu schützen; und

10.1.3 in den Betriebsstätten des Auftragnehmers Videoüberwachungssysteme einzusetzen und dazugehörige Aufnahmemedien als Reaktion auf Sicherheitsvorfälle, Sicherheitsüberwachungsinstrument, zur Abschreckung und zur Unterstützung bei der Ergreifung von Tätern, die auf frischer Tat ertappt werden. Der Auftragnehmer hat dafür zu sorgen, dass Videoüberwachungsaufnahmen 20 Tage gespeichert werden, um für Ermittlungen verwendet werden zu können; und

10.1.4 BT einen Lageplan der Sicherheitsbereiche in den Betriebsstätten des Auftragnehmers zu übergeben und

10.1.5 sicherzustellen, dass Schränke von BT und Kunden von BT in Betriebsstätten des Auftragnehmers verschlossen sind und nur befugte BT-Mitarbeiter, Vertreter von BT und verantwortliche Mitarbeiter Zugang haben und

10.1.6 ein sicheres Schlüsselmanagement-Verfahren in der Betriebsstätte des Auftragnehmers einzurichten und

10.1.7 die Umgebung der Betriebsstätte des Auftragnehmers regelmäßig auf Risiken oder Bedrohungen zu überprüfen und

10.1.8 Arbeitsanweisungen (in der Sprache des Landes, aus der die Arbeit von BT stammt) schriftlich festzuhalten und aufzubewahren zur Erfüllung der einzelnen Sicherheitsanforderungen in Absatz 10 und auf Aufforderung BT Zugang zu der Dokumentation zu gewähren.

10.2 BT hat an den Auftragnehmer zu liefern:

10.2.1 Eine Aufstellung von Sachwerten von BT oder deren Kunden, die sich in den Betriebsstätten des Auftragnehmers befinden; und

10.2.2 Angaben zu Mitarbeitern, Subunternehmern und Handelsvertretern von BT, die Zugang zu den Betriebsstätten des Auftragnehmers erhalten (fortlaufend).

11 ENTWICKLUNG VON LEISTUNGEN

Dieser Abschnitt ist zu beachten, wenn der Auftragnehmer Leistungen entwickelt zur Anwendung durch BT und/oder Kunden von BT. Dies schließt „Standardkomponenten“, Softwarekonfiguration und Herstellung von Komponenten für die Lieferungen und Leistungen ein.

11.1 Der Auftragnehmer hat an allen gelieferten Komponenten, die zu den Lieferungen und/oder Leistungen gehören, vereinbarte Sicherheitsmaßnahmen einzurichten, um die Vertraulichkeit, Verfügbarkeit und Vollständigkeit der Auftragsverpflichtungen zu garantieren. Dazu gehört:

11.1.1 geeignete Dokumentation über Sicherheitsvorkehrungen (in der Sprache des Landes, aus der die Arbeit von BT stammt) aufzubewahren zur Gewährleistung, dass dies den besten Industriestandards entspricht;

11.1.2 die Gelegenheiten, dass unbefugte Personen (z.B. Hacker) Zugang zu BT-Systemen und -Daten, Netzwerken oder Lieferungen und Leistungen erhalten, so gering wie möglich zu halten und

11.1.3 das Risiko, BT-Systeme, -Daten, -Netzwerke oder -Leistungen zu missbrauchen und so möglicherweise Verluste an Einnahmen oder Leistungen zu verursachen, so gering wie möglich zu halten.

11.2 Der Auftragnehmer hat auf Verlangen darzulegen, dass Soft- oder Hardware, die der Auftragnehmer herstellt und an BT liefert (eigene Soft- oder Hardware des Auftragnehmers oder Standardware) den mit BT vereinbarten Lieferungen entspricht. Der Auftragnehmer hat die hergestellten Waren vollständig zu halten, einschließlich Upgrades, Betriebssysteme und Anwendungen von Anfang bis Ende.

11.3 Der Auftragnehmer hat dafür zu sorgen, dass die Entwicklung von Systemen, die von BT genutzt werden oder die Herstellung und Wartung von BT-eigener Hardware BT-Sicherheitsanforderungen für IT standhält, wenn sie durch das operative Team von BT geliefert wird oder nach den besten Industriestandards entwickelt wurde.

11.4 Der Auftragnehmer hat dafür zu sorgen, dass Systeme und Verfahren, die für Tests und Entwicklungsaktivitäten verwendet werden, von Produktionssystemen abgetrennt werden. Für die Umsetzung von Codes in die Produktionsumgebung ist eine Kontrollverfahren zu verwenden. Testdaten, die von BT bereitgestellt werden sind nach einer vom Eigentümer der BT-Daten festgelegten Zeit zu löschen. Echtzeitdaten oder Produktionsdaten dürfen nicht in Entwicklungs- oder Testumgebungen verwendet werden.

11.5 Alle kritischen Sicherheitsschwachstellen, die in Sicherheitstests auftreten und als mittleres oder höheres Risiko eingestuft werden, sind vor Veröffentlichung zu beheben. Sicherheitsschwachstellen bei Leistungen, die von BT oder dem Auftragnehmer festgestellt werden, sind auf Kosten des Auftragnehmers zu beheben innerhalb eines zumutbaren, von BT verlangten Zeitrahmens.

11.6 Die Leistungen sind unabhängigen Penetrationstests zu unterziehen, die der Auftragnehmer auf eigene Kosten vor Veröffentlichung in Auftrag gibt, mindestens einmal pro Jahr und im Anschluss an größere Änderungen oder Vorfälle.

11.7 Lieferungen und Leistungen, die zur Verwendung durch BT oder deren Kunden entwickelt werden, sind nach dokumentierten und anerkannten Industriestandards des Secure Development LifeCycle (SDLC) zu entwickeln, um das Risiko des Auftretens von Sicherheitsschwachstellen in der Produktionsumgebung und/oder bei Kunden so gering wie möglich zu halten. SDLC hat folgende Tore zu enthalten mit greifbaren Ergebnissen aus jeder Prüfung und zur Untersuchung durch BT innerhalb des Prüfungsrahmens nach Paragraph 5 in Teil 3 der vorliegenden Sicherheitsanforderungen:

11.7.1 Sicherheitsüberprüfung der Geschäftsanforderungen;

11.7.2 Sicherheitsüberprüfung des Designs;

11.7.3 Sicherheitsüberprüfung des Quellcodes - automatisch und/oder manuell; und

11.7.4 Sicherheitsaudit der Lösung vor deren Einsatz (simulierte Angriffe eingeschlossen) nach einem dokumentierten, projektspezifischen Auditplan auf der Grundlage der Berichte aus Sicherheitsprüfungen zu Geschäftsanforderungen, Design und Code.

Weitere Orientierungshilfen sind unter Industriestandards für Dritte unter ‘Sichere Codierung' zu finden:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm

12 ANDERKONTO

Bestimmungen hierzu finden sich jetzt im Hauptvertrag.

13 ZUGANG ZU BT-SYSTEMEN

Die Einhaltung der Bestimmungen in diesem Abschnitt ist erforderlich, wenn Mitarbeiter des Auftragnehmers zur Auftragserfüllung Zugang zu BT-Systemen benötigen.

13.1 BT hat das Recht, nach eigenem Ermessen, beschränkten Zugang zu gewähren soweit dies für die Auftragserfüllung absolut notwendig ist.

13.2 In Bezug auf den Zugang hat der Auftragnehmer alle Bestimmungen, Standards und Anweisungen von BT einzuhalten und sicherzustellen, dass er selbst (und alle Mitarbeiter):

13.2.1 garantieren, dass Nutzeridentifikation, Passwörter, PIN, Tokens und Zugangsschlüssel für Konferenzen persönliche Daten einzelner Mitarbeiter sind und nicht gemeinsam benutzt werden dürfen. Angaben sind sicher und getrennt von dem Gerät zu speichern, das zum Zugang verwendet wird. Erhält eine andere Person Kenntnis eines Passworts, ist dieses unverzüglich zu ändern;

13.2.2 auf begründetes Verlangen von BT Berichte zu Mitarbeitern mit Zugangsberechtigung zu BT-Systemen zu übergeben;

13.2.3 Domain übergreifende Verbindung zu BT-Systemen ist nur zulässig bei besonderer Genehmigung durch den BT-Sicherheitsbeauftragten;

13.2.4 alle zumutbaren Anstrengungen zu unternehmen, um sicherzustellen, dass keine Viren oder schädliche Codes (diese Begriffe werden nach dem allgemeinen Verständnis in der Computerindustrie verwandt) in Systeme gelangen, um Risiken der Verletzung von BT-Systemen oder Daten auf jegliche Art und Weise so gering wie möglich zu halten und

13.2.5 zumutbare Anstrengungen zu unternehmen, um sicherzustellen, dass Dateien mit Informationen, Daten oder Medien, die für die Auftragserfüllung nicht relevant sind, nicht auf BT-Anlagen, -Servern, von BT zur Verfügung gestellten Laptops und Desktops, BT- Speicherzentralen oder BT-Systemen gespeichert werden.

13.2.6 Ermöglicht BT dem Auftragnehmer Zugang zum Internet oder zum BT-Intranet, hat der Auftragnehmer dafür zu sorgen, dass Mitarbeiter den Zugang nur ordnungsgemäß nutzen sollen, der Zugang nur im Rahmen der entsprechenden Lieferungen und Leistungen erfolgen soll und der Nutzer unangemessene oder gefährliche Seiten sperren muss. Der Auftragnehmer hat für zu sorgen, dass Mitarbeiter mindestens einmal pro Jahr eine Orientierungshilfe zu Missbrauch im Internet und bei E-Mail erhalten. Die Orientierungshilfe hat vorzuschreiben, dass

13.2.6.1 Nutzer:

(i) keine beleidigenden, sexuellen, sexistischen, rassistischen oder politischen Inhalte abrufen,
(ii) keine Aktionen ausführen, die BT oder einzelne Personen in Verruf bringen können,
(iii) kein privates Unternehmen führen dürfen,
(iv) (d) keine Urheberrechte verletzten dürfen oder
(v) Firewalls oder sonstige Sicherheitsmechanismen von BT umgehen oder untergraben dürfen,

13.2.6.2 Mitarbeiter dürfen keine Beiträge zu Seiten leisten oder online-Stellungnahmen veröffentlichen, die als Standpunkte von BT verstanden werden können.

13.3 Der Auftragnehmer hat regelmäßige Überprüfungen durchzuführen, um sicherzustellen, dass Zugänge zur Aufgabenerfüllung verlangt werden. Kopien von Prüfdokumenten sind der Kontrolle durch BT im Rahmen des in Paragraph 5.1 enthaltenen Prüfungsrahmens zur Verfügung zu stellen.

13.4 Der Auftragnehmer hat BT unverzüglich, spätestens jedoch innerhalb von 5 Werktagen zu benachrichtigen, wenn Arbeitnehmer, einschließlich Auftragnehmer, befristet beschäftigte Arbeitnehmer und Leiharbeitnehmer keinen Zugang mehr zu BT-Systemen benötigten, zum Beispiel wenn sie das Unternehmen verlassen oder andere Stellen besetzen.

14 ZUGANG ZU BT-DATEN IN SYSTEMEN DES AUFTRAGNEHMERS

Die Einhaltung der Bestimmungen in diesem Abschnitt ist erforderlich, wenn BT-Daten in Systemen des Auftragnehmers gespeichert oder verarbeitet werden.

14.1 Der Auftragnehmer ist verantwortlich für den Zugang von Mitarbeitern zu Systemen des Auftragnehmers zum Zweck der Durchführung von Lieferungen und/oder Leistungen (einschließlich, aber nicht beschränkt auf die Verwendung von einzigen Nutzeridentifikation, Passwortmanagement und klare Prüfpfade/ Prüfprotokolle für alle Tätigkeiten von Mitarbeitern)

14.2 Der Auftragnehmer hat Systeme vorzuhalten, die Beschädigungs-, Veränderungs- oder unbefugten Zugangsversuche an BT-Daten in Systemen des Auftragnehmers feststellen und aufzeichnen. Beispiele einschließlich, aber nicht beschränkt auf Verfahren zu Systemlogging und Audits, IDS und IPS etc.

14.3 Der Auftragnehmer hat Kontrollen durchzuführen, um Schadsoftware, Viren und schädliche Codes auf seinen Systemen festzustellen und es gegen solche Bedrohungen zu schützen und er hat dafür zu sorgen, dass geeignete Nutzersensibilisierungsverfahren eingerichtet werden.

14.4 Der Auftragnehmer hat dafür zu sorgen, dass mindestens einmal pro Monat nicht genehmigte Software in Systemen des Auftragnehmers, die BT-Daten enthält, verarbeitet oder auf solche zugreift, festgestellt und von diesen entfernt wird.

14.5 Der Auftragnehmer hat dafür zu sorgen, dass Zugang zu Diagnose- und Managementports sowie Diagnosetools sicher gesteuert werden.

14.6 Der Auftragnehmer hat dafür zu sorgen, dass der Zugang zu eigenen Audittools auf Mitarbeiter beschränkt wird und deren Verwendung überwacht wird.

14.7 Der Auftragnehmer hat dafür zu sorgen, dass ein unabhängiges Team Code-Überprüfungen und Penetrationstests an jeder intern produzierten Software (einschließlich sämtlicher Software), die zur Verarbeitung von BT-Daten verwendet wird, durchführt, wobei dem Team Entwickler der Software nicht angehören dürfen.

14.8 Soweit Server eingesetzt werden, um Lieferungen und Leistungen zu erbringen, dürfen diese nicht ohne geeignete Sicherheitskontrolle in nicht vertrauenswürdigen Netzwerken eingesetzt werden (Netzwerke außerhalb der Sicherheitszone des Auftraggebers, die unter dessen Verwaltungskontrolle, z.B. Internetverbindung).

14.9 Der Auftragnehmer hat dafür zu sorgen, dass Veränderungen an einzelnen Systemen des Auftragnehmers, die BT-Daten enthalten oder verarbeiten und/oder zur Auftragserfüllung verwendet werden, überwacht werden und formellen Änderungsverfahren unterliegen.

14.10 Der Auftragnehmer hat sicherzustellen, dass alle Systemuhren und -zeiten synchronisiert sind und die neueste Version des NTP oder eine ähnliche Zeitsynchronisierungs-Technologie verwenden.

14.11 Liefert der Auftragnehmer Systeme, die Online-Zugänge für BT-Kunden bereitstellen:

14.11.1 Online-Zugangsdaten für BT-Kunden müssen mindestens folgende Elemente enthalten:

14.11.1.1 Benutzername;

14.11.1.2 Online-Passwort;

14.11.1.3 drei Fragen und Antworten zur Authentifizierung für den Kontozugang; und

14.11.1.4 eine alternative Kontaktmöglichkeit zur Authentifizierung.

14.11.2 Der BT-Kunde muss einen eigenen Benutzernamen für Online-Zugangsdaten wählen können, wobei das Online-Passwort nicht den eigenen Benutzernamen enthalten darf.

14.11.3 Das Online-Passwort von BT-Kunden muss eine Mindestlänge von 8 Zeichen haben und mindestens 1 Zeichen aus jeder der folgenden 3 Zeichengruppen enthalten: (i) Ziffer (0-9), (ii) Großbuchstabe (A-Z), (iii) Kleinbuchstabe (a-z) (iv) Sonderzeichen

14.11.4 Zur Änderung des Online-Passworts hat der BT-Kunde das aktuelle Passwort einzugeben und anschließend zweimal das neue Passwort.

14.11.5 Hat ein BT-Kunde seinen Benutzernamen oder sein Passwort vergessen, hat das System des Auftragnehmers eine E-Mail zu erzeugen und an die registrierte E-Mail-Adresse des BT-Kunden zu senden mit einem Link, der den Benutzernamen oder das Passwort nach erfolgreichem Ausfüllen des Online-Formulars mit folgenden Angaben zurücksetzt:

14.11.5.1 MSISDN oder Festnetznummer

14.11.5.2 Online-Passwort

14.11.5.3 Benutzername des BT-Kunden

14.11.6 Der Link zum Zurücksetzen des Passworts darf maximal 30 Minuten gültig sein, anschließend verfällt der Link und der Kunde hat eine neue Anfrage für Passwort-Zurücksetzung durchzuführen.

14.11.7 Wird das Passwort erfolgreich zurückgesetzt, muss der Kunde das Passwort gegen ein neues Passwort austauschen.

14.11.8 Hat der BT-Kunde sowohl den Benutzernamen als auch das Online-Passwort vergessen, sind die Zugangsdaten des Kunden wiederherzustellen. Hierzu ist eine E-Mail zu erzeugen und an die registrierte E-Mail-Adresse zu versenden mit einem Link, der den Benutzernamen und das Passwort nach erfolgreichem Ausfüllen des Vor- und Nachnamens, Telefonnummer und E-Mail-Adresse des BT-Kunden.

14.11.9 Je nach Sensibilität der Daten und Funktionen, auf die zugegriffen werden soll, können zusätzliche Authentifizierungsschritte eingerichtet werden.

15 HOSTING VON BT-DATEN DURCH DEN AUFTRAGNEHMER

Die Einhaltung der Bestimmungen in diesem Abschnitt ist erforderlich, wenn der Auftragnehmer BT-Daten, die als "vertraulich" oder "streng vertraulich" eingestuft werden, extern hostet, in einer Cloud oder in Servern des Auftragnehmers oder von Subunternehmern.

15.1 Der Auftragnehmer hat in Bezug auf die Lieferungen und Leistungen dafür zu sorgen, dass Umgebungen, in denen BT-Daten gehostet werden, die mit nachfolgendem Link aufrufbaren Anforderungen für externes Datenhosting durch Dritte einhalten:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

16 NETZWERKSICHERHEIT

Die Einhaltung der Bestimmungen in diesem Abschnitt ist erforderlich, wenn der Auftragnehmer BT-Netzwerke oder Netzwerkkomponenten erstellt, entwickelt oder unterstützt.

16.1 Der Auftragnehmer hat in Bezug auf Lieferungen und Leistungen an allen gelieferten Komponenten Sicherheitsmaßnahmen einzurichten, um die Vertraulichkeit, Verfügbarkeit und Vollständigkeit der BT-Netzwerke und/oder 21CN-Anlagen zu garantieren. Der Auftragnehmer hat BT die vollständigen Unterlagen in Bezug auf die Einrichtung von Netzwerksicherheit für die Lieferungen und Leistungen zu übergeben und dafür zu sorgen, dass:

16.1.1 die gesamte Netzwerksicherheit in seiner Verantwortung den gesetzlichen und aufsichtsrechtlichen Anforderungen entspricht und

16.1.2 der Auftragnehmer sein Bestes tut, unbefugte Personen (z.B. Hacker) davon abzuhalten, Zugang zu Elementen des Netzwerkmanagements oder sonstigen Elementen über die BT-Netzwerke und/oder 21CN zu erhalten und

16.1.3 der Auftragnehmer sein Bestes tut, das Missbrauchsrisiko von BT-Netzwerken und/oder 21CN durch zugangsberechtigte Personen zu reduzieren, wodurch Verluste bei Einnahmen oder Leistungen entstehen können und

16.1.4 der Auftragnehmer sein Bestes tut, mögliche Sicherheitsverstöße festzustellen und diese schnell zu korrigieren, sowie festzustellen, welche Personen auf welche Weise Zugang erhalten haben und

16.1.5 die Gefahr der Fehlkonfiguration von BT-Netzwerken zu verringern, zum Beispiel durch die Vergabe von möglichst wenig Genehmigungen zur Vertragserfüllung.

16.2 Der Auftragnehmer hat alles zu unternehmen, sämtliche Schnittstellen bei Lieferungen und/oder Leistungen zu sichern und darf nicht voraussetzen, dass gelieferte Komponenten in einer sicheren Umgebung bedient werden.

16.3 Der Auftragnehmer hat dem BT-Sicherheitsbeauftragten Namen, Adressen (und sonstige Angaben auf Anfrage von BT) der einzelnen Mitarbeiter mitzuteilen, die gelegentlich direkt an Einsatz, Wartung und/oder Management der Lieferungen und Leistungen beteiligt sind bevor diese Aufgaben tatsächlich ausgeführt werden.

16.4 Hinsichtlich unterstützender Aktivitäten in Großbritannien hat der Auftragnehmer ein ausgebildetes Sicherheitsteam mit mindestens einem britischen Staatsangehörigen vorzuhalten, der die Verbindung zum BT-Sicherheitsbeauftragten (der seiner Vertreter) herstellt. Das Team hat an den gelegentlich vom BT-Sicherheitsbeauftragten anzuberaumenden Besprechungen teilzunehmen.

16.5 Der Auftragnehmer hat dem BT-Sicherheitsbeauftragten eine (gelegentlich zu aktualisierende) Übersicht aller aktiven Komponenten der Lieferungen und/oder Leistungen und die entsprechenden Quellen zu übergeben.

16.6 Der Auftragnehmer hat Angaben zur Person mitzuteilen, die in Verbindung mit dem Team des BT-Schwachstellenmanagement (CERT) steht zwecks Besprechung von durch BT und dem Auftragnehmer festgestellten Sicherheitslücken bei Lieferungen und/oder Leistungen. Der Auftragnehmer hat BT zeitnah Informationen zu Schwachstellen zu übermitteln und (auf eigene Kosten) nach Mitteilung durch den BT-Sicherheitsbeauftragten die Anforderungen zu Schwachstellen zu erfüllen. Der Auftragnehmer hat BT sämtliche Schwachstellen so zeitnah mitzuteilen, dass Kontrollen angewandt oder eingerichtet werden können, die diese entschärfen bevor der Auftragnehmer damit an die Öffentlichkeit geht.

16.7 Der Auftragnehmer hat dem BT-Sicherheitsbeauftragten und seinen Vertretern von Zeit zu Zeit unbeschränkt Zugang zu allen Betriebseinrichtungen zu gewähren, in denen Lieferungen und Leistungen entwickelt, hergestellt oder geschaffen werden, um die Einhaltung von Sicherheitsbestimmungen zu überprüfen und zu bewerten, wobei der Auftragnehmer zur Mitarbeit verpflichtet ist (und dafür zu sorgen hat, dass alle Mitarbeiter sich kooperativ verhalten).

16.8 Der Auftragnehmer hat dafür zu sorgen, dass sicherheitsrelevante Komponenten der Lieferungen und Leistungen wie sie von oder gegenüber BT von Zeit zu Zeit näher bezeichnet werden, auf eigene Kosten durch Dritte bewertet werden.

16.9 Hinsichtlich von Daten, die von BT übergeben oder erhalten werden und als "**STRENG VERTRAULICH**" eingestuft werden oder leicht als vertraulich verstanden werden können, hat der Auftragnehmer sicherzustellen, dass:

16.9.1 nur besonders von BT befugte Mitarbeiter Zugriff erhalten, um diese einzusehen und zu bearbeiten, und solche Zugriffe aufgezeichnet werden;

16.9.2 Daten sehr vorsichtig bearbeitet, verwendet und gespeichert werden und vor Speicherung mit PGP oder WinZip 9 verschlüsselt werden, so dass sie vorsätzlichen Schädigungen widerstehen (z.B. Verwendung sehr starker Verschlüsselungslogarithmen / starker Passwörter) und eine vollendete oder versuchte Schädigung leicht festzustellen ist;

16.9.3 bei Übertragungen entsprechende Sicherheitsvorkehrungen getroffen werden durch Verschlüsselung mit Secure Email, PGP oder WinZip 9 und

16.9.4 Daten ohne schriftliche Genehmigung von BT nicht außerhalb des Europäischen Wirtschaftsraums exportiert werden.

16.10 Der Auftragnehmer hat unverzüglich, spätestens innerhalb von 7 Werktagen dem BT-Sicherheitsbeauftragten alle Einzelheiten zu Mechanismen und/oder Funktionen von Lieferungen und Leistungen (oder der Planungen) mitzuteilen, die:

16.10.1 der Auftragnehmer kennt oder

16.10.2 von denen der BT-Sicherheitsbeauftragte annimmt und dies dem Auftragnehmer mitteilt, dass sie entworfen wurden oder dazu benutzt werden können, Telekommunikationsverkehr rechtmäßig oder in sonstiger Weise zu überwachen. Die Einzelheiten umfassen alle Daten, die erforderlich sind, den BT-Sicherheitsbeauftragten in die Lage zu versetzen, die Art, Zusammensetzung und Reichweite der Mechanismen und/oder Funktionen zu verstehen.

16.11 Zur Aufrechterhaltung des Zugangs zu BT-Netzwerken und/oder -Systemen hat der Auftragnehmer BT unverzüglich über Änderungen seiner Zugangsmethoden über Firewalls, einschließlich Netzwerkadressübersetzung zu unterrichten.

16.12 Der Auftragnehmer ist nicht berechtigt, Instrumente zur Netzwerküberwachung einzusetzen, mit denen Anwendungsinformationen eingesehen werden können.

16.13 Der Auftragnehmer hat dafür zu sorgen, dass die Funktion IPv6 in Betriebssystemen an Hosts deaktiviert wird (zum Beispiel Endgeräte oder Server), die mit dem BT-Netzwerk verbunden sind und dass Domains deaktiviert werden, wenn sie nicht benötigt werden.

16.14 Der Auftragnehmer hat die anwendbaren BT-Standards und Sicherheitsanforderungen einzuhalten und für deren Einhaltung bei Lieferungen und Leistungen zu sorgen. Jede Nichteinhaltung ist bei Unterzeichnung des Vertrags zu vereinbaren oder im Wege eines Änderungsprozesses (oder ähnlichem Verfahren).

16.15 Der Auftragnehmer hat dafür zu sorgen, dass alle Mitarbeiter eine geeignete Zuverlässigkeitsprüfung vorweisen, entsprechend der Zugangsstufe für Daten unter https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

Auftragnehmer, die BT-Netzwerke oder Netzwerkanlagen errichten, entwickeln oder unterstützen, haben dafür zu sorgen, dass alle Mitarbeiter mindestens eine L2-Zuverlässigkeitsprüfung vorweisen. L3-Zuverlässigkeitsprüfungen sind für Funktionen erforderlich, die der BT-Sicherheitsbeauftragte bestimmt. Ist der Auftragnehmer nicht in der Lage, eine Sicherheitsüberprüfung von Mitarbeitern als Teil der L3-Prüfung zu erhalten, wird BT auf Kosten des Auftragnehmers bei der Überprüfung behilflich sein.

16.16 Der Auftragnehmer hat Hard- und Software nach den Angaben der Hersteller zu warten.

16.17 Der Auftragnehmer ist nicht berechtigt, auswechselbare Datenträger (Festplatten, USB-Laufwerke etc.), die für Support und Wartung eingesetzt werden, für andere Zwecke zu benutzen.

17 NETZWERKSICHERHEIT DES AUFTRAGNEHMERS

Die Einhaltung der Bestimmungen in diesem Abschnitt ist erforderlich, wenn das Netzwerk des Auftragnehmers zur Leistungserbringung verwendet wird (einschließlich LAN, WAN, Internet, Wireless- und Radionetze).

17.1 Der Auftragnehmer hat in Bezug auf Lieferungen und Leistungen an allen Netzwerken Sicherheitsmaßnahmen einzurichten, um die Vertraulichkeit, Verfügbarkeit und Vollständigkeit von BT-Daten zu garantieren. Für Maßnahmen und Auftragnehmer gilt:

17.1.1 sie müssen alle gesetzlichen und aufsichtsrechtlichen Anforderungen erfüllen und

17.1.2 der Auftragnehmer verpflichtet sich, sein Bestes zu tun, unbefugte Personen (z.B. Hacker) davon abzuhalten, Zugang zu Netzwerken des Auftragnehmers zu erhalten;

17.1.3 der Auftragnehmer verpflichtet sich, sein Bestes zu tun, um die Gefahr des Missbrauchs seiner Netzwerke durch zugangsberechtigte Personen zu reduzieren, wodurch Verluste bei Einnahmen oder Leistungen entstehen können und

17.1.4 sein Bestes zu tun, sicherheitsrelevante Verstöße festzustellen und schnelle Korrekturen zu garantieren, sowie festzustellen, welche Personen auf welche Weise Zugang erhalten haben.

17.2 Es sind geeignete Maßnahmen zu ergreifen, um die Sicherheit von Komponenten zu garantieren, einschließlich, jedoch nicht beschränkt auf:

17.2.1 Verwendung eines "**gestaffelten Sicherheitskonzepts**";

17.2.2 Verwendung von Kontrollen, die vorsätzliche Angriffe verhindern;

17.2.3 Verwendung von Firewalls, Routern, Schaltern;

17.2.4 sichere Kommunikation zwischen Geräten und Managementstationen;

17.2.5 sichere Kommunikation unter Geräten, einschließlich Verschlüsselung aller Administrator-Zugänge über Betriebssysteme;

17.2.6 klare Architektur, die abgestuft und in Bereiche unterteilt ist mit solidem Identitätsmanagement und Betriebssystem , dessen Konfiguration entsprechend stark und dokumentiert sein muss;

17.2.7 Deaktivierung (falls möglich) von Leistungen, Anwendungen und Schnittstellen, die nicht benutzt werden.

17.2.8 Deaktivierung und Löschung von Besucherkonten.

17.2.9 Einrichtung der neuesten Sicherheitspatches auf dem(den) Netzwerk(en) und System(en) des Auftragnehmers sobald als möglich im Anschluss an entsprechende Tests. Alle Ausnahmen sind BT mitzuteilen, die das Risiko der Ausnahmen bewertet. BT behält sich vor, den Auftragnehmer zur Einrichtung von Sicherheitspatches im Anschluss an eine Risikobewertung zu verpflichten;

17.2.10 Vermeidung von Vertrauensbeziehungen zwischen Servern;

17.2.11 Verwendung des Prinzips "**geringste Rechte**" für beste Sicherheitspraktiken bei Ausführung einer Funktion;

17.2.12 Anwendung geeigneter Maßnahmen im Umgang mit Dienstverweigerungen;

17.2.13 Anwendung geeigneter Maßnahmen bei Einbruchmeldung und/oder zum Einbruchschutz;

17.2.14 Überwachung von Anbietern und sonstigen Informationsquellen in Bezug auf Warnmeldungen zu Schwachstellen;

17.2.15 bei Bedarf Durchführung von Identitätsüberwachung zur Feststellung von zugefügten, veränderten oder entfernten kritischen Systemdateien oder Daten; und

17.2.16 Änderung aller Standardpasswörter und Passwörter von Anbietern bevor Netzwerkkomponenten in Betrieb gehen.

18 CLOUDSICHERHEIT

Die Einhaltung der Bestimmungen in diesem Abschnitt ist erforderlich, wenn der Auftragnehmer Cloud-Leistungen für BT erbringt.

18.1 Der Auftragnehmer hat folgende Bestimmungen einzuhalten:

die neueste Version der Cloud Security Alliance Cloud Controls Matrix (CCM); Anforderungen von BT an externe Host-Sicherheit sind einzusehen unter: https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm Bei Vereinbarungen über Netzwerk- und Infrastrukturdienste (als interne oder ausgelagerte Dienste) sind Sicherheitskontrollen, Kapazitäts- und Leistungsstufen, Geschäfts- oder Kundenforderungen eindeutig zu dokumentieren.

18.2 Der Auftragnehmer hat Sicherheitsmaßnahmen in allen gelieferten Komponenten so auszuführen, dass die Vertraulichkeit, Verfügbarkeit, Qualität und Vollständigkeit der Auftragsleistungen gewahrt werden, wobei Gelegenheiten für unbefugte Personen auf BT-Daten und BT-Leistungen zugreifen zu können, möglichst gering zu halten sind.

19 KONTAKTZENTRUM

Die Einhaltung der Bestimmungen in diesem Abschnitt ist erforderlich, wenn der Auftragnehmer ein Kontaktzentrum für BT liefert.

19.1 Der Auftragnehmer hat in Bezug auf die Auftragserfüllung sicherzustellen, dass Umgebungen, in denen BT-Daten gespeichert, verarbeitet oder eingesehen werden, den aktuellen Fassungen der Standards für Dritte in Kontaktzentren entsprechen. Diese sind einzusehen unter:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

TEIL 5: DEFINITIONEN

In vorliegenden Sicherheitsanforderungen sind die folgenden Definitionen zu verwenden, im Übrigen sind die Bestimmungen des Vertrags anwendbar und alle Begriffe und Ausdrücke in den Sicherheitsanforderungen haben die gleiche Bedeutung wie im Vertrag:

"**Zugang"/"Zugriff**" – Verarbeitung, Handhabung oder Speicherung von BT-Daten in einer oder mehrerer der nachfolgend genannten Formen:

- Durch Verbindung mit BT-Systemen
- Durch Übergabe in Papier oder anderen nicht elektronischen Formaten
- BT-Daten auf Systemen von Auftragnehmern
- durch mobile Medien

und/oder Zugang zu Geschäftsräumen von BT zwecks Lieferung, ausgenommen bei Lieferung von Hardware und Besprechungen).

"**Genehmigt**" - BT hat Zugriffsberechtigung als Teil des BT System Interconnect - Verfahrens oder erhält eine schriftliche Genehmigung des Sicherheitsbeauftragten von BT. "**Genehmigung**" ist entsprechend zu verwenden. Die vergebene Zugangsberechtigungsstufe ist abhängig von und beschränkt auf die Anforderungen an die Lieferungen.

"**BT-Verwaltungssysteme**" – Plattform zur Rechnungsstellung von BT (derzeit iSupplier), oder sonstige reine Verwaltungssysteme, in Abstimmung mit BT;

"BT-Kunde" – umfasst im Sinne der vorliegenden Sicherheitsanforderungen juristische und natürliche Personen, die von BT Waren oder Dienstleistungen erhalten.

"**BT Daten**" – sämtliche Daten in Bezug auf BT oder einen Kunden von BT, die dem Auftragnehmer übergeben werden und sämtliche Daten, die der Auftragnehmer im Namen von BT oder eines Kunden von BT im Rahmen des Vertrags verarbeitet oder behandelt.

"**BT Netzwerke**" - das Netzwerk, das unter der Kontrolle oder Verwaltung von BT steht.

"**BT Sachwerte**" - alle Sachwerte beim Auftragnehmer (einschließlich, aber nicht beschränkt auf Router, Schalter, Schlüssel für Serverschränke, Laptop Tokens, Zugangskarten, Pläne oder Dokumente) im Eigentum von BT.

"**BT-Sicherheit**" - die interne Sicherheitsorganisation von BT.

"**BT-Sicherheitsbeauftragter**" – der interne Mitarbeiter für Datensicherheit bei BT- Sicherheit oder ein kaufmännischer Mitarbeiter bei BT, der bei Benachrichtigung des Auftragnehmers oder der Sicherheitszentrale 0800 321999 [+44 1908 641100] als einzige Anlaufstelle für Angelegenheiten in Zusammenhang mit Sicherheitsanforderungen oder sicherheitsrelevanten Zwischenfällen zur Verfügung steht.

"**BT-Systeme**" – Service und Servicekomponenten, Produkte, Netzwerke, Server, Verfahren, papiergestützte oder IT-Systeme (insgesamt oder Teile hiervon), die BT gehören und/oder von BT betrieben werden oder sonstige Systeme, die in Räumlichkeiten von BT beherbergt werden, einschließlich iSupplier (gemäß Definition in den Bestimmungen "**Zahlung und Rechnungstellung**").

"**Massenaufzeichnungen**" – bedeutet über 1000 Einzelaufzeichnungen von BT-Daten, die als vertraulich eingestuft werden, oder 100 Einzelaufzeichnungen von BT-Daten, die als streng vertraulich eingestuft werden.

"**CCTV**" - Videoüberwachung.

"**Mitarbeiter**", "**Zuständige Mitarbeiter**" - wie im Vertrag definiert.

"**Cyber Essentials Plus**" – ist ein Förderprogramm der Regierung Großbritanniens zur Unterstützung von Organisationen, sich selbst gegen gängige Cyberangriffe zu schützen, derzeit erhältlich unter https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

"**Gute Sicherheitspraktiken**" – sind in Bezug auf alle Unternehmungen und Umstände die Sicherheitspraktiken, -bestimmungen, -standards und -instrumente, die zumutbar und gewöhnlich von einer ausgebildeten und erfahrenen Person bei gleichen Aktivitäten unter den gleichen oder ähnlichen Umständen erwartet werden.

"**Information / Daten"** – Materielle oder in sonstiger Form vorhandene Daten, einschließlich und ohne Beschränkung Spezifikationen, Berichte, Daten, Notizen, Dokumente, Entwürfe, Software, Computerausgaben, Zeichnungen, Schaltpläne, Modelle, Muster, Proben, Erfindungen (unabhängig von ihrer Patentierbarkeit) und Know-how, sowie (gegebenenfalls) das Medium, auf dem derartige Daten enthalten sind.

"**Intern**", "**Öffentlich**", "**Vertraulich**" und "**Streng Vertraulich**" – haben die Bedeutungen wie sie in den Bestimmungen zur Klassifizierung von Informationen Dritter und den Abwicklungsspezifikationen enthalten sind.

"**ISO 27001**" – die aktuelle Fassung des internationalen Standards für Informationssicherheits-Managementsysteme der Internationalen Organisation für Normung und der Internationalen Elektrotechnischen Kommission.
"**Vermögenswerte des Netzes**" - Gerät oder Komponente des BT-Netzwerks zur Unterstützung von Netzwerkaktivitäten.
"**Netzwerksicherheit**" - die Sicherheit von Verbindungen von Kommunikationswegen und -knoten, die Anwendertechnologien logisch untereinander und mit Managementsystemen verknüpfen.
"**Verfahren**", "**Verarbeitet**" oder "**Abwicklung**" "**Verfahrensanhang**" und "**personenbezogene Daten**" - haben die Bedeutungen, wie sie in den Bestimmungen mit der Überschrift "**Schutz von persönlichen Daten**" enthalten sind.
"**Sicherheitsrelevanter Zwischenfall**" - eine festgestellte oder vermutete Sicherheitsschwachstelle in System oder Service und sicherheitsrelevante Ereignisse, die die vertragsgemäße Lieferung oder Durchführung berührt (einschließlich tatsächlicher oder vermuteter Verlust, Schaden, Diebstahl oder Missbrauch von BT-Daten oder BT-Systemen), einschließlich, jedoch nicht beschränkt auf:

- Leistungsausfall, Verlust von Geräten oder Einrichtungen;
- Korruption, Beschädigung oder Missbrauch von BT-Sachwerten;
- Systemstörungen oder -überlastungen;
- menschliches Versagen;
- Nichterfüllung der im vorliegenden Dokument enthaltenen Sicherheitsanforderungen;
- Verstoß gegen Sicherheitsvorkehrungen;
- unkontrollierte Systemveränderungen;
- Störungen der Soft- oder Hardware;
- Zugriffsverletzungen und
- festgestellte oder vermutete Datenverluste bei BT zugehörigen Systemen und Verbindung(en) zwischen BT und Auftragnehmer.

"**Remote-Zugriff**" - Zugriff aus der Ferne von zu Hause oder einem anderen Ort über ein öffentliches Netzwerk (z.B. Internet) oder bei Zugriff des Auftragnehmernetzwerks in ein BT-System aus der Ferne.
"**Sicherheitsanforderungen**" - sind die vorliegenden und von Zeit zu Zeit aktualisierten BT-Sicherheitsanforderungen.
"**Leistungen und Lieferungen**" – sind sämtliche "**Dienstleistungen**", "**Lieferungen**", "**Waren**" und "**Arbeiten**" nach den Definitionen im Vertrag und dessen Ausführung.
"**Systeme des Auftragnehmers**" – Computer-, Anwendungs- oder Netzwerksysteme im Eigentum des Auftragnehmers, die für den Zugriff, die Speicherung oder Verarbeitung von BT-Daten oder für Leistungen zur Auftragserfüllung verwendet werden.
"**Sicherheitsbeauftragter des Auftragnehmers**" – eine Person, deren Kontaktdaten vom Auftragnehmer an BT von Zeit zu Zeit mitgeteilt werden und als einziger Ansprechpartner für Angelegenheiten in Zusammenhang mit vorliegenden Sicherheitsanforderungen und allen sicherheitsrelevanten Vorfällen zur Verfügung steht.
"**Übertragung**" oder "**Übertragen**" - Der Umzug von BT-Daten in Besitz von Mitarbeitern (einschließlich, aber nicht beschränkt auf personenbezogene Daten) von einer Stelle oder Person an einen oder eine andere, über physische, akustische oder elektronische Mittel; Gewährleistung des Zugangs zu BT-Daten in Besitz von Mitarbeitern (einschließlich, aber nicht beschränkt auf personenbezogene Daten) von einer Stelle oder Person an einen oder eine andere, über physische, akustische oder elektronische Mittel.
"**Einstufung von Daten Dritter und Handhabungsbeschreibung**" sind die Anforderungen an den Auftragnehmer zur Handhabung von Daten, beschrieben unter https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm in der jeweils aktuellen Version.