Inhalt

1. Einführung

1.1 Die Kunden von BT haben die Erwartung, dass BT und seine Drittanbieter-Lieferkette ihre Dienste unter Verwendung von branchenüblichen Verwaltungssystemen für Informationssicherheit (ISMS) bereitstellen. Das ISMS des Drittanbieters sollte Infrastruktur, Netzwerke, Ausrüstung und IT-Systeme abdecken, um bereitgestellte Dienste und BT-Kundeninformationen im Umfang der Dienstleistungen zu schützen. Dieses Dokument legt die Sicherheitsanforderungen von BT fest und gilt für alle Drittanbieter, die für oder im Namen der BT-Gruppe einschließlich Openreach, EE und Plusnet – im Rest des Dokuments als „BT“ bezeichnet. Drittanbieter werden darüber informiert, welche Sicherheitskontrollsätze für die Dienste gelten, die sie für BT erbringen.

1.2 Diese Sicherheitsanforderungen gelten zusätzlich zu und unbeschadet aller anderen Verpflichtungen des Drittanbieters im Vertrag. Sie sind dazu vorgesehen, dass BT die Kontrolle und Aufsicht über sein Netzwerk und seine Nutzerdaten behält.

2. Anforderungen für eingeschränkten Zugriff/Zugang

2.1 Unbeschadet etwaiger Geheimhaltungspflichten muss der Drittanbieter, wenn die Mitarbeiter des Drittanbieters Zugriff auf Informationen von BT haben:

2.2 sicherstellen, dass BT-Informationen nicht an die Mitarbeiter von Drittanbietern weitergegeben werden oder diese keinen Zugriff darauf erhalten, es sei denn, dies ist für die Erbringung der Dienstleistung erforderlich; und

2.3 alle technischen und organisatorischen Systeme und Prozesse bereitstellen, die erforderlich sind, um BT-Informationen (i) vor versehentlicher oder unrechtmäßiger Zerstörung und (ii) vor Verlust, Änderung, unbefugter Offenlegung von oder Zugang zu BT-Informationen gemäß den geschäftsüblichen Sicherheitspraktiken der Branche zu schützen.

3. Allgemeine Informationssicherheit

3.1 Auf entsprechende Anfrage stellt der Drittanbieter BT Kopien von Sicherheitsbescheinigungen und Konformitätserklärungen, die für den Dienst relevant sind, als Nachweis der Einhaltung dieser Sicherheitsanforderungen zur Verfügung.

3.2 Sollte es zu einer wesentlichen Änderung der Technologie oder der Industriesicherheitsstandards kommen oder es wesentliche Änderungen der Dienste oder der Art und Weise, wie sie erbracht werden, geben, kann BT während der Laufzeit eine Vertragsänderung einfordern, wenn eine Änderung der geltenden Sicherheitsanforderungen erforderlich ist. Der Drittanbieter muss die vereinbarte Vertragsänderung innerhalb eines angemessenen Zeitraums erfüllen, wobei die Art der Änderung und das Risiko für BT zu berücksichtigen sind.

3.3 Falls es wesentliche Änderungen der Dienste oder der Art und Weise, wie sie erbracht werden, gibt, muss der Drittanbieter diese Richtlinie für Sicherheitsanforderungen überprüfen, um sicherzustellen, dass sie weiterhin alle geltenden Sicherheitskontrollen erfüllen.

3.4 Wenn der Drittanbieter Verpflichtungen aus dem Vertrag an Subunternehmer vergibt, muss der Drittanbieter BT eine Liste der relevanten Subunternehmer und deren

Standorte zur Verfügung stellen und sicherstellen, dass alle Verträge mit relevanten Subunternehmern und deren Subunternehmern schriftliche Bedingungen enthalten, die den Subunternehmer verpflichten, die anwendbaren Teile entweder dieser Sicherheitsanforderungen oder gleichwertige Sicherheitsanforderungen des Drittanbieters zu erfüllen, dies schließt Auditrechte, equivalent zu Anschnitt 5, der BT ein.

3.5 Wenn ein Viertanbieter für die Erbringung der Dienste eingesetzt wird und dieser BT-Informationen speichert oder verarbeitet, muss der Drittanbieter dies zuvor von BT genehmigen lassener .. Der Drittanbieter muss sicherstellen, dass er eine vertragliche Beziehung mit dem Viertanbieter hat und dass der Viertanbieter in einem Sicherheitsrahmen nach Industriestandard arbeitet.

3.6 Die BT-Informationen dürfen so lange es notwendig ist, um den Vertrag zu erfüllen, aufbewahrt werden. Danach sollten sie nicht länger als maximal zwei Jahre aufbewahrt werden, es sei denn, es wurde eine andere Aufbewahrungsfrist zwischen BT und einem Drittanbieter vereinbart oder durch geltende Gesetze vorgeschrieben.

3.7 Wenn die Dienste direkt einen Vertrag mit der Regierung des Vereinigten Königreiches unterstützen, muss der Drittanbieter die aktuelle Version von Cyber Essentials Plus – https://www.cyberessentials.ncsc.gov.uk/ – einhalten.

3.8 Wenn BT-Informationen außerhalb des Landes verarbeitet oder gespeichert werden, muss der Drittanbieter BT über die geografischen Standorte informieren. BT behält sich das Recht vor, Standorte abzulehnen, die als hochriskant gelten.

Handhabung von BT-Informationen

3.9 Sofern vom BT-Stakeholder nicht anders angegeben, werden alle BT-Informationen als „vertraulich“ eingestuft. Wenn personenbezogene Daten oder sensible personenbezogene Daten in den Geltungsbereich fallen, sollte das Datenschutzteam des Drittanbieters um Rat gebeten werden, falls zusätzliche Regelungen erforderlich sind.

Die folgenden Sicherheitsregelungen sind „Anforderungen an die Sprachverarbeitung“, die sich auf verbale Kommunikation beschränken.

3.10 Wenn es notwendig ist, BT-Informationen über eine Kollaborationsplattform zu diskutieren, anzuzeigen oder auszutauschen (z. B. Teams):

- Stellen Sie sicher, dass nur Personen anwesend sind, die die Informationen kennen müssen.
- Wenn ein Dritter oder externer Auftragnehmer beteiligt ist, muss dieser entweder einen unterzeichneten Vertrag mit Ihnen haben oder vor Beginn der Gespräche über ein NDA verfügen.
- Der Drittanbieter muss vor Beginn der Konferenz überprüfen, wer an der Konferenz teilnimmt.

3.11 Wenn es notwendig ist, BT-Informationen mit jemandem von Angesicht zu Angesicht, über ein Mobiltelefon oder Standardtelefon zu besprechen:

- Gespräche dürfen nicht von jemandem gehalten oder gehört werden, der keine Kenntnis benötigt.

- Wenn das Gespräch mit einem externen Auftragnehmer notwendig ist, muss dieser entweder einen unterzeichneten Vertrag mit dem Drittanbieter haben oder vor Beginn der Gespräche über ein NDA verfügen.
- Vertrauliche oder streng vertrauliche Informationen dürfen nicht auf Anrufbeantwortern hinterlassen werden.

Die folgenden Sicherheitsregelungen sind „schriftliche Handhabungsanforderungen“ und umfassen Material, das im Papierformat aufbewahrt wird. Dies umfasst unter anderem handschriftliche Briefe, Protokolle, Notizen und Memos. Dazu gehören auch gedruckte elektronische Materialien wie Arbeitsdokumente und Berichte, sobald sie in Papierform vorliegen.

3.12 Wenn Kopien von BT-Informationen in Papierform in Räumlichkeiten von Drittanbietern aufbewahrt werden, müssen diese bei Nichtgebrauch in einer abschließbaren Einrichtung gesichert werden, wobei der Zugriff auf diejenigen beschränkt sein muss, die das Material ansehen müssen. Dokumente dürfen nicht unbeaufsichtigt gelassen werden.

3.13 Falls BT-Informationen gedruckt, kopiert oder dupliziert werden müssen, gelten die folgenden Sicherheitsregelungen:

- Verwenden Sie nur Druck- oder Kopiereinrichtungen in eigenen Räumlichkeiten des Drittanbieters.
- Fotokopien oder Ausdrucke dürfen am Druckort nicht unbeaufsichtigt gelassen werden und müssen zum Zeitpunkt der Erstellung abgeholt werden.
- Wenn der Drucker oder Fotokopierer über einen Speicher verfügt, aus dem kopiertes Material abgerufen und erneut gedruckt werden kann, sollte dieser so bald wie möglich neu gestartet werden, um den Speicher zu leeren.

3.14 Falls Kopien von BT-Informationen aus Räumlichkeiten von Drittanbietern entfernt werden müssen:

- Sofern nicht bereits im Rahmen des Arbeitsumfangs vereinbart, muss der Drittanbieter eine nachgewiesene Zustimmung des BT-Stakeholders einholen.
- Bei Genehmigung dürfen die Informationen während des Transports nicht identifizierbar sein und müssen in einem anonymisierten oder einfachen Ordner, einer Tasche oder einem Etui aufbewahrt werden.
- Das Material darf nicht unbeaufsichtigt gelassen werden und muss – insbesondere in öffentlichen Verkehrsmitteln – der unmittelbaren Kontrolle der Person unterliegen, die das Material transportiert.

3.15 Wenn Papierkopien der BT-Informationen nicht mehr benötigt werden, müssen diese wie folgt entsorgt werden:

- Papierkopien dürfen nicht über allgemeine Abfallbehälter entsorgt werden.
- Wenn ein Schredder verwendet wird, muss er mindestens dem Standard P4 DIN66399 entsprechen.
- Wenn zugelassene Schredder nicht verfügbar sind, müssen die Informationen in vertraulichen Abfallbehältern entsorgt werden.

Für „Streng vertrauliche Informationen“ gilt ergänzend Folgendes:

- Informationen dürfen nur nach dem Schreddern in vertraulichen Abfallbehältern entsorgt werden.
- Für Informationen, die vom Lieferanten vor Ort geschreddert werden müssen, muss vom Lieferanten ein Vernichtungszertifikat ausgestellt werden.

Die folgenden Sicherheitsregelungen beziehen sich auf BT-Informationen in elektronischem Format.

3.16 Wenn BT-Informationen auf einem PC oder Laptop von Drittanbietern gespeichert werden, gelten die folgenden Regelungen:

- Nur auf Geräten mit Festplattenverschlüsselung (z. B. Bitlocker) zulässig.
- Alle Dokumente müssen einzeln verschlüsselt werden.
- Das Information Rights Management (IRM) muss auf das Dokument angewendet werden.
- Falls mitgeteilt, müssen die Informationen die BT-Klassifizierungskennzeichnung enthalten.

3.17 Beim Speichern eines BT-Dokuments an einem internen Speicherort für die Dateifreigabe zur allgemeinen Speicherung, Zusammenarbeit oder Dateifreigabe gelten die folgenden Sicherheitsregelungen:

- Am Speicherort des Materials müssen Zugriffsberechtigungen angewendet werden, um nur Personen zuzulassen, die das Dokument sehen oder verwenden müssen.
- Falls mitgeteilt, müssen die Informationen die BT-Klassifizierungskennzeichnung enthalten.
- Alle Dokumente müssen einzeln verschlüsselt werden.
- Das Information Rights Management (IRM) muss auf das Dokument angewendet werden.
- Wenn im Rahmen der Dienstleistung PCI- und Zahlungskartenmaterial bereitgestellt wird, darf dieses zu keinem Zeitpunkt an Datenspeicherorten gespeichert werden.
- Wenn Gastzugänge einem externen Auftragnehmer für den Zugriff eingerichtet werden müssen, muss dieser entweder einen unterzeichneten Vertrag mit dem Drittanbieter haben oder vor Gewährung des Zugriffs über ein NDA verfügen.

3.18 Wenn BT-Informationen auf Wechseldatenträgern von Drittanbietern gespeichert werden müssen (z. B. ein USB-Speicherstick) gelten die folgenden Sicherheitsregelungen:

- Das Gerät muss auf dem gleichen Niveau wie die Festplatte verschlüsselt sein.
- Bei Verlust oder Diebstahl muss der Drittanbieter einen Sicherheitsvorfall melden.
- Der Drittanbieter muss die Nachweise der vorherigen Genehmigung des BT-Stakeholders haben, um „streng vertrauliches“ Material auf einen Wechseldatenträger zu übertragen.
- PCI-Material oder personenbezogene Daten dürfen im Rahmen der Dienstleistung nicht auf Wechseldatenträgern gespeichert werden.

- Geräte, die zur Unterstützung und Wartung bestimmt sind, dürfen nicht für andere Zwecke verwendet werden.

3.19 BT-Informationen dürfen nicht auf persönlichen PCs, Laptops, Wechseldatenträgern oder mobilen Geräten gespeichert werden.

3.20 BT-Informationen dürfen nicht von einer Unternehmens-E-Mail-Adresse des Drittanbieters an ein persönliches oder externes E-Mail-Konto gesendet oder automatisch weitergeleitet werden, es sei denn, es handelt sich um einen externen Auftragnehmer, der einen unterzeichneten Vertrag mit dem Drittanbieter hat oder über ein NDA verfügt und zur Erbringung der Dienstleistung verwendet wird.

3.21 Um die Angriffsfläche und die Möglichkeiten für Angreifer zu minimieren, menschliches Verhalten durch ihre Interaktion mit Webbrowsern und E-Mail-Systemen zu manipulieren, implementieren Sie Prozesse, um sicherzustellen, dass nur vollständig unterstützte Webbrowser und E-Mail-Clients erlaubt sind, und deinstallieren oder deaktivieren Sie nicht autorisierte Browser- oder E-Mail-Client-Plugins oder Add-on-Anwendungen.

3.22 Drittanbieter müssen über Sicherungsmaßnahmen verfügen, um BT-Informationen im Falle von Beschädigung, Verlust oder Verschlechterung innerhalb von 3 Arbeitstagen wiederherzustellen.

3.23 Wenn BT-Daten/-Informationen entsorgt werden, müssen vollständige Aufzeichnungen über die Aufbewahrung und Entsorgung von Daten geführt werden, die einen Prüfpfad, Nachweise und eine Nachverfolgung ermöglichen. Diese müssen beinhalten:

- Nachweis der Vernichtung und/oder Entsorgung (einschließlich des Datums und der verwendeten Methode).
- Systemprüfungsprotokolle für die Löschung.
- Zertifikate der Datenvernichtung.
- Wer die Entsorgung übernommen hat (einschließlich eventueller Entsorgungspartner/Drittanbieter oder Auftragnehmer).
- Ein Vernichtungs- und Verifizierungsbericht muss erstellt werden, um den Erfolg oder Misserfolg eines Vernichtungs-/Löschvorgangs zu bestätigen (d. h. bei einem Überschreibungsprozess muss ein Bericht erstellt werden, in dem alle Sektoren, die nicht gelöscht werden konnten, detailliert aufgeführt sind).

3.24 Bei der Entsorgung von Geräten, auf denen BT-Daten/-Informationen vorhanden waren, muss ein Prüfpfad für die folgenden Gerätetypen bereitgestellt werden:

- Wechselmedien.
- Diskettenlaufwerke.
- Backup-Bänder.
- Computer-Komponenten.

3.25 Es müssen vollständige Aufzeichnungen vorhanden sein, die mindestens einen Prüfpfad enthalten müssen:

- Der Name der Anwendung oder des Dienstes, der dieses Gerät verwendet hat.
- Art des Geräts, z. B. Desktop, Laptop, Server, Band, Router usw.
- Anzahl der Festplattenlaufwerke, die das Gerät enthält (falls zutreffend).

- Gerät, das durch die Seriennummer identifiziert wird.
- Komponenten von Geräten, die durch die Seriennummer identifiziert werden.
- Vollständige Nachverfolgung aller Geräte und Komponententeile über den gesamten Lebenszyklus der Geräteentsorgung.
- Nachweis der Vernichtung und/oder Entsorgung (einschließlich des Datums und der verwendeten Methode).
- Einzelheiten darüber, wer die Entsorgung übernommen hat (einschließlich eventueller Entsorgungspartner / Drittanbieter / Auftragnehmer für die Entsorgung).
- Ein Vernichtungs- und Verifizierungsbericht muss erstellt werden, um den Erfolg oder Misserfolg eines Recyclings-/Bereinigungs- oder Vernichtungsvorgangs zu bestätigen. Bei einem Überschreibungsprozess z. B. muss ein Bericht erstellt werden, in dem alle Sektoren, die nicht gelöscht werden konnten, detailliert aufgeführt sind. Diese Berichte haben die Kapazität, die Marke, das Modell und die Seriennummer der Medien zu enthalten.

Rollen und Verantwortlichkeiten

3.26 Alle Drittanbieter müssen die Anforderungen dieser Sicherheitsregelungen kennen und verstehen und sind dafür verantwortlich, dass alle Personen, die an der Erbringung eines Dienstes für BT beteiligt sind, mit den relevanten Anforderungen dieses Standards vertraut sind und diese erfüllen.

Governance

3.27 Der Drittanbieter muss über einen etablierten und konsistenten Industriestandard-Sicherheitsrahmen für die Informations- und Cybersicherheits-Governance verfügen, der die folgenden Komponenten umfasst:

- Angemessene Informations- und Cyber-Sicherheitsrichtlinien und -verfahren, die genehmigt und mitgeteilt werden.
- Eine Informationssicherheitsstrategie.
- Einschlägige gesetzliche und regulatorische Anforderungen in Bezug auf Informations- und Cybersicherheit (einschließlich Datenschutz), die verstanden und verwaltet werden.
- Governance- und Risikomanagementprozesse, die sich mit Informations- und Cybersicherheitsrisiken befassen.

3.28 Der Drittanbieter muss sicherstellen, dass angemessene Rollen und Verantwortlichkeiten für die Informations- und Cybersicherheit definiert und umgesetzt werden. Diese umfassen Folgendes:

- Ein in Vollzeit beschäftigter "Chief Information Security Officer" (oder in vergleichbarer Position), der eine ausreichend hochrangige Position hat und die Verantwortung für das Informationssicherheitsprogramm trägt.
- Eine hochrangige Arbeitsgruppe, ein Ausschuss oder ein gleichwertiges Gremium unter dem Vorsitz eines entsprechend hochrangigen Mitarbeiters, der die

Aktivitäten im Bereich der Informationssicherheit beim gesamten Drittanbieter koordiniert und sich regelmäßig trifft.

- Eine spezialisierte Informationssicherheitsfunktion mit geeigneten und definierten Rollen und Verantwortlichkeiten.

3.29 Der Drittanbieter muss sicherstellen, dass es eine individuelle Verantwortung für Informationen und Systeme gibt, indem er dafür sorgt, dass es ein angemessenes Eigentumsrecht an kritischen Geschäftsumgebungen, Informationen und Systemen gibt und dass diese fähigen Personen zugewiesen wird.

3.30 Der Drittanbieter muss sicherstellen, dass er BT (schriftlich) benachrichtigt, sobald er rechtlich dazu in der Lage ist, wenn der Drittanbieter Gegenstand einer Fusion, Übernahme oder eines anderen Eigentümerwechsels ist.

Incident Management (Vorfallmanagement)

3.31 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk für das Incident Management verfügen, um sicherzustellen, dass Vorfälle angemessen gehandhabt, eingedämmt und gemildert werden, und das die folgenden Komponenten umfasst:

- Sicherstellen, dass die Mitarbeiter, wenn eine Reaktion erforderlich ist, ihre Rollen und die Reihenfolge der Abläufe kennen.
- Sicherstellen, dass Vorfälle nach den festgelegten Kriterien gemeldet werden.
- Sicherstellen, dass die Auswirkungen von Vorfällen verstanden werden.
- Sicherstellen, dass die Forensik, wenn nötig, entweder intern oder durch eine Fachfunktion durchgeführt wird.
- Sicherstellen, dass die aus den Vorfällen gezogenen Lehren in die bewährten Methoden einfließen.
- Sicherstellen, dass Informationen, die sich auf einen Vorfall beziehen, der eine Auswirkung auf BT hat, als „vertraulich“ behandelt werden.

3.32 Der Drittanbieter unternimmt alle angemessenen Schritte, um sicherzustellen, dass (eine) geeignete Person(en) als Ansprechpartner für Sicherheitsrisiken, Incident Management und Compliance Management bestimmt und dafür verantwortlich gemacht wird. Der Drittanbieter teilt dem BT-Stakeholder die Kontaktdaten der Person(en) und jegliche Änderungen dieser mit.

3.33 Der Drittanbieter informiert BT per E-Mail security@bt.com oder per Telefon unter +44 0800 321 999 innerhalb eines angemessenen Zeitraums nach Bekanntwerden eines Vorfalls, der sich auf die Dienste für BT oder BT-Informationen auswirkt, auf jeden Fall aber spätestens vierundzwanzig (24) Stunden, nachdem der Vorfall dem Drittanbieter zur Kenntnis gelangt ist.

3.34 Der Drittanbieter ergreift ohne unangemessene Verzögerung angemessene und rechtzeitige Korrekturmaßnahmen, um alle Risiken und Auswirkungen im Zusammenhang mit dem Vorfall zu mindern, um die Schwere und Dauer des Vorfalls zu verringern.

3.35 Der Drittanbieter legt dem BT-Stakeholder innerhalb von 30 Tagen nach einem Vorfall einen Bericht über jeden Vorfall vor, der sich auf die Dienste für BT oder die BT-Informationen auswirkt. Dieser Bericht hat mindestens das Folgende zu beinhalten:

Datum und Uhrzeit, Art des Vorfalls, Auswirkung, Status und Ergebnis (einschließlich der Lösungsempfehlungen oder ergriffenen Maßnahmen).

3.36 Der Drittanbieter muss eine Ursachenanalyse aller Sicherheitsvorfälle durchführen. Die Ergebnisse dieser Analyse sind an die entsprechenden Managementebenen innerhalb der Organisation des Drittanbieters weiterzuleiten.

Änderungsmanagement

3.37 Der Drittanbieter muss sicherstellen, dass alle IT-Änderungen vor der Implementierung genehmigt, protokolliert und getestet werden, einschließlich der Rücknahme fehlgeschlagener Änderungen, um eine Unterbrechung des Dienstes oder Sicherheitsverletzungen zu verhindern. Der Drittanbieter muss ebenfalls sicherstellen, dass es einen Prozess für die kontrollierte Durchführung von Notfall-Updates gibt.

3.38 Der Drittanbieter muss sicherstellen, dass die Änderungen sowohl in den Produktions- als auch DR-Umgebungen berücksichtigt werden.

3.39 Der Drittanbieter muss sicherstellen, dass die Wartung und Reparatur von Anlagen des Unternehmens mit genehmigten und kontrollierten Werkzeugen durchgeführt und protokolliert werden.

3.40 Der Drittanbieter muss sicherstellen, dass die Fernwartung von Anlagen des Unternehmens genehmigt, protokolliert und so durchgeführt wird, dass ein unbefugter Zugriff verhindert wird.

Cyber-Risiko- und Bedrohungsmanagement

3.41 Der Drittanbieter muss sicherstellen, dass es ein fortlaufenden Rahmenwerk für die Bewertung von Risiken und Bedrohungen der Cybersicherheit gibt, um sicherzustellen, dass das Risikoprofil der Cybersicherheit für den Betrieb, die Anlagen, die Räumlichkeiten und die Personen des Unternehmens verstanden und verwaltet wird:

- Bewertung der Anlagenschwachstellen.
- Identifizierung von internen und externen Bedrohungen.
- Sensibilität der Informationen/Daten im Geltungsbereich.
- Abschätzung der potenziellen geschäftlichen Auswirkungen
- Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen zur Bestimmung des Risikos.
- Sicherstellen, dass das Rahmenwerk für das Management von Cyberrisiken und -bedrohungen auf einer geeigneten Ebene im Unternehmen vereinbart wird.

3.42 Der Drittanbieter muss sicherstellen, dass alle Risiken und Bedrohungen, die im Rahmen der Bewertung der Risiken und Bedrohungen der Cybersicherheit identifiziert wurden, nach Priorität geordnet und entsprechende Maßnahmen ergriffen werden, um die Risiken in einem geeigneten Zeitrahmen zu mindern.

3.43 Der Drittanbieter muss dem BT Stakeholder mitteilen, wenn er nicht in der Lage ist, wesentliche Risikobereiche, die sich auf die zu erbringende Dienste auswirken könnten, zu beheben oder zu reduzieren.

Identitätsmanagement und Zugangskontrolle

3.44 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk verfügen, um sicherzustellen, dass Identitäten und Berechtigungen von autorisierten Mitarbeitern sicher verwaltet werden:

- Gewähren, erneutes Aktivieren, Ändern und Deaktivieren von Zugriffsrechten nur auf Grundlage dokumentierter und autorisierter Genehmigungen.
- Sicherstellen, dass ruhende Konten deaktiviert werden.
- Deaktivieren der Konten von Mitarbeitern, die nicht mehr beim Unternehmen tätig sind
- Implementieren von Prozessen und Werkzeugen, um die Verwendung, Zuweisung und Konfiguration von Administratorrechten auf Computern, Netzwerken und Anwendungen zu verfolgen, zu steuern, zu verhindern und zu korrigieren.
- Regelmäßige Überprüfungen der Zugangsrechte, um sicherzustellen, dass die Zugangsrechte zweckmäßig sind.
- Bei Nutzerkonten muss mindestens einmal im Jahr und bei privilegierten Konten vierteljährlich der Zugang rezertifiziert werden.
- Sicherstellen, dass dauerhafte Anmeldeinformationen und Geheimnisse (z. B. der Zugang zu Break Glass) innerhalb eines hardwaregeschützten Speichers geschützt sind und nur im Notfall der/den verantwortlichen Person(en) zur Verfügung gestellt werden.
- Sicherstellen, dass nicht dauerhafte Anmeldeinformationen (z. B. Authentifizierung mit Benutzername und Passwort) in einem zentralisierten Dienst mit angemessener rollenbasierter Zugriffskontrolle gespeichert werden, die entsprechend der relevanten Änderungen bei Rollen und Verantwortlichkeiten innerhalb der Organisation aktualisiert wird.

3.45 Die zentrale Speicherung dauerhafter Anmeldeinformationen ist durch Hardware zu schützen. Beispielsweise könnte das Laufwerk auf einem physischen Host mit einem Trusted Platform Module (TPM) verschlüsselt werden. Wenn ein virtueller Computer (VM) zur Bereitstellung eines zentralen Speicherdienstes verwendet wird, müssen diese VM und die darin enthaltenen Daten ebenfalls verschlüsselt sein, einen sicheren Bootvorgang verwenden und so konfiguriert sein, dass sichergestellt ist, dass sie nur in einer geeigneten Umgebung gebootet werden kann. Der Drittanbieter muss sicherstellen, dass der Fernzugriff so verwaltet wird, dass nur zugelassene Personen eine Fernverbindung zu den Systemen des Drittanbieters herstellen können, und dass die Verbindungen sicher sind und Datenverluste verhindert werden und dass eine angemessene Zugangskontrolle, wie z. B. eine Multi-Faktor-Authentifizierung, vorhanden ist.

Eine Zwei-Faktor-Authentifizierung muss mit einer Nutzer-ID, einem Passwort und einer der folgenden Methoden erreicht werden:

- Ein Generator für Einmalpasswörter, der eine nutzerspezifische PIN/ein nutzerspezifisches Passwort benötigt, um das Einmalpasswort anzuzeigen.
- Eine Smartcard mit einem ISO 7816-konformen Chip und dem dazugehörigen Kartenleser und der dazugehörigen Software. Kontaktlose Chipkarten sind nicht erlaubt.

- Zertifikatsbasierte Authentifizierung, die in Übereinstimmung mit der Infosec-Zertifikatsrichtlinie des Drittanbieters ausgestellt wurde.

Um Zweifel zu vermeiden, wenn ein privilegierter Zugang für den Support über Fernzugriff gewährt wird, muss dieser über eine sichere Verbindung erfolgen und eine Zwei-Faktor-Authentifizierung verwenden.

3.46 Der Drittanbieter muss sicherstellen, dass die Zugriffsrechte und -berechtigungen für alle Systeme (einschließlich Tools, Anwendungen, Datenbanken, Betriebssysteme, Hardware usw.) nach den Grundsätzen der geringsten Privilegien und der Aufgabentrennung verwaltet werden.

3.47 Der Drittanbieter muss sicherstellen, dass jede Transaktion einer einzigen, eindeutig identifizierbaren Person zugeordnet werden kann. Falls es gemeinsam genutzte Anmeldeinformationen gibt, muss er sicherstellen, dass es angemessene Kompensationskontrollen (einschließlich „Break-Glass“-Verfahren) gibt. Gemeinsam genutzte Anmeldeinformationen für privilegierten Zugriff sind nicht zulässig.

3.48 Der Drittanbieter muss sicherstellen, dass die gesamte Authentifizierung entsprechend dem Risiko der Transaktion verwaltet wird, d. h. angemessene Passwortlänge und -komplexität, Häufigkeit von Passwortänderungen, Multi-Faktor-Authentifizierung, sichere Verwaltung der Passwortzugangsdaten oder andere Kontrollen. Privilegierter Zugriff muss über Konten erfolgen, die mit einer Mulit-Faktor-Authentifizierung gesichert sind. Privilegierte „Break-Glass“-Benutzerkonten müssen über starke Anmeldeinformationen verfügen, die für jeden Netzausrüstungs-Zugangspunkt eindeutig sind.

3.49 Es müssen angemessene Regelungen vorhanden sein, um mit fehlgeschlagenen Authentifizierungen umzugehen, einschließlich Bildschirmbenachrichtigungen, Protokollierung von Fehlern und Nutzersperrung.

3.50 Es müssen Prozesse und Regelungen vorhanden sein, um Gäste- und Servicekonten zu verwalten und zu autorisieren.

Datenklassifizierung und Datenschutz

3.51 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk/Schema für die Klassifizierung, Bezeichnung und Handhabung von Daten/Informationen verfügen (ausgerichtet an der guten Branchenpraxis / den Anforderungen von BT), das die folgenden Komponenten enthält:

- Richtlinien zum Umgang mit Informationen.
- Die Informationen werden entsprechend dem zugewiesenen Geheimhaltungsgrad geschützt.
- Es muss sichergestellt werden, dass sich alle Mitarbeiter bewusst sind, dass die BT-Informationen nicht für andere Zwecke als den, für den sie bereitgestellt wurden, verwendet werden dürfen.

Verhinderung von Datenlecks

3.52 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk verfügen, um sicherzustellen, dass ein Schutz gegen unangemessene Datenlecks besteht, wobei der Schutz auch (aber nicht nur) die folgenden Vektoren umfasst:

- E-Mail, Internet/Web-Gateway (einschließlich Online-Speicher und Webmail), USB, optische und andere Formen von Ports / tragbaren Speichern usw., Mobile Computing und BYOD, Remote Access Services, Dateifreigabemechanismen und soziale Medien.
- Nicht autorisierte Geräte dürfen nicht an das Netzwerk angeschlossen werden (weder an das Unternehmensnetzwerk des Verkäufers noch an die Systeme / das Netzwerk von BT) oder für den Zugriff auf nicht-öffentliche Informationen verwendet werden.

Vulnerability Management (Management von Schwachstellen)

3.53 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk für das Vulnerability Management verfügen, das die folgenden Komponenten umfasst:

- Prozessrichtlinien und -verfahren.
- Definierte Rollen und Verantwortlichkeiten.
- Geeignete Werkzeuge wie Intrusion-Detection-Systeme und Schwachstellen-Scansysteme.

3.54 Das Rahmenwerk für das Vulnerability Management des Drittanbieters muss, um potenzielle Cyber-Sicherheitsereignisse zu erkennen, sicherstellen, dass Folgendes routinemäßig überwacht wird:

- Wichtige Systeme und Anlagen.
- Unerlaubte Verbindungen.
- Unerlaubte Software / Anwendungen.
- Netzwerk-Aktivität.

3.55 Das Rahmenwerk für das Vulnerability Management des Drittanbieters muss folgendes sicherstellen:

- Es sind Prozesse eingerichtet, um Schwachstellen, die der Organisation aus internen und externen Quellen (z. B. interne Tests, Sicherheitsbulletins oder Sicherheitsforscher) bekannt werden, entgegenzunehmen, zu analysieren und darauf zu reagieren.
- Nur autorisierte Werkzeuge, Technologien und Nutzer sind erlaubt.
- Identifizierte Schwachstellen werden gemildert oder als akzeptierte Risiken dokumentiert.

Sicherheit, kontinuierliche Protokollierung und Überwachung.

3.56 Der Drittanbieter muss sicherstellen, dass es ein etabliertes und konsistentes Rahmenwerk für Audit- und Protokollverwaltungs gibt, das gewährleistet, dass die Schlüsselsysteme einschließlich der Anwendungen so eingestellt sind, dass sie Schlüsselereignisse (darunter auch solche mit privilegiertem Zugang und Personalaktivitäten) protokollieren. Diese Protokolle müssen mindestens 13 Monate lang aufbewahrt werden. Protokolle für Netzwerkgeräte in sicherheitskritischen Funktionen müssen vollständig aufgezeichnet und 13 Monate lang für Audits zur Verfügung gestellt werden.

Als Mindestanforderung muss der Drittanbieter sicherstellen, dass die Protokolle die folgenden Ereignisse enthalten:

- Starten und Herunterfahren des Systems.
- Erfolgreiche und fehlgeschlagene Authentifizierungen
- System-Protokollstart/-stopp
- Erstellung, Änderung und Löschung von Konten
- Änderung von Anmeldeinformationen
- Rechteausweitung
- Kontoaussperrung
- Hardwareeinbindung und -entfernung
- System- und Netzwerkmanagement-Alarme und -Fehlermeldungen
- Änderungen des Sicherheitsereignis-Administrators; einschließlich Änderungen der Gruppenverwaltung und Sicherheitsrichtlinie
- Start- und Stopppunkte des protokollierten Prozesses
- Protokoll-Aktivierungs- oder -Deaktivierungsereignisse
- Änderungen der Art der protokollierten Ereignisse entsprechend den Anforderungen der Prüfkette (z. B. die Startparameter und deren Änderungen).
- Protokollveränderungen (oder versuchte Änderung)
- Jede Form des Zugangs zur Verwaltungsebene der Systeme, die im Zusammenhang mit einem öffentlichen elektronischen Kommunikationsnetzwerk oder -dienst im Vereinigten Königreich genutzt wurde

Als Mindestanforderung muss der Drittanbieter sicherstellen, dass die folgenden Protokollparameter für jedes Ereignis erfasst werden:

- Identität der Anlage, auf die sich das Ereignis bezieht
- Art des Ereignisses
- Datum und Zeitpunkt des Ereignisses
- Angabe zu Erfolg/Misserfolg des Ereignisses
- Benutzer-ID des Kontos
- Identifikation der Quelle eines Ereignisses, z. B. Benutzer-/Systemstandort, IP-Adressen der Terminal ID, Terminal ID oder anderer Identifikationsmittel

3.57 Das Rahmenwerk des Drittanbieters für die Prüfung, Protokollierung und Überwachnung muss die folgenden Komponenten umfassen:

- Ereignisprotokolle erzeugen Alarme in Echtzeit oder Fast-Echtzeit, um nicht autorisierte Aktivitäten zu erkennen
- Ereignisse und Alarme werden durch eine unabhängige Funktion auf dauerhafter Basis überwacht und werden untersucht, selektiert und einem Schweregrad zugewiesen
- Selektierte Alarme rufen Incident-Management-Prozesse basierend auf aufgestellten schützenden Überwachungsanwendungsfällen und -Playbooks entsprechend der Dienstleistungsvereinbarung und Schwere auf

- Protokolle werden so behandelt als hätten sie mindestens die Einstufung „vertraulich“ und werden vor Manipulation, nicht autorisiertem Zugriff und Verlust geschützt
- Die Protokollierungs- und Überwachunsaktivität wird mit einer zugelassenen NTP-Zeitquelle synchronisiert
- Es werden Prozesse aufgestellt, um zusätzliche schützende Überwachungsanwendungsfälle und damit in Verbindung stehende Ereignisprotokolle, Zusammenhänge und Alarme zu identifizieren und zu konfigurieren, die notwendig sind, um existierende oder aufkommende signifikante Bedrohungen oder Risiken anzugehen

4. Sicherheit des Personals von Drittanbietern

4.1 Der Drittanbieter stellt sicher, dass es für alle Mitarbeiter des Drittanbieters Vertraulichkeitsvereinbarungen gibt, bevor Mitarbeiter des Drittanbieters in den BT-Räumlichkeiten oder an den BT-Systemen arbeiten oder Zugang zu BT-Informationen erhalten. Diese Vertraulichkeitsvereinbarungen müssen vom Drittanbieter aufbewahrt werden, und die Nachweise müssen für die Prüfung durch BT zur Verfügung gestellt werden.

4.2 Der Drittanbieter muss gegen Verstöße gegen die Sicherheitskontrollen und -standards des Drittanbieters und von BT durch formelle Verfahren und Disziplinarmaßnahmen vorgehen. Dies kann bedeuten, dass:

- dem Mitarbeiter der Zugriff auf BT-Systeme oder zu BT-Informationen entzogen wird; oder
- der Mitarbeiter von Arbeiten, die mit der Bereitstellung des Dienstes verbunden sind, ausgeschlossen wird.

Darüber hinaus hat der Drittanbieter dafür Sorge zu tragen, dass er über relevante Prozesse verfügt, um sicherzustellen, dass Mitarbeiter des Drittanbieters, die auf diese Weise entfernt wurden, nicht nachträglich Zugang zu BT-Systemen und BT-Informationen erhalten oder in Verbindung mit der Bereitstellung des Dienstes arbeiten dürfen.

4.3 Der Drittanbieter unterhält im Rahmen der gesetzlichen Anforderungen eine vertrauliche Kontaktstelle, die von den Mitarbeitern des Drittanbieters dafür verwendet werden kann, anonym zu melden, wenn sie die Anweisung erhalten, auf eine Weise zu handeln, die diesen Sicherheitsanforderungen widerspricht oder sie verletzt. Entsprechende Meldungen müssen an BT erfolgen.

4.4 Wenn der Mitarbeiter des Drittanbieters dem Dienst nicht mehr zugewiesen wird, müssen nach Wahl von BT alle physischen Anlagen oder Informationen von BT, die sich im Besitz des Mitarbeiters des Drittanbieters befinden, entweder: gemäß Sicherheitsregelung 3.22 und 3.23 an das entsprechende operative Team von BT zurückgegeben oder sicher zerstört werden.

4.5 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk für die akzeptable Nutzung von privaten und geschäftlichen sozialen Medien verfügen und sicherstellen, dass das Personal:

- nichts Verleumderisches, Obszönes oder Beleidigendes über das Unternehmen, seine Kunden oder Auftraggeber veröffentlicht.
- Unternehmens- oder Kundenlogos nicht ohne vorherige Genehmigung verwendet.
- Nicht-öffentliche Informationen des Unternehmens oder von Kunden nicht ohne vorherige Genehmigung offenlegt.
- Meinungen über das Unternehmen, seine Kunden oder Auftraggeber, die aus angemessener Sicht als offizielle Stellungnahme des Unternehmens oder seiner Auftraggeber ausgelegt werden könnten, nicht veröffentlicht.
- BT-Informationen, die als „vertraulich“ oder „streng vertraulich“ gekennzeichnet sind, nicht veröffentlicht.

4.6 Der Drittanbieter muss sicherstellen, dass alle seiner Kontrolle unterstehenden Mitarbeiter des Drittanbieters innerhalb eines Monats nach Eintritt in die Firma eine obligatorische Sicherheitsschulung zur Informationssicherheit absolvieren, die die bewährten Methoden der Cybersicherheit und den Schutz personenbezogener Daten umfasst und mindestens einmal im Jahr, gegebenenfalls auch in Form einer Auffrischung, durchgeführt wird:

- Privilegierte Nutzer
- Stakeholder des Drittanbieters (z. B. Subunternehmer, Kunden, Partner)
- Leitende Angestellte
- Physisches und Cyber-Sicherheitspersonal

4.7 Der Drittanbieter muss sicherstellen, dass es eine Testkomponente gibt, um zu überprüfen, ob der Nutzer die Schulung und das Bewusstsein versteht.

4.8 Der Drittanbieter muss sicherstellen, dass stets ein aktuelles Register geführt wird, in dem das Personal des Drittanbieters, das die in Absatz 4.6 genannte Schulung erhalten hat, die zugehörigen Trainingsinhalte und – wo anwendbar - die durchgeführten Bewertungen aufgeführt sind.

4.9

5. Prüfung und Sicherheitsüberprüfung

5.1 Unbeschadet aller anderen Prüfungsrechte, die BT möglicherweise hat, gewährt der Drittanbieter zur Beurteilung der Einhaltung der Sicherheitsregelungen dieser Richtlinie für Sicherheitsanforderungen durch den Drittanbieter, BT oder seinen Vertretern Zugang und Unterstützung, soweit dies notwendig und angemessen ist, um dokumentenbasierte Sicherheitsüberprüfungen oder Vor-Ort-Prüfungen zu ermöglichen. Der Drittanbieter wird mindestens 30 Arbeitstage vor einer routinemäßigen Vor-Ort-Prüfung informiert.

Der Umfang der Prüfung besteht darin, einige oder alle Aspekte der Richtlinien, Prozesse und des Systems / der Systeme des Drittanbieters zu überprüfen (vorbehaltlich des Schutzes der Vertraulichkeit aller Informationen, die nicht mit der Erbringung der Dienstleistung für BT zusammenhängen), die für die zu erbringende Dienstleistung relevant sind.

5.2 Der Drittanbieter arbeitet mit BT zusammen, um vereinbarte Empfehlungen umzusetzen und alle Korrekturmaßnahmen, die sich aus einer dokumentengestützten Sicherheitsüberprüfung oder einer Vor-Ort-Prüfung ergeben, innerhalb von 30 Tagen nach der Benachrichtung durch BT über einen groben Verstoß, 90 Tagen nach der Benachrichtigung durch BT über einen geringen Verstoß oder eines anderweitig zwischen den Parteien vereinbarten Zeitraums auf Kosten des Drittanbieters durchführen.

6. Recht auf Überprüfung

6.1 Der Drittanbieter muss BT erlauben, eine Inspektion der Kontrollumgebung durchzuführen, in der die Dienstleistungen entwickelt, hergestellt oder bereitgestellt werden, um auf angemessenen Antrag (oder unmittelbar nach einem Zwischenfall) Prüfungen und/oder Bewertungen der Sicherheitskonformität durchzuführen.

6.2 Der Drittanbieter ist für die Kosten der Behebung der von BT festgestellten Sicherheitsmängel innerhalb eines von beiden Parteien vereinbarten Zeitrahmens verantwortlich.

6.3 Im Falle eines schwerwiegenden Vorfalls arbeitet der Drittanbieter in vollem Umfang mit BT bei allen nachfolgenden Untersuchungen durch BT, durch eine Regulierungsbehörde und/oder eine Strafverfolgungsbehörde zusammen, indem er Zugang gewährt und Unterstützung leistet, soweit dies für die Untersuchung des Vorfalls erforderlich und angemessen ist. BT muss möglicherweise die Quarantäne des Drittanbieters für die Bewertung aller relevanten Anlagen, die dem Drittanbieter gehören, beantragen, um die Untersuchung zu unterstützen, und der Drittanbieter darf diesen Antrag nicht unangemessen zurückhalten oder verzögern.

7. Sicherheitszertifikate

7.1 Die Systeme, Dienstleistungen, zugehörigen Dienste, Prozesse und physischen Standorte des Drittanbieters müssen mit der Norm ISO/IEC 27001 (oder Zertifizierung(en), die gleichwertige Kontrollen beinhaltet/beinhalten, unterstützt durch einen unabhängigen Prüferbericht) und jeder geänderten oder zukünftigen Version des Standards konform sein und diese kontinuierlich erfüllen. Diese Konformität muss durch die Zertifizierung des ISMS des Drittanbieters durch einen Akkreditierungsdienst des Vereinigten Königreiches (UK Accreditation Service, UKAS) oder eine international gleichwertige zugelassene Zertifizierungsstelle sichergestellt werden, wobei der Anwendungsbereich und die Erklärung der Anwendbarkeit die Dienstleistungen umfasst, die an den Standorten erbracht werden, an denen sie erbracht werden.

7.2 Der Drittanbieter muss zu Beginn des Vertrags und bei zukünftigen Rezertifizierungen ein gültiges Zertifikat vorlegen.

7.3 Sollte sich der Umfang des Zertifikats oder der Geltungserklärung während der Vertragslaufzeit ändern, soweit er nicht mehr alle an den Standorten – von denen aus sie erbracht werden – erbrachten Leistungen abdeckt, hat der Drittanbieter BT innerhalb einer angemessenen Frist zu informieren. Der Drittanbieter muss BT innerhalb von 2 Arbeitstagen über jede größere Nichtkonformität informieren, die von der

Zertifizierungsstelle oder dem Drittanbieter festgestellt wird und die ein Risiko für die bereitgestellten Leistungen darstellt.

8. Physische Sicherheit – BT-Räumlichkeiten

8.1 Der Drittanbieter soll sich an die betreffenden Anweisungen halten, die ihm hinsichtlich des Zugangs zu BT-Räumlichkeiten und Gebäude-Zugangssystemen mitgeteilt wurden. Alle in BT-Räumlichkeiten arbeitenden Mitarbeiter von Drittanbietern müssen im Besitz eines von dem Drittanbieter oder BT zur Verfügung gestellten Ausweises mit wahrheitsgetreuem Lichtbild sein und diesen an gut sichtbarer Stelle tragen.

8.2 BT kann den Mitarbeitern des Drittanbieters auch eine elektronische Zugangskarte und/oder zeitlich beschränkter Besucherkarte aushändigen, die in Übereinstimmung mit den lokalen Ausgabe- und Widerrufsanweisungen verwendet werden sollen.

8.3 Der Drittanbieter ist dafür verantwortlich, BT innerhalb von 24 Stunden zu informieren, wenn eine dritte Person keinen Zugang zu BT-Gebäuden und/oder Zugang zu BT-Zugangssystemen mehr benötigt.

8.4 Nur zugelassene von BT gebaute Server, BT Webtop-PCs und vertrauenswürdige Endgeräte können eine direkte Verbindung (Anschluss an einen LAN-Port oder eine drahtlose Verbindung) zu BT-Domänen herstellen. Drittanbieter dürfen ohne vorherige schriftliche Genehmigung von BT keine Geräte, die nicht von BT genehmigt sind, an eine BT-Domäne anschließen.

8.5 Der physische Schutz und die Richtlinien für die Arbeit in den Räumlichkeiten von BT müssen eingehalten werden, einschließlich, aber nicht beschränkt auf die Begleitung des Personals von Drittanbietern und die Einführung geeigneter Arbeitspraktiken in sicheren Bereichen.

8.6 Wenn ein Drittanbieter berechtigt ist, seinen Mitarbeitern ungehinderten Zugang zu Bereichen innerhalb der BT-Räumlichkeiten zu gewähren; müssen sich der Unterzeichnungsberechtigte des Drittanbieters und die Mitarbeiter des Drittanbieters an Leitfaden Lieferantenzugang zu BT-Standorten – Verpflichtender Sicherheitsleitfaden Verkauf an BT halten.

9. Physische Sicherheit – Räumlichkeiten von Drittanbietern

9.1 Der Drittanbieter muss über ein Verfahren für den physischen Zugang verfügen, das die Zugangsmethoden und -berechtigungen zu den Räumlichkeiten des Drittanbieters (Standorte, Gebäude oder interne Bereiche) umfasst, in denen Dienstleistungen erbracht werden oder in denen BT-Informationen gespeichert oder verarbeitet werden. Die Zugangsmethode muss einen oder mehrere der folgenden Punkte umfassen:

- Ein autorisierter Ausweis des Drittanbieters mit Foto, das ein eindeutiges und ein wahres Abbild der Person darstellt.
- Eine autorisierte elektronische Zugangskarte für den Zutritt zu den entsprechenden Bereichen der Räumlichkeiten.
- Einen Sicherheitszugang über ein Tastenfeld, der über Verfahren verfügen muss für: die Autorisierung, die Verbreitung von Codeänderungen (die mindestens monatlich erfolgen müssen) und Ad-hoc-Codeänderungen.

- Biometrische Erkennung

9.2 Der Drittanbieter muss über Prozesse und Verfahren zur Kontrolle und Überwachung von Besuchern und anderen externen Personen einschließlich Personal mit physischem Zugang zu Sicherheitsbereichen oder zum Zweck der Wartung im Rahmen der Umweltkontrolle, Wartung von Alarmsystemen und Reinigung verfügen.

9.3 Sichere Bereiche in Räumlichkeiten von Drittanbietern, die für die Bereitstellung des Dienstes genutzt werden (z. B. Netzwerkkommunikationsräume), sind von allgemeinen Zugangsbereichen zu trennen und durch geeignete Zugangskontrollen zu schützen, um sicherzustellen, dass nur autorisierten Personen der Zugang gestattet wird. Der Zugang zu diesen Bereichen muss regelmäßig überprüft werden und es muss mindestens jährlich eine Bewertung der Wiedererteilung der Zugangsrechte zu diesen Bereichen durchgeführt werden.

9.4 Der Drittanbieter muss über Videoüberwachungssysteme an den Orten verfügen, an denen BT-Informationen gespeichert oder verarbeitet werden. Aufnahmen und Aufnahmegeräte müssen sicher verwahrt werden, um eine Änderung, Löschung oder das „beiläufige“ Betrachten der zugehörigen Bildschirme zu verhindern. Der Zugang zu den Aufzeichnungen muss kontrolliert und auf autorisierte Personen beschränkt werden. Die Aufzeichnungen der Videoüberwachung müssen mindestens 20 Tage lang aufbewahrt werden.

9.5 Der Drittanbieter muss geeignete Maßnahmen zur Gewährleistung der physischen Sicherheit in Bezug auf folgende Punkte getroffen haben:

- Maßnahmen zur Brandverhütung, unter anderem Alarm-, Erkennungs- und Unterdrückungseinrichtungen.
- Klimatische Bedingungen unter Berücksichtigung von Temperatur, Feuchtigkeit und statischer Elektrizität und das damit verbundene Management, die Überwachung und die Reaktion auf extreme Bedingungen (wie z. B. automatische Abschaltung, Alarme).
- Kontrollausrüstung wie Klimaanlagen und Wassererkennung.
- Verhinderung von Wasserschäden, Lage der Wassertanks, Leitungen usw. innerhalb des Geländes.

9.6 Der Drittanbieter muss sicherstellen, dass der physische Zugang zu den Bereichen, in denen BT-Information untergebracht sind, mit Smart- oder Proximity-Karten (oder gleichwertigen oder besseren Sicherheitssystemen) erfolgt. Der Drittanbieter muss darüber hinaus monatliche Kontrollen durchführen, um sicherzustellen, dass nur relevante Personen diesen Zugang erhalten.

9.7 Der Drittanbieter muss sicherstellen, dass das Fotografieren und/oder die Bildaufnahme von BT-Informationen verboten ist. Wenn eine geschäftliche Notwendigkeit besteht, solche Bilder zu erfassen, muss eine schriftliche Bestätigung des BT-Stakeholders eingeholt werden.

10. Bereitstellung einer Hosting-Umgebung für BT-Geräte

10.1 Der Drittanbieter muss, wenn der Drittanbieter in seinen Räumlichkeiten einen sicheren Zugangsbereich für das Hosting von Geräten von BT oder das Hosting von Geräten von Kunden von BT zur Verfügung stellt:

- BT einen Grundriss des zugewiesenen Platzes im gesicherten Bereich der Räumlichkeiten zur Verfügung stellen.
- Sicherstellen, dass die Schränke von BT und BT-Kunden in den Räumlichkeiten verschlossen bleiben und nur autorisierten BT-Mitarbeitern, zugelassenen BT-Vertretern und relevanten Mitarbeitern von Drittanbietern zugänglich sind.
- Einen sicheren Schlüsselverwaltungsprozess implementieren.

10.2 BT muss dem Drittanbieter Folgendes zur Verfügung stellen:

- Ein Verzeichnis der physischen Anlagen von BT und/oder der Kunden von BT, die sich in den Räumlichkeiten des Drittanbieters befinden.
- Einzelheiten zu den Mitarbeitern, Subunternehmern und Agenten von BT, die Zugang zu den Räumlichkeiten des Drittanbieters benötigen (kontinuierlicher aktualisiert).

11. Sichere Software-Entwicklung

11.1 Der Drittanbieter muss sicherstellen, dass Produktions- und Nicht-Produktionsumgebungen angemessen kontrolliert werden, indem er dafür sorgt, dass die folgenden Komponenten vorhanden sind:

- Trennung von Produktions- und Nichtproduktionsumgebungen mit Aufgabentrennung.
- Es werden ohne die vorherige Zustimmung des Dateneigentümers und Kontrollen, die der Produktionsumgebung angemessen sind, im Test keine Live-Daten verwendet.
- Aufgabentrennung zwischen Produktions- und Nichtproduktionsentwicklung.

11.2 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk für die Systementwicklung verfügen, um Sicherheitslücken und Cyber-Sicherheitsverletzungen zu verhindern. Dieser muss die folgenden Komponenten enthalten:

- Die Systeme werden in Übereinstimmung mit der den bewährten Methoden für sichere Entwicklung (z. B. OWASP) entwickelt.
- Der Code wird sicher gespeichert und unterliegt der Qualitätssicherung.
- Der Code ist vor unbefugten Änderungen angemessen geschützt, sobald die Tests abgezeichnet sind und in die Produktion geliefert wurden.

12. Hinterlegung

12.1 Wenn zum Schutz aller Parteien eine Hinterlegung erforderlich ist, muss der Drittanbieter entweder für Erstanbieter- oder Drittanbieter-Hinterlegung (d. h. für geistiges Eigentum/Quellcode usw.) ein konsistentes und etabliertes Rahmenwerk haben, das die folgenden Komponenten umfasst:

- Abschluss und Umsetzung des Hinterlegungsvertrages mit einem unabhängigen, neutralen, und zuverlässigen Treuhänder.
- Lieferung und laufende Aktualisierung des Quellcodes und anderer Materialien an den Treuhänder, um sicherzustellen, dass die erforderlichen Informationen auf dem neuesten Stand sind.

- Sichere Speicherung von Quellcode und anderen Materialien, bis die Freigabebedingungen erfüllt sind.
- Geeignete Freigabebedingungen.
- Laufende Aktualisierungen, angemessene Zahlungen , und Überprüfungen des Hinterlegungsvertrages.

13. Zugriff auf BT-Systeme

13.1 Der Drittanbieter hat sich an die betreffenden Anweisungen zu halten, die ihm hinsichtlich des Zugriffs auf und der Nutzung von BT-Systemen mitgeteilt wurden.

13.2 Der Drittanbieter ist dafür verantwortlich, BT innerhalb von 24 Stunden zu informieren, wenn ein Mitarbeiter des Drittanbieters keinen Zugang mehr benötigt.

13.3 Der Drittanbieter stellt sicher, dass Nutzeridentifikation, Passwörter, PINs, Token und Konferenzzugang für einzelne Mitarbeiter des Drittanbieters bestimmt sind und nicht gemeinsam genutzt werden. Einzelheiten müssen sicher und getrennt von dem Gerät, das für den Zugriff verwendet wird, aufbewahrt werden. Wenn ein Passwort einer anderen Person bekannt ist, muss es sofort geändert werden.

System-zu-System-Konnektivität

13.4 Inter-Domain-Linking zu BT-Systemen ist nicht zulässig, es sei denn, es wurde ausdrücklich von BT genehmigt und autorisiert.

13.5 Der Drittanbieter muss alle angemessenen Anstrengungen unternehmen, um sicherzustellen, dass keine Malware (entsprechend der allgemeinen Begrifflichkeit in der Computerindustrie) in BT Systems eingeführt wird.

13.6 Besteht eine Verbindung zwischen den Systemen des Drittanbieters und den Systemen von BT, so erfolgt die Verbindung über sichere Verbindungen mit Daten, die durch Verschlüsselung gemäß den Kryptographieregelungen in 14.9, 14.10, 14.11, 14.12 und 14.13 geschützt sind.

13.7 Der Drittanbieter stellt sicher, dass die verwendeten Systeme und die Infrastruktur in ein dediziertes logisches Netzwerk eingebunden sind. Dieses Netzwerk darf nur aus den Systemen bestehen, die für die Lieferung einer sicheren Kundendatenverarbeitungsmöglichkeit bestimmt sind.

14. Drittanbieter-Systeme, die BT-Informationen speichern

14.1 Der Drittanbieter muss sicherstellen, dass die neuesten Sicherheitspatches auf Systeme/Anlagen/Netzwerke/Anwendungen angewendet werden, um zu gewährleisten, dass:

- der Drittanbieter Patches so schnell wie angemessen möglich bereitstellt und sich nach besten Kräften bemüht, innerhalb der folgenden Fristen nach Veröffentlichung des Patches bereitzustellen:

	Aktiv ausgenutzt	**Hoher EPSS** Anfälligkeit CVSS: > 8.0 (Hoch + Kritisch) EPSS: >= 70 % (Netzwerkangriffsvektor – siehe Abschnitt Begriffsbestimmungen)	**Niedriger EPSS** Anfälligkeit CVSS: > 8.0 (Hoch + Kritisch) EPSS: < 70 % (Netzwerkangriffsvektor – siehe Abschnitt Begriffsbestimmungen)	**Sonstige** (kein Netzwerkangriffsvektor)
Externe offene Schnittstelle	7 Tage	14 Tage	30 Tage	90 Tage
Interne offene Schnittstelle	7 Tage	14 Tage	30 Tage	90 Tage/BAU

- der Drittanbieter Patches verwendet, die er von nachstehend qualifizierten Anbietern direkt für proprietäre Systeme erhält und Patches, die entweder (i) digital signiert oder (ii) durch die Verwendung eines Anbieter-Hashes (MD5-Hashes dürfen nicht verwendet werden) für das Update-Paket verifiziert werden, so dass der Patch als von einer zuverlässigen Support-Community für Open-Source-Software stammend identifiziert werden kann.
- der Drittanbieter alle Patches auf Systemen testet, die die Konfiguration der Ziel-Produktionssysteme exakt repräsentieren, bevor der Patch auf die Produktionssysteme verteilt wird, und dass die korrekte Funktion des gepatchten Dienstes nach jeder Patch-Aktivität überprüft wird.
- alle zutreffenden Anbieter und andere relevante Informationsquellen auf Schwachstellenwarnungen überprüft werden.
- Wenn ein System nicht gepatcht werden kann, sind geeignete Gegenmaßnahmen zu ergreifen.
- Der Drittanbieter installiert kritische Sicherheitspatches getrennt von Feature-Releases, um die Geschwindigkeit zu maximieren, mit der der Patch bereitgestellt werden kann, und priorisiert wann immer möglich kritische Sicherheitspatches vor Funktionalitätsupdates.

14.2 Der Drittanbieter muss sicherstellen, dass mindestens einmal jährlich eine unabhängige von BT-Sicherheit zugelassene IT-Sicherheitsbewertung/Penetrationsprüfung der IT-Infrastruktur und der Anwendungen des Drittanbieters, die für die Bereitstellung von Diensten verwendet werden, einschließlich der Disaster-Recovery-Standorte, in Auftrag gegeben wird, um Schwachstellen zu ermitteln, die zur Verletzung von Daten/Diensten ausgenutzt werden könnten, und um Sicherheitsverletzungen durch Cyber-Angriffe zu verhindern. Der Drittanbieter muss BT auf begründeten Antrag Zugriff auf für die angebotenen Dienste relevante Penetrationstestberichten gewähren.

14.3 Der Drittanbieter muss sicherstellen, dass der Zugang zu den Diagnose- und Verwaltungsanschlüssen sowie zu den Diagnosewerkzeugen sicher kontrolliert wird.

14.4 Der Drittanbieter muss sicherstellen, dass der Zugang zu den Audit-Tools auf die entsprechenden Mitarbeiter des Lieferanten beschränkt ist und ihre Verwendung überwacht wird.

14.5 Der Drittanbieter muss sicherstellen, dass alle Server, die für die Bereitstellung des Dienstes verwendet werden, nicht ohne angemessene Sicherheitskontrollen in nicht vertrauenswürdigen Netzwerken (Netzwerke außerhalb des Sicherheitsbereichs des Drittanbieters, die sich seiner administrativen Kontrolle entziehen, z. B. mit Internetanschluss) eingesetzt werden.

Verwaltung von Assets

14.6 Der Drittanbieter muss ein genaues und aktuelles Inventar aller Technologie-Assets mit dem Potenzial, Informationen zu speichern oder zu verarbeiten, führen, so dass nur autorisierte Geräte Zugriff erhalten und nicht autorisierte und nicht verwaltete Geräte entdeckt und daran gehindert werden, Zugriff zu erhalten. Dieses Inventar muss alle Hardware-Assets umfassen, unabhängig davon, ob sie mit dem Netzwerk der Organisation verbunden sind oder nicht. Soweit BT-Geräte in Räumlichkeiten von Drittanbietern gehostet werden, sind sie in das Inventar aufzunehmen.

14.7 Der Drittanbieter muss sicherstellen, dass in dem Bestandsverzeichnis des Informationsguts die folgenden Komponenten inventarisiert oder katalogisiert sind:

- Physikalische Geräte und Systeme, Software-Plattformen und Anwendungen, externe Informationssysteme.
- Ressourcen (z. B. Hardware, Geräte, Daten, Zeit und Software) werden auf der Grundlage ihrer Klassifizierung, ihrer Kritikalität und ihres Geschäftswerts priorisiert.
- Unternehmens- und Kommunikationsdatenflüsse, einschließlich externer / Drittanbieter-Flüsse.
- Manuelle Prozesse, die mit Daten von BT oder Daten von Kunden von BT umgehen.

14.8 Der Drittanbieter muss ein genaues und aktuelles Software-Asset-Inventar für alle Software im Netzwerk führen, so dass nur autorisierte Software installiert und ausgeführt werden kann und dass nicht autorisierte und nicht verwaltete Software entdeckt und an der Installation und Ausführung gehindert wird.

Kryptographie

14.9 Der Drittanbieter muss sicherstellen, dass BT-Informationen, die als vertraulich oder höher eingestuft sind, angemessen verschlüsselt werden (während der Übertragung und im Ruhezustand). Alle Verschlüsselungen müssen mit starken modernen kryptografischen Algorithmen und Chiffren durchgeführt werden, die robuste Integritätsschutzmechanismen und in Übereinstimmung mit Industriestandards für sichere Schlüssel- und Protokollverhandlungen und Schlüsselverwaltung verwenden. Für Daten sind während der Übertragung folgende TLS-Optionen nicht zulässig: TLS v1.0, TLS v1.1 und SSL (alle Versionen). Die folgenden SSH (SFTP)-Optionen sind nicht zulässig: SSH v1. Die folgenden IPSec-Optionen sind nicht zulässig: IKE Version 1.

14.10 Kryptographische Schlüssel müssen die folgenden Mindestlängen erfüllen oder überschreiten:

- Symmetrische Schlüssel (z. B. AES) müssen eine Schlüssellänge von mindestens 256 Bit haben.
- Asymmetrische Schlüssel (z. B. RSA) müssen eine Schlüssellänge von mindestens 3072 Bit haben.
- Elliptische Kurvenschlüssel müssen eine Schlüssellänge von mindestens 384 Bit haben.

14.11 Wenn das NIST bekannt gibt, dass ein Kryptoalgorithmus nicht mehr sicher ist, darf er nicht für neue Einsätze verwendet werden. Bestehende Implementierungen müssen die weitere Verwendung veralteter Kryptoalgorithmen überprüfen und einen Migrationsplan vorlegen, um von veralteten Kryptoalgorithmen zu einer hinreichend sicheren Lösung überzugehen.

14.12 Für die symmetrische Verschlüsselung sind die folgenden Algorithmen nicht zulässig: 3DES-168 (sofern nicht durch einen internationalen Standard vorgeschrieben), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed und ARIA.

14.13 Salted Hashes müssen verwendet werden, um die Daten im Speicher, d. h. die Passwörter, zu schützen. Hashing kann auch zur Anonymisierung von Daten vor der Verarbeitung verwendet werden, z. B. MSISDNs oder Zahlungen. Die folgenden Hashing-Algorithmen sind nicht zulässig: MD2, MD4, MD5 und SHA-1.

Systemkonfiguration

14.14 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk verfügen, um sicherzustellen, dass die Systeme angemessen konfiguriert sind und die folgenden Komponenten umfassen:

- Systeme und Netzwerkgeräte werden so konfiguriert, dass sie im Einklang mit den Sicherheitsprinzipien funktionieren (z. B. Konzept der geringsten Funktionalität und keine unautorisierte Software).
- Sicherstellen, dass die Geräte die korrekte und konsistente Zeit haben.
- Die Systeme sind frei von bösartiger Software.
- Es gibt geeignete Tests und Überwachungen, um die Integrität der Builds/Geräte zu gewährleisten.

Malware-Schutz

14.15 Vulnerability Management muss sicherstellen, dass der aktuelle Malware-Schutz auf alle anwendbaren IT-Ressourcen angewendet wird, um eine Unterbrechung der Dienste oder Sicherheitsverletzungen zu verhindern und sicherzustellen, dass geeignete Verfahren zur Sensibilisierung der Nutzer implementiert werden.

Anti-Malware muss die Erkennung von (nicht begrenzt auf) Ransomware, unautorisiertem mobilen Code, Viren, Spyware, Key-Logger-Software, Botnets, Würmern, Trojanern usw umfassen.

Minderung von Denial of Service.

14.16 Der Drittanbieter muss sicherstellen, dass Schlüsselsysteme gegen Denial of Service (DoS)- und Distributed Denial of Service (DDoS)-Angriffe geschützt sind.

15. Drittanbieter-Systeme, die BT-Informationen hosten

15.1 Zusätzlich zu den Regelungen in Abschnitt 14. Drittanbieter-Systeme, die BT-Informationen speichern, wenn der Drittanbieter die Informationen von BT in einem Datenzentrum oder einer Cloud-Lösung hostet, müssen die Räumlichkeiten über ein gültiges ISO/IEC 27001-Zertifikat für das Sicherheitsmanagement verfügen (oder über eine oder mehrere Zertifizierung(en), die gleichwertige Kontrollen nachweisen, die durch einen unabhängigen Prüferbericht unterstützt werden).

16. Netzwerksicherheit – eigenes Netzwerk von BT

Wenn der Drittanbieter Geräte installiert, konfiguriert, wartet, repariert oder das BT-eigene Netzwerk überwacht, gelten die folgenden Regelungen:

16.1 Auf Antrag stellt der Drittanbieter BT die Namen, Adressen und andere Details zur Verfügung, die BT aus angemessener Sicht von allen einzelnen Mitarbeitern des Drittanbieters verlangt, die:

- direkt an der Bereitstellung, Wartung und/oder Verwaltung der Dienstleistung(en) beteiligt sein müssen, bevor sie jeweils beauftragt werden.
- wegen durch BT und/oder den Drittanbieter identifizierte Schwachstellen im Dienst / in den Diensten mit BT in Verbindung treten müssen.

16.2 In Bezug auf seine Unterstützungsaktivitäten im Vereinigten Königreich hält der Drittanbieter ein qualifiziertes Sicherheitsteam vor, dem mindestens ein Staatsangehöriger des Vereinigten Königreiches angehört, der für die Verbindung mit BT zur Verfügung steht. Das Team nimmt an den Sitzungen teil, die BT von Zeit zu Zeit aus angemessener Sicht verlangt.

16.3 Der Drittanbieter stellt BT eine (bei Bedarf aktualisierte) Aufstellung aller aktiven Komponenten, die in den Diensten enthalten sind, und deren jeweiligen Quellen zur Verfügung.

16.4 Der Drittanbieter muss sicherstellen, dass die Installation von neuen Systemen, Geräten oder neuer Software im eigenen Netzwerk von BT die aktuellen Software-Versionen und Patches nutzt.

16.5 Der Drittanbieter muss sicherstellen, dass jede sicherheitsrelevante Protokollierung auf jedem Netzwerkgerät, das durch den Drittanbieter installiert wird, aktiviert ist und an die Protokollsysteme des BT-Netzwerks gesendet wird.

16.6 Der Drittanbieter stellt BT rechtzeitig (d. h. so bald wie möglich, um eine Behebung vor der öffentlichen Veröffentlichung zu ermöglichen) Informationen in Bezug auf Schwachstellen in den Diensten zur Verfügung und erfüllt (auf Kosten des Drittanbieters) die angemessenen Anforderungen in Bezug auf Schwachstellen, die von BT gemeldet werden können.

16.7 Der Drittanbieter stellt sicher, dass alle sicherheitsrelevanten Komponenten, die von Zeit zu Zeit von oder für BT identifiziert werden, auf Kosten des Drittanbieters extern zur angemessenen Zufriedenheit von BT bewertet werden.

16.8 Der Drittanbieter muss BT unverzüglich – auf jeden Fall aber innerhalb von 7 Werktagen – alle Einzelheiten zu allen Merkmalen und/oder Funktionalitäten des Dienstes oder der in der Roadmap für den jeweiligen Dienst geplanten mitteilen, so dass von Zeit zu Zeit:

- der Drittanbieter weiß; oder
- BT vernünftigerweise davon ausgeht und den Drittanbieter darüber informiert, dass sie für die rechtmäßige Überwachung oder jede andere Art der Überwachung des Telekommunikationsverkehrs vorgesehen sind oder verwendet werden könnten. Diese Angaben umfassen alle Informationen, die vernünftigerweise erforderlich sind, damit BT die Art, Zusammensetzung und den Umfang dieser Merkmale und/oder Funktionen vollständig verstehen kann.

16.9 Der Drittanbieter darf keine Netzwerküberwachungswerkzeuge verwenden, die Anwendungsinformationen anzeigen können.

16.10 Der Aufbau, die Entwicklung und/oder die Unterstützung des eigenen Netzwerks von BT durch das Personal von Drittanbietern muss mindestens einer L2-Kontrolle vor der Einstellung unterliegen. L3-Kontrollen vor der Einstellung sind für die von BT festgelegten Rollen erforderlich.

16.11 Der Drittanbieter gestattet BT die Installation von Sicherheitssoftware nach BT-Spezifikation auf einer virtuellen Infrastruktur von Drittanbietern (einschließlich, jedoch nicht beschränkt auf virtuelle Computer und Container) oder einem von Drittanbietern installierten Betriebssystem, das in BT-Netzwerken ausgeführt wird.

16.12 Der Drittanbieter muss sicherstellen, dass die neuesten Sicherheitspatches auf Systeme/Anlagen/Netzwerke/Anwendungen angewendet werden, um zu gewährleisten, dass:

- der Drittanbieter Patches so schnell wie angemessen möglich bereitstellt und sich nach besten Kräften bemüht, innerhalb der folgenden Fristen nach Veröffentlichung des Patches bereitzustellen:

	Aktiv ausgenutzt	**Hoher EPSS** Anfälligkeit CVSS: > 8.0 (Hoch + Kritisch) EPSS: >= 70 % (Netzwerkangriffsvektor – siehe Abschnitt Begriffsbestimmungen)	**Niedriger EPSS** Anfälligkeit CVSS: > 8.0 (Hoch + Kritisch) EPSS: < 70 % (Netzwerkangriffsvektor – siehe Abschnitt Begriffsbestimmungen)	**Sonstige** (kein Netzwerkangriffsvektor)
Externe offene Schnittstelle	7 Tage	14 Tage	30 Tage	90 Tage
Interne offene Schnittstelle	7 Tage	14 Tage	30 Tage	90 Tage/BAU

- der Drittanbieter Patches verwendet, die er von nachstehend qualifizierten Anbietern direkt für proprietäre Systeme erhält und Patches, die entweder (i) digital signiert oder (ii) durch die Verwendung eines Anbieter-Hashes

(MD5-Hashes dürfen nicht verwendet werden) für das Update-Paket verifiziert werden, so dass der Patch als von einer zuverlässigen Support-Community für Open-Source-Software stammend identifiziert werden kann.

- der Drittanbieter alle Patches auf Systemen testet, die die Konfiguration der Ziel-Produktionssysteme exakt repräsentieren, bevor der Patch auf die Produktionssysteme verteilt wird, und dass die korrekte Funktion des gepatchten Dienstes nach jeder Patch-Aktivität überprüft wird.
- alle zutreffenden Anbieter und andere relevante Informationsquellen auf Schwachstellenwarnungen überprüft werden.
- Wenn ein System nicht gepatcht werden kann, sind geeignete Gegenmaßnahmen zu ergreifen.
- Der Drittanbieter liefert kritische Sicherheitspatches getrennt von Feature-Releases, um die Geschwindigkeit zu maximieren, mit der der Patch bereitgestellt werden kann, und priorisiert wann immer möglich kritische Sicherheitspatches vor Funktionalitätsupdates.

Wenn der Drittanbieter Waren, Dienstleistungen oder Einrichtungen zur Nutzung in Verbindung mit einem ICT Service oder ICT Produkt (einschließlich einem öffentlichen elektronischen Kommunikationsnetzwerk oder – dienst) liefert oder verfügbar macht, gelten die folgenden Sicherheitsregelungen:

16.13 Unterstützt ein Drittanbieter mehr als einen Betreiber, müssen Kontrollen durchgeführt werden, um zu verhindern, dass ein Betreiber oder sein Netzwerk einen anderen Betreiber oder dessen Netzwerk beeinträchtigen.

16.14 Wenn der Drittanbieter als externer Administrator für mehr als einen Betreiber arbeitet, gelten die folgenden Regelungen:

- Implementierung einer logischen Trennung innerhalb des Netzwerks von Drittanbietern, um Kundendaten und -netzwerke zu trennen.
- Implementierung einer Trennung zwischen Drittanbieter-Managementumgebungen, die für verschiedene Betreibernetzwerke verwendet werden.
- Implementierung und Durchsetzung von Sicherheitsfunktionen am Übergang zwischen dem Drittanbieternetzwerk und dem Betreibernetzwerk.
- Implementierung von technischen Kontrollen, um das Potenzial für Benutzer oder Systeme zu begrenzen, mehr als einen Betreiber negativ zu beeinflussen.
- Implementierung von physisch und logisch unabhängigen Workstations mit privilegiertem Zugriff pro Betreiber.
- Implementierung von unabhängigen administrativen Domänen und Konten pro Betreiber.

16.15 Bei der Bereitstellung von Netzwerkausrüstung müssen Drittanbieter eine „Sicherheitserklärung“ darüber vorlegen, wie die sichere Ausrüstung hergestellt wird und wie die Sicherheit der Ausrüstung während ihrer gesamten Lebensdauer gewährleistet ist. Diese Sicherheitserklärung muss die Anforderungen der Lieferantensicherheitsbewertung erfüllen, die in Anhang B des Verhaltenskodex für die Telekommunikationssicherheit veröffentlicht werden - gemäß den Abschnitten 105E

und 105F des UK Communications Act 2003 - Diese „Sicherheitserklärung“ muss vom Management des Drittanbieters bestätigt werden. Details sind zuvor mit BT abzustimmen.

16.16 Wenn der Drittanbieter Netzwerkausrüstung bereitstellt, gelten die folgenden Regelungen:

- Der Drittanbieter garantiert, dass er einen Standard einhält, der nicht niedriger ist als seine veröffentlichte „Sicherheitserklärung“.
- Der Drittanbieter liefert aktuelle Leitlinien, wie die Ausrüstung sicher eingesetzt werden kann.
- Der Drittanbieter unterstützt alle Geräte und alle Software- und Hardware-Teilkomponenten für die Dauer des Vertrages.
- Der Drittanbieter stellt Einzelheiten zu allen wichtigen Komponenten und Abhängigkeiten von Drittanbietern bereit, einschließlich, jedoch nicht beschränkt auf Produkte und Versionen, Open-Source-Komponenten und Umfang des Supports und Zeitraums.
- Der Drittanbieter wird alle Sicherheitsprobleme, die ein Sicherheitsrisiko für das Netzwerk oder den Dienst von BT darstellen, die in seinen Produkten entdeckt wurden, innerhalb einer angemessenen Frist nach der Benachrichtigung beheben und in der Zwischenzeit regelmäßige Aktualisierungen über den Fortschritt bereitstellen. Diese Frist wird zwischen BT und dem Drittanbieter nach vernünftigem Ermessen vereinbart. Dies umfasst alle von der Sicherheitsanfälligkeit betroffenen Produkte und nicht nur das Produkt, für das die Sicherheitsanfälligkeit gemeldet wurde.
- Der Drittanbieter wird Standardpasswörter und Standard- oder feste Konten entweder entfernen oder ändern oder sicherstellen, dass das Netzwerkgerät so konfiguriert ist, dass BT hierzu in der Lage ist.
- Der Drittanbieter wird wann immer möglich nicht verschlüsselte Managementprotokolle deaktivieren und falls dies nicht möglich ist BT über das Vorhandensein solcher Protokolle in Kenntnis setzen, damit deren Nutzung minimiert werden kann.

16.17 Wenn der Drittanbieter international anerkannte Sicherheitsbewertungen oder -zertifizierungen für Geräte erhalten hat (z. B. Common Criteria oder NESAS), müssen diese mit BT geteilt werde, einschließlich der vollständigen Erkenntnisse, die diese Bewertung oder dieses Zertifikat belegen.

16.18 Wenn das eigene Netzwerk des Drittanbieters Auswirkungen auf die Netzwerke von BT haben kann, wird der Drittanbieter, wie von BT empfohlen, das gleiche Testniveau wie BT für die Netzwerke von BT durchlaufen und identifizierte Schwachstellen, wie von beiden Parteien vereinbart, beheben.

16.19 Der Drittanbieter ermächtigt BT, Einzelheiten zu Sicherheitsfragen weiterzugeben, soweit dies für die Zwecke der Netzwerksicherheit erforderlich ist.

16.20 Infrastruktur und Systeme, die zur Wartung der Netzwerke von BT verwendet werden, müssen sich innerhalb des Vereinigten Königreichs befinden.

16.21 Wenn der Drittanbieter die Netzwerküberwachungsfunktionen von BT ausführt, müssen sich die für diese Funktion verwendeten Geräte im Vereinigten Königreich befinden und von Personal mit Sitz im Vereinigten Königreich betrieben werden.

16.22 Wenn der Drittanbieter für Netzwerksicherheit und Auditprotokolle verantwortlich ist, müssen diese innerhalb des Vereinigten Königreichs gespeichert und entsprechend dem Recht des Vereinigten Königreiches geschützt werden.

16.23 Wenn der Drittanbieter als Dritter Administrator tätig ist, behält sich BT das Recht vor, die Berechtigung der Konten festzulegen, die vom Drittanbieter für den Zugriff auf sein Netzwerk genutzt werden, und alle Protokolle in Bezug auf die Sicherheit des Drittanbieter-Netzwerks in dem Umfang zu erfordern, wie solche Protokolle in Bezug auf den Zugang in das Netzwerk von BT stehen. Der Drittanbieter hat die Aktivitäten seiner Mitarbeiter zu überwachen und zu prüfen, wenn diese auf das Netzwerk von BT zugreifen.

17. Sicherheit des Netzwerks von Drittanbietern

17.1 Der Drittanbieter muss sicherstellen, dass die Netzwerkintegrität hergestellt und aufrechterhalten wird, indem er dafür sorgt, dass die folgenden Komponenten angemessen kontrolliert werden, und BT darüber in Kenntnis setzen, falls dies in irgendeinem Fall technisch nicht möglich ist:

- Externe Verbindungen zum Netzwerk werden dokumentiert, durch eine Firewall geleitet und vor dem Aufbau der Verbindungen verifiziert und genehmigt, um Datensicherheitsverletzungen zu verhindern.
- Das Netzwerk wird nach den Prinzipien der „Defence in Depth“ (Tiefenverteidigung) angemessen gestaltet, um sicherzustellen, dass Cyber-Sicherheitsverletzungen durch geeignete Kontrollen, die jeden gezielten Angriff wie die „Netzwerksegmentierung“ verhindern, minimiert werden.
- Die Gestaltung und Umsetzung des Netzwerks werden mindestens jährlich überprüft.
- Jeder drahtlose Zugriff auf das Netzwerk unterliegt der Autorisierung, Authentifizierung, Segmentierung und Verschlüsselungsprotokollen, um Sicherheitsverletzungen zu verhindern.
- Verwendung sicherer Kommunikation zwischen den Geräten und Verwaltungsstationen.
- Verwendung angemessener sicherer Kommunikation zwischen den Geräten, einschließlich der Verschlüsselung aller Nicht-Konsolen-Administratorzugriffe;
- Verwendung eines starken Architekturdesigns, das in Schichten und Zonen mit effektiver Identitätsverwaltung und Betriebssystemkonfiguration unterteilt ist, die entsprechend verstärkt und dokumentiert werden müssen.
- Deaktivierung (wo möglich) von Diensten, Anwendungen und Ports, die nicht genutzt werden.
- Deaktivierung oder Entfernung von Gastkonten.
- Vermeidung von vertrauenswürdigen Beziehungen zwischen Servern.

- Anwendung des Best-Practice-Sicherheitsprinzips der „geringsten Privilegien“ zur Ausführung einer Funktion.
- Gewährleistung geeigneter Maßnahmen zur Erkennung von und/oder zum Schutz vor Eindringlingen.
- Gegebenenfalls Überwachung der Integrität von Dateien, um das Hinzufügen, Ändern oder Löschen von kritischen Systemdateien oder Daten zu erkennen.
- Änderung aller standardmäßig und vom Lieferanten gesetzten Passwörter, bevor die Netzwerkkomponenten in Betrieb genommen werden.
- Deaktivierung unverschlüsselter Managementprotokolle wann immer dies technisch möglich ist.

17.2 Das Netzwerk des Drittanbieters hat alle gesetzlichen und regulatorischen Anforderungen zu erfüllen, und:

- sich nach besten Kräften bemühen, Unbefugten (z. B. Hackern) den Zugang zu dem/den Netzwerk(en) des Drittanbieters zu verwehren.
- sich nach besten Kräften bemühen, das Risiko eines Missbrauchs des/der Netzwerke(s) durch die zugangsberechtigten Personen zu verringern.
- sich nach besten Kräften bemühen, Sicherheitsverletzungen aufzudecken und eine rasche Behebung von Verstößen zu gewährleisten, die Personen identifizieren, die Zugang erhalten haben, und legen bestimmen, wie sie den Zugang erhalten haben.

17.3

Wenn der Drittanbieter Waren, Dienstleistungen oder Einrichtungen zur Nutzung in Verbindung mit einem ICT Service oder ICT Produkt (einschließlich einem öffentlichen elektronischen Kommunikationsnetzwerk oder –dienst) liefert oder verfügbar macht, gelten die folgenden Sicherheitsregelungen:

17.4

- Außenliegende Systeme, mit Ausnahme von Customer Premises Equipment (CPE), werden alle zwei Jahre oder bei wesentlichen Änderungen sicherheitstechnisch geprüft.
- Sensible Datensätze und sensible oder kritische Funktionen werden nicht auf Geräten am Exposed Edge des Netzwerks gehostet.
- Falls nicht kryptographisch geschützt, muss eine physische und logische Trennung zwischen dem Exposed Edge und sensiblen oder kritischen Funktionen implementiert werden.
- Die Sicherheitstrennung mithilfe von Sicherheitsfunktionen muss zwischen dem Exposed Edge und sensiblen oder kritischen Funktionen implementiert werden.

18. Cloud Sicherheit

18.1 Der Drittanbieter muss nach der neuesten Version von ISO 27017 zertifiziert sein oder über ein etabliertes und konsistentes Rahmenwerk verfügen, um sicherzustellen, dass die gesamte Nutzung der Cloud-Technologie und der in der Cloud gespeicherten nicht-öffentlichen Daten genehmigt ist und angemessenen Kontrollen unterliegt, die der neuesten Version der Cloud Security Alliance, Cloud Controls Matrix (CCM) entspricht.

18.2 Netz- und Infrastruktur-Service-Level-Vereinbarungen (intern oder extern) müssen geteilte Verantwortlichkeiten, Sicherheitskontrollen, Kapazitäten und Service-Level sowie Geschäfts- oder Kundenanforderungen klar dokumentieren.

18.3 Der Drittanbieter muss Sicherheitsmaßnahmen in allen Aspekten des zu erbringenden Dienstes umsetzen, so dass die Vertraulichkeit, Verfügbarkeit, Qualität und Integrität gewährleistet sind, indem die Möglichkeit, dass unbefugte Personen (z. B. andere Cloud-Kunden) Zugang zu BT-Informationen und den von BT genutzten Diensten erhalten, minimiert wird.

18.4 Soweit der Drittanbieter gehostete Anwendungen oder Dienstleistungen für BT bereitstellt – ob Einzel- oder Mehrmandanten – einschließlich Software-as-a-Service, Plattform-as-a-Service, Infrastruktur-as-a-Service und ähnliche Angebote, um vertrauliche Daten zu sammeln, zu übertragen, zu speichern oder anderweitig zu verarbeiten, stellt der Drittanbieter BT die Fähigkeit zur Verfügung:

- solche vertraulichen Daten logisch von den Daten anderer Kunden des Drittanbieters zu isolieren.
- jederzeit den Zugriff auf solche vertraulichen Daten einzuschränken, zu protokollieren und zu überwachen – einschließlich des Zugriffs durch Mitarbeiter des Drittanbieters.
- den obersten Verschlüsselungsschlüssel (bekannt als kundenverwalteter Schlüssel), der zum Verschlüsseln und Entschlüsseln nachfolgender Schlüssel – einschließlich des untersten Datenverschlüsselungsschlüssels – verwendet wird, zu erstellen, zu aktivieren, zu deaktivieren und zu löschen.
- den Zugriff auf den kundenverwalteten Schlüssel jederzeit einzuschränken, zu protokollieren und zu überwachen; und zu keinem Zeitpunkt darf ein nachfolgender Verschlüsselungsschlüssel, ein Verschlüsselungsschlüssel in einer Schlüsselhierarchie, die niedriger als der kundenverwaltete Schlüssel ist, im gleichen System wie vertrauliche Daten gespeichert werden, es sei denn er wird durch den vom Kunden verwalteten Schlüssel verschlüsselt (auch als vom kundenverwalteten Schlüssel umhüllt bekannt).

19. SIM-Karten

19.1 Wenn der Drittanbieter SIM-Karten bereitstellt, gelten die folgenden Regelungen:

- Bei SIM-Karten mit festem Profil stellt der Drittanbieter sicher, dass sensible Daten vom Hersteller der SIM-Karte angemessen geschützt werden.
- Bei SIM-Karten mit festem Profil stellt der Drittanbieter sicher, dass die Vertraulichkeit und Verfügbarkeit der mit dem Hersteller der SIM-Karte geteilten sensiblen Daten der SIM-Karte in jeder Phase ihres Lebenszyklus geschützt ist.

20. Vom HMG als „VS – VERTRAULICH“ oder höher eingestufte Informationen

20.1 Die zusätzlichen Sicherheitsanforderungen, die in Anhang 1 dieser Sicherheitsanforderungen aufgeführt sind, gelten für alle Drittanbieter, die als „VS – VERTRAULICH“ eingestufte Informationen in Übereinstimmung mit dem von Zeit zu Zeit

aktualisierten Klassifikationsschema der Regierung Seiner Majestät speichern, verarbeiten oder übermitteln.

21. Definierte Begriffe und Interpretation

21.1 Sofern im Folgenden nicht anders definiert, haben die in diesen Sicherheitsanforderungen verwendeten Wörter und Begriffe die gleiche Bedeutung wie im Vertrag:

„Zugriff“ und **„Zugegriffen“** bezeichnet die Verarbeitung, Handhabung oder Speicherung von BT-Informationen durch eine oder mehrere der folgenden Methoden:

a. durch die Verbindung mit BT Systemen;

b. in Papier- oder nicht-elektronischem Format bereitgestellt;

c. BT-Informationen in Lieferantensystemen; oder

d. durch mobile Medien

und/oder Zugang zu den Räumlichkeiten von BT für die Bereitstellung der Lieferungen, mit Ausnahme der Lieferung von Hardware und der Teilnahme an Meetings.

„BT-Informationen“ bezeichnet alle Informationen über BT oder einen BT-Kunden, die dem Lieferanten zur Verfügung gestellt werden, sowie alle Informationen, die vom Lieferanten im Namen von BT oder einem BT-Kunden im Rahmen des Vertrags verarbeitet oder bearbeitet werden.

„BT-Stakeholder“ bezeichnet den BT-Vertreter, der Eigentümer des vom Drittanbieter ausgeführten Arbeitsumfangs ist.

„BT-Systeme“ bezeichnet die Services und Servicekomponenten, Produkte, Netzwerke, Server, Prozesse, papiergestützte Systeme oder IT-Systeme (ganz oder teilweise), die sich im Besitz von BT befinden und/oder von BT betrieben werden, oder andere Systeme, die auf dem Gelände von BT gehostet werden können.

„BT-Netzwerke“ bezeichnet jedes öffentliche elektronische Kommunikationsnetz, das von BT betrieben wird, wie in Abschnitt 32 des Communications Act 2003 festgelegt.

„BYOD“ bedeutet, dass Sie Ihr eigenes Gerät mitbringen (Bring Your Own Device).

„Vertrag“ bezeichnet den von den Parteien abgeschlossenen Vertrag über die Lieferung von Waren, Software oder Dienstleistungen, der auf diese Sicherheitsanforderungen verweist.

„Ausrüstung am Standort des Kunden“ bezeichnet Ausrüstung, die Kunden vom Anbieter zur Verfügung gestellt und vom Anbieter verwaltet wird. Sie wird als Teil eines Netzwerks oder Dienstes verwendet oder ist dafür vorgesehen. Dies schließt elektronische Verbrauchergeräte wie Mobiltelefone und Tablets aus, umfasst jedoch Geräte wie Edge-Firewalls, SD-WAN-Geräte und einen festen drahtlosen Zugangssatz. “”

„Cyber Essentials Plus“ bezeichnet ein von der Regierung des Vereinigten Königreiches unterstütztes Programm, das Unternehmen dabei helfen soll, sich gegen die üblichen Cyber-Angriffe zu schützen.

„Cybersicherheit“ bezeichnet die Art und Weise, wie Einzelpersonen und Organisationen das Risiko von Cyberangriffen verringern. Die Kernfunktion von Cybersicherheit besteht darin, die von uns allen genutzten Geräte (Smartphones, Laptops, Tablets und

Computer) und die Dienste, auf die wir zugreifen – sowohl online als auch bei der Arbeit – vor Diebstahl oder Beschädigung zu schützen.

„EPSS“ bezeichnet das Exploit Prediction Scoring System (System zur Bewertung von Schwachstellen).

“Escrow” bezeichnet die in Übereinstimmung mit dem Vertrag abgeschlossene Vereinbarung über die Hinterlegung des Quellcodes, diesen Quellcode für die Geschäftszwecke von BT zu verwenden, zu kopieren, zu pflegen und zu modifizieren (einschließlich des Rechts, diesen Quellcode zu kompilieren).

„Exposed Edge“ bezeichnet Geräte, die sich entweder innerhalb des Kundengeländes befinden, direkt von Kunden-/Benutzergeräten aus ansprechbar oder physisch anfällig sind. Zu den physisch gefährdeten Geräten gehören Geräte in Schaltschränken auf der Straße oder an Straßeneinrichtung befestigte Geräte. Das Exposed Edge umfasst CPEs, Ausrüstung von Basisstationen, OLT-Ausrüstung und MSAN/DSLAM-Ausrüstung.

„Gute Sicherheitspraxis in der Industrie“ bezeichnet in Bezug auf jedes Unternehmen und alle Umstände die Umsetzung der Sicherheitspraktiken, -richtlinien, -standards und -werkzeuge, die aus angemessener Sicht und normalerweise von einer qualifizierten und erfahrenen Person erwartet werden, die unter gleichen oder ähnlichen Umständen mit derselben Art von Tätigkeit befasst ist.

„ICT Produkt“ bezeichnet ein Element oder eine Gruppe von Elementen eines Netzwerks oder Informationssystems.

„ICT Service“ bezeichnet einen Dienst, der vollständig oder hauptsächlich in der Übertragung, Speicherung, dem Abruf oder der Verarbeitung von Informationen mittels Netzwerk- und Informationssystemen besteht.

„NDA“ bezeichnet eine Geheimhaltungsvereinbarung und ist ein verbindlicher Vertrag zwischen zwei oder mehr Parteien, der die Weitergabe sensibler Informationen an andere Einschränkungen unterwirft.

„NESAS“ bezeichnet das Network Equipment Security Assurance Scheme der GSM Association.

„Netzwerk-Asset“ bezeichnet ein Element, das Teil einer Sammlung von miteinander verbundenen Komponenten wie Computern, Routern, Hubs, Verkabelung und Telekommunikationscontrollern ist, die ein Netzwerk bilden.

„Netzwerk-Angriffsvektor“ bedeutet, dass die gefährdete Komponente an den Netzwerk-Stack gebunden ist und Menge der möglichen Angreifer geht über die unten aufgeführten Optionen hinaus, bis hin zum und einschließlich dem gesamten Internet. Eine solche Gefährdung wird oft als „extern ausnutzbar“ bezeichnet und kann als ausnutzbarer Angriff auf der Protokollebene einen oder mehrere Netzwerkschritte entfernt (z. B. über einen oder mehrere Router) verstanden werden. Ein Beispiel für einen Netzwerkangriff ist ein Angreifer, der einen Denial of Service (DoS) verursacht, indem er ein speziell gestaltetes TCP-Paket über ein WAN versendet (z. B. CVE 2004 0230).

„Netzwerkaufsichtsfunktion“ bezeichnet die Komponenten des BT-Netzwerks, die die sicherheitskritischen Funktionen überwachen und steuern, womit sie für die allgemeine Netzwerksicherheit von entscheidender Bedeutung sind. Sie sind für BT unerlässlich, um das Netzwerk zu verstehen, das Netzwerk zu sichern oder das Netzwerk wiederherzustellen.

„Netzwerksicherheit“ bezeichnet die Sicherheit der miteinander verbundenen Kommunikationspfade und Knoten, die die Endbenutzertechnologien und die zugehörigen Managementsysteme logisch miteinander verbinden.

„NIST“ bezeichnet das National Institute of Standards and Technology – eine Abteilung des US-Handelsministeriums. Vormals als National Bureau of Standards bekannt, fördert und pflegt das NIST Messstandards. Es hat auch aktive Programme, um Industrie und Wissenschaft zu ermutigen und zu unterstützen, diese Standards zu entwickeln und zu nutzen.

„Offizielle Sensibilitätserklärung“ bezeichnet die schriftliche Erklärung, die vom Lieferanten vorzulegen ist und die sich auf Funktionen bezieht, die der Lieferant als mit Zugang zu als „official sensitive“ eingestuften Informationen oder mit erhöhten Privilegien für eine Infrastruktur, die als „official sensitive“ eingestufte Informationen speichert, verarbeitet oder überträgt, identifiziert hat. Eine Vorlage hierfür ist in Anhang 1 enthalten.

„Privileged Access Workstation (PAW)“ bezeichnet Workstations, über die ein privilegierter Zugriff möglich ist.

„Sicherheitskritische Funktion“ bezeichnet jede Funktion des BT-Netzwerks oder des Dienstes, deren Betrieb voraussichtlich einen wesentlichen Einfluss auf den ordnungsgemäßen Betrieb des gesamten Netzwerks oder Dienstes oder eines wesentlichen Teils davon hat.

„Sicherheitsanforderungen“ bezeichnet dieses regelmäßig aktualisierte Dokument.

„SIM“ bezeichnet eine eindeutige Hardwarekomponente oder ein einzigartiges Token und eine zugehörige Software, die zur Authentifizierung des Zugangs des Teilnehmers zum Netzwerk verwendet wird. Wie in diesem Dokument verwendet, umfasst SIM die Hardware UICC/eUICC, die SIM/USIM/ISIM-Anwendungen, die eSIM- und RSP-Funktionalität und alle SIM-Applets.

„Subunternehmer“ bezeichnet einen Subunternehmer des Lieferanten, der die Lieferungen ausführt oder an der Bereitstellung der Lieferungen beteiligt ist oder der Personen beschäftigt oder einsetzt, die an der Bereitstellung der Lieferungen beteiligt sind.

„Dienstleistung“ bezeichnet jede und alle **„Waren“**, **„Software“** oder **„Dienstleistungen“**, wie im Vertrag definiert.

„Transaktionen“ bezeichnet Transaktionsdaten/-informationen, die aus Transaktionen erfasst werden, d. h. Daten, die von verschiedenen Anwendungen während der Ausführung oder Unterstützung alltäglicher Geschäftsprozesse generiert werden.

„Trusted Platform Module“ bezeichnet Technologie, die entworfen wurde, um hardwarebasierte, sicherheitsrelevante Funktionen bereitzustellen. Ein TPM-Chip ist ein sicherer Krypto-Prozessor, der entworfen wurde, um kryptographische Operationen durchzuführen. Der Chip enthält mehrer physische Softwaremechanismen, um ihn manipulationssicher zu machen und Schadsoftware kann die Sicherheitsfunktionen des TPM nicht manipulieren. Die gebräuchlichsten TPM-Funktionen werden für Maßnahmen der Systemintegrität und die Erstellung und Verwendung von Schlüsseln verwendet. Während des Bootvorgangs eines Systems kann der geladene Boot-Code (einschließlich Firmware und den Komponenten des Betriebssystems) im TPM gemessen und aufgezeichnet werden. Die Integritätsmessungen können als Beweismittel verwendet werden, wie ein System gestartet wurde, und um

sicherzustellen, dass ein TPM-basierter Schlüssel nur verwendet wurde, wenn die richtige Sofware zum booten des Systems verwendet wurde.

„Drittanbieter“ bezeichnet einen Lieferanten von BT.

„Drittanbieter-Administrator“ bezeichnet einen verwalteten Diensteanbieter, Anbieter von Gruppenfunktionen oder externe Unterstützung für Ausrüstung eines dritten Anbieters (z. B. Unterstützungsfunktion eines Dritten)

„Mitarbeiter des Drittanbieters“ bezeichnet alle Personen, die vom Lieferanten oder seinen Subunternehmern zur Erfüllung der vertraglichen Verpflichtungen des Lieferanten eingesetzt werden.

„Drittanbieter-Netzwerk“ bezeichnet jedes Lieferantennetzwerk.

„Drittanbieter-Systeme“ sind alle lieferanteneigenen Computer-, Anwendungs- oder Netzwerksysteme, die für den Zugriff, die Speicherung oder Verarbeitung von BT-Informationen verwendet werden oder an der Bereitstellung der Lieferungen beteiligt sind.

Interpretation

21.2 Alle Wörter, die den Begriffen „einschließlich“, „einschließen“, „insbesondere“, „zum Beispiel“ oder ähnlichen Ausdrücken folgen, werden als illustrativ ausgelegt und schränken den Sinn der diesen Begriffen vorausgehenden Wörter, Beschreibungen, Definitionen, Phrasen oder Begriffe nicht ein.

21.3 Jedes Mal, wenn das Recht oder die Verpflichtung einer Vertragspartei als ein Recht oder eine Verpflichtung ausgedrückt wird, das bzw. die sie ausüben oder erfüllen **„kann“**, liegt die Option zur Ausübung oder Erfüllung dieses Rechts oder dieser Verpflichtung im alleinigen Ermessen dieser Vertragspartei.

21.4 Wenn auf einen Hyperlink (**„URL“**) verwiesen wird, so ist dieser Verweis auf eine solche Online-Ressource, die über diese URL oder eine andere Ersatz-URL, die der betreffenden Partei von Zeit zu Zeit mitgeteilt wird, zugänglich.

Fassung	Beschreibung	Autor	Datum
5.0	Gesetzgebung zum Telecommunications (Security) Act 2021 (TSA) und die Annahme des CIS durch BT	Jemma Turner	25/10/22
5.1	Änderung von 14.9 TLS	Jemma Turner	17/04/23
5.2	Änderungen verschiedener Klauseln zur Einbindung von TSA und Schwachstellen	Jemma Turner	30/11/23

ANHANG 1 – Zusätzliche Sicherheitsanforderungen

Wenn es für den Drittanbieter erforderlich ist, auf als „VS – VERTRAULICH“ oder höher eingestufte Informationen zuzugreifen, diese zu speichern, zu verarbeiten oder zu übermitteln, erfüllt der Drittanbieter die BT-Sicherheitsanforderungen und zusätzlich die in diesem Anhang 1 aufgeführten Anforderungen. In allen Fällen ersetzt die Kontrolle auf höchster Ebene die an anderer Stelle dieser Sicherheitsanforderungen dokumentierten Anforderungen.

1. MITARBEITER

1.1 Alle vom Drittanbieter beschäftigten Personen, die Zugang zu als „VS – VERTRAULICH“ oder höher eingestuften Informationen oder erhöhte Privilegien für die Infrastruktur haben, die als „VS – VERTRAULICH“ oder höher eingestufte Informationen speichert, verarbeitet oder überträgt:

1.1.1 müssen vor der Einstellung mindestens einem Screening nach dem BPSS-Standard (Baseline Personnel Security Standard) unterzogen werden;

1.1.2 müssen eine Erklärung nach dem Official Secrets Act unterzeichnen; und

1.1.3 müssen am Zugriff auf Informationen oder System gehindert werden, sofern sie nicht die im entsprechenden Vertrag festgelegten Sicherheitsfreigaben haben.

2. SICHERHEITSTRAINING

2.1 Der Drittanbieter wird für alle Mitarbeiter, die Zugang zu als „VS – VERTRAULICH“ oder höher eingestuften Informationen oder erhöhte Privilegien für die Infrastruktur haben, die als „VS – VERTRAULICH“ oder höher eingestufte Informationen speichert, verarbeitet oder überträgt, bei Einstellung und mindestens jährlich in Auftrag geben. Dieses Training wird die Anforderungen an den Umgang mit Informationen in Übereinstimmung mit den Anforderungen des „His Majesty's Government Security Classification Scheme“ (Sicherheitsrisikoschema der Regierung Seiner Majestät) abdecken, wie in der BT-Anleitung zum Schutz von HMG-Informationen für Drittanbieter ausführlich beschrieben, die dem Drittanbieter durch BT zur Verfügung gestellt wird.

2.2 Der Drittanbieter aktualisiert die Stellenbeschreibung für alle Mitarbeiter die Zugang zu als „VS – VERTRAULICH“ oder höher eingestuften Informationen oder erhöhte Privilegien für die Infrastruktur haben, die als „VS – VERTRAULICH“ oder höher eingestufte Informationen speichert, verarbeitet oder überträgt, um die Teilnahme an der in Absatz 2.1 oben beschriebenen Schulung zu ermöglichen. Der Drittanbieter führt ein Protokoll über die Schulung, das BT auf Anfrage zur Verfügung gestellt werden muss.

3. ZUGANGSKONTROLLE

3.1 Wenn Mitarbeiter kündigen oder die Rolle wechseln, müssen ihre Zugriffsrechte innerhalb eines (1) Werktags in den entsprechenden Drittanbieter-Systemen entzogen werden.

3.2 Wenn die Mitarbeiter des Drittanbieters, einschließlich Auftragnehmer, Zeitarbeitnehmer und Leiharbeiter, über erhöhte Berechtigungen für die BT-Infrastruktur verfügen, muss der Drittanbieter BT innerhalb eines Werktags schriftlich benachrichtigen, wenn ein Mitarbeiter keinen Zugang zu den BT-Systemen mehr benötigt (z. B. wenn Mitarbeiter die Stelle wechseln oder die Rolle wechseln).

3.3 Wenn die Mitarbeiter des Drittanbieters, einschließlich Auftragnehmer, Zeitarbeitnehmer und Leiharbeiter, über erhöhte Berechtigungen für die BT-Infrastruktur verfügen, muss der Drittanbieter BT innerhalb eines Werktags schriftlich benachrichtigen, wenn ein Mitarbeiter keinen Zugang zu den BT-Räumlichkeiten mehr benötigt (z. B. wenn Mitarbeiter kündigen oder die Rolle wechseln).

4. BEWERTUNG UND KLASSIFIZIERUNG VON ANLAGEN

4.1 Der Drittanbieter wird zusätzliche Verfahren zur Handhabung von Informationen umsetzen, um die Anforderungen an den Umgang mit Informationen in Übereinstimmung mit den regelmäßig aktualisierten Anforderungen des „His Majesty's Government Security Classification Scheme“ (Sicherheitsrisikoschema der Regierung Seiner Majestät) zu erfüllen.

5. INCIDENT RESPONSE UND BERICHTSWESEN – SERVICE LEVEL AGREEMENTS

5.1 Der Drittanbieter wird über spezifische Service-Level-Vereinbarungen beraten, um den Prozess der Reaktion auf Vorfälle zu unterstützen. Diese können alle früheren Vereinbarungen, die in diesen Sicherheitsanforderungen dargelegt sind, ersetzen.

6. PRÜFUNG, TESTS UND ÜBERWACHUNG

6.1. Der Drittanbieter wird jeden Tag rund um die Uhr eine Sicherheitsüberwachung umsetzen, sofern dies durch BT für Infrastruktur des Drittanbieters, die die Verarbeitung, Speicherung oder Übertragung von als AMTLICH oder höher eingestufter Informationen unterstützt, festgelegt wird.

7. GESCHÄFTSKONTINUITÄT UND NOTFALLWIEDERHERSTELLUNG

7.1 Der Drittanbieter erstellt innerhalb von 30 Tagen nach Vertragsunterzeichnung einen Plan für die Geschäftskontinuität und die Notfallwiederherstellung in Übereinstimmung mit BS ISO 22301.

8. STANDORT

8.1. Sofern nicht anderweitig angegeben, muss sich der Dienst physisch innerhalb der physischen Grenzen des Vereinigten Königreichs oder ggf. des EWR befinden. Jede Remote-Unterstützung und/oder -Verwaltung des Dienstes durch den Anbieter von einem Offshore-Standort aus, darf nur in Übereinstimmung mit den Genehmigungsverfahren durchgeführt werden, die im zutreffenden Vertrag zwischen BT und der entsprechenden Regierungsabteilung festgelegt sind.

9. ZUSÄTZLICHE ANFORDERUNGEN FÜR „VS – VERTRAULICH“ ODER HÖHER

9.1 Alle vom Drittanbieter identifizierten Rollen, die Zugang zu als „VS – VERTRAULICH“ oder höher eingestuften Informationen, oder erhöhte Privilegien für Infrastruktur haben, die als „VS – VERTRAULICH“ oder höher eingestufte Informationen speichert, verarbeitet oder überträgt sind in der „OFFICIAL SENSITIVE Declaration“ zu dokumentieren. Die ausgefüllte „OFFICIAL SENSITIVE Declaration“ muss BT vor der Vertragsunterzeichnung bereitgestellt werden.

9.2 Wenn der Lieferant auf Informationen, die als „HMG OFFICIAL-SENSITIVE“ („VS – VERTRAULICH“) oder höher eingestuft sind, zugreifen, diese speichern, verarbeiten oder übermitteln muss, hat der Lieferant eine Sicherheitsrisikoberwertung des Personals für alle Rollen durchzuführen, die in der „OFFICIAL SENSITIVE Declaration“, Absatz 2, in Übereinstimmung mit den Anforderungen im Dokument National

Protective Security Authority (NPSA) Personnel Security Risk assessment – A Leitfaden (4. Ausgabe – Juni 2013 oder später) festgelegt sind.

ANHANG 1, ANLAGE 1 – VORLAGE „OFFICIAL SENSITIVE DECLARATION“

1. Systeme/Dienstleistungen im Auftragsumfang

Bitte führen Sie die Systeme und Dienstleistungen auf, die zur Unterstützung des HMG-Kunden bereitgestellt werden.

System	Dienstleistung

2. Drittanbieter-Rollen, die eine Sicherheitsfreigabestufe erfordern.

Rolle	Erforderliche Sicherheitsfreigabestufe
* z. B. DBA	SC

3. Vulnerability Management (Management von Schwachstellen)

System	Art der Schwachstellenbewertung	Häufigkeit

4. Prüfung, Tests und Überwachung

Systeme, die auf Empfehlung von BT jeden Tag rund um die Uhr überwacht werden sollen.

ANHANG 2, Telecommunications (Security) Act 2021 – Umstellung des Verhaltenskodex auf vertraglich definierte Sicherheitsanforderungen

Code-Nummerierung	Anforderung	BT-Sicherheitsanforderungsklausel
M1.02	Sicherheitstests an nach außen gerichteten Systemen mit Ausnahme von CPE sollten in der Regel mindestens alle zwei Jahre und in jedem Fall kurz nach einer wesentlichen Änderung durchgeführt werden.	17.3
M1.03	Geräte am Exposed Edge dürfen keine sensiblen Daten oder sicherheitskritischen Funktionen beherbergen.	17.3
M1.04	Physische und logische Trennung muss zwischen Exposed Edge und sicherheitskritischen Funktionen implementiert werden. (Beachten Sie, dass diese Maßnahme möglicherweise nicht erforderlich ist, sobald Datensätze und Funktionen kryptographisch vor Gefährdung geschützt werden können.)	17.3
M1.05	Zwischen dem Exposed Edge und kritischen oder sensiblen Funktionen, die Schutzmaßnahmen umsetzen, müssen Sicherheitsgrenzen bestehen.	17.3
M2.02	Jeder priviliegierte Zugang ist zu protokollieren.	3.56, 3.57
M2.06	Die zur Unterstützung des Anbieter-Netzwerks genutzte Infrastruktur liegt in der Verantwortung des Anbieters oder einer anderen Entität, die die Regularien, Maßnahmen und Aufsicht so einhält, wie sie für den Anbieter gelten (z. B. ein dritter Lieferant, mit dem der Anbieter eine vertragliche Bindung hat). Sofern der Anbieter oder eine andere Entität, die die Regularien einhält, die Verantwortung hat, soll diese Verantwortung das Festhalten an der Aufsicht über die Verwaltung dieser Infrastruktur umfassen (einschließlich Aufsicht über Verwaltungsaktivitäten, Personal mit Verwaltungszugang und Verwaltungsprozesse).	3.56, 3.57 und 4, 14
M5.05	Anbieter haben eine Ursachenanalyse für alle Sicherheitsvorfälle durchzuführen. Die Ergebnisse dieser Analyse werden auf eine angemessene Ebene eskaliert, zu der auch der Verwaltungsrat des Anbieters gehören kann.	3.36
M6.01	Nicht dauerhafte Zugangsdaten (z. B. Authentifizierung mit Benutzername und Passwort) müssen in einem zentralisierten Dienst mit angemessener rollenbasierter Zugriffskontrolle gespeichert werden, der entsprechend relevanter Änderungen an Rollen und Verantwortlichkeiten innerhalb der Organisation aktualisiert werden muss.	3.44

M6.02	Privilegierter Zugriff muss über Konten mit eindeutiger Benutzer-ID und Authentifizierungsdaten für jeden Benutzer erfolgen und darf nicht geteilt werden.	3.47
M6.04	Alle „Break-Glass“-privilegierten Benutzerkonten sollen eindeutige, starke Zugangsdaten für jedes einzelne Teil der Netzwerkausrüstung haben.	3.48
M6.05	Standard- und hartkodierte Konten müssen deaktiviert werden.	16.16
M8.05	Anbieter müssen alle Geräte erfassen, die in ihren Netzwerken eingesetzt werden, und proaktiv – mindestens jährlich – deren Exposition bewerten, für den Fall, dass der Drittanbieter nicht mehr in der Lage ist, das Gerät zu unterstützen.	16.16, 16.5
M8.06	Anbieter müssen Standardpasswörter und -konten für alle Geräte im Netzwerk entfernen und sollten unverschlüsselte Verwaltungsprotokolle deaktivieren. Falls unverschlüsselte Verwaltungsprotokolle nicht deaktiviert werden können, müssen Anbieter die Verwendung dieser Protokolle soweit wie möglich einschränken und minimieren.	16.16 und 17.1
M8.07	Anbieter müssen sicherstellen, dass die gesamte sicherheitsrelevante Protokollierung für alle Netzwerkgeräte aktiviert ist und an die Protokollsystem des Netzwerks gesendet wird.	16.5
M8.08	Anbieter müssen kritische Sicherheits-Patches wann immer möglich vor Funktionsupdates priorisieren.	14.1 und 16.12
M8.12	Bei SIM-Karten mit festem Profil muss der Anbieter sicherstellen, dass sensible SIM-Daten während ihres gesamten Lebenszyklus sowohl vom Hersteller der SIM-Karte als auch innerhalb des Betreibernetzes angemessen geschützt werden, da bei Verlust dieser Informationen die Ausfallsicherheit und Vertraulichkeit des Netzes gefährdet sind.	19.1
M8.13	Bei SIM-Karten mit festem Profil muss die Vertraulichkeit, Integrität und Verfügbarkeit der mit dem Hersteller der SIM-Karte geteilten sensiblen Daten der SIM-Karte in jeder Phase ihres Lebenszyklus geschützt sein.	19.1
M10.04	Der Incident-Management-Prozess des Anbieters und der ihrer Drittanbieter müssen gegenseitige Unterstützung bei der Lösung von Vorfällen bieten.	3.31-3.36
M10.06	Der Anbieter muss festlegen, welche Information dem Drittanbieter zugänglich zugemacht wird, um sicherzustellen, dass es das notwendige Minimum zur Erfüllung ihrer Funktion ist. Anbieter müssen Kontrollen auf dieser Information platzieren und den	3.44

	Drittanbieterzugriff auf das notwendige Minimung zur Erfüllung der Geschäftsfunktion beschränken.	
M10.09	Wenn ein Netzwerk- oder Benutzerdaten die Kontrolle des Anbieters verlassen, muss der Anbieter vertraglich fordern und überprüfen, dass die Daten als Konsequenz ordnungsgemäß geschützt sind. Dies muss die Bewertung der Kontrolle des Drittanbieters umfassen, um sicherzustellen dass die Anbieterdaten nur für bestimmte Mitarbeiter und von bestimmten Standorten sichtbar und zugänglich sind.	3.44-3.50 und 14, 15, 17 und 18
M10.11	Anbieter stellen vertraglich sicher, dass Drittanbieter den Anbieter innerhalb von 48 Stunden benachrichtigen, nachdem ihnen Sicherheitsvorfälle bekannt werden, die das Auftreten einer Sicherheitsgefährdung verursacht oder dazu beigetragen haben, oder wenn sie ein erhöhtes Risiko für das Auftreten einer solchen Gefährdung identifizieren. Dies schließt Vorfälle im Entwicklungsnetzwerk des Anbieters oder deren Firmennetzwerk ein, ist jedoch nicht darauf beschränt.	3.33
M10.12	Anbieter stellen vertraglich sicher, dass Drittanbieter den Anbieter bei Untersuchungen von Vorfällen unterstützen, die das Auftreten einer Sicherheitsgefährdung in Bezug auf den Erstanbieter verursachen oder dazu beitragen, oder über ein erhöhtes Risiko des Auftretens einer solchen Gefährdung.	3.31-3.36
M10.13	Anbieter stellen vertraglich sicher, dass die Drittanbieter die Hauptursache eines Sicherheitsvorfalls, der zu einem Sicherheitsverlust im Vereinigten Königreich führen könnte, innerhalb von 30 Tagen ermitteln und melden und festgestellte Sicherheitsmängel beheben.	3.35
M10.16	Anbieter stellen vertraglich sicher, dass die Drittanbieter Sicherheitsprüfungen, -bewertungen oder -tests, die vom Anbieter in Bezug auf die Sicherheit des eigenen Netzwerks des Anbieter erforderlich sind, unterstützen – soweit dies angemessen ist –, einschließlich solcher, die notwendig sind, um die Sicherheitsanforderungen in diesem Dokument zu bewerten.	5.1-5.2, 6.1-6.3
M10.18	Der Anbieter muss das Recht behalten, die Berechtigungen der Konten festzulegen, die von Administratoren des Drittanbieters genutzt werden, um auf sein Netzwerk zuzugreifen.	16.23
M10.21	Anbieter müssen das vertragliche Recht haben, die Mitglieder des Administrationspersonals des Drittanbieters zu kontrollieren, die in die Bereitstellung der Administratordienste des Drittanbieters eingebunden sind, einschließlich dem Administrator von Drittanbietern vorzuschreiben, dass ein Mitglied des Personal keinen weiteren Zugang zum Netzwerk hat.	13.1

M10.24	Anbieter stellen vertraglich sicher, dass die Administratoren von Drittanbietern technische Kontrollen durchführen, um zu verhindern, dass ein Anbieter oder dessen Netzwerk einen anderen Anbieter oder dessen Netzwerk beeinträchtigt.	16.13
M10.25	Anbieter stellen vertraglich sicher, dass die Administratoren von Drittanbietern eine logische Trennung innerhalb des Netzwerkes der Administratoren von Drittanbietern durchführen, um Kundendaten und Netzwerke zu trennen.	16.14
M10.26	Anbieter stellen vertraglich sicher, dass die Administratoren von Drittanbietern die Trennung zwischen Verwaltungsumgebungen von Drittanbietern implementieren, die für verschiedene Anbieternetze verwendet werden.	16.14
M10.27	Anbieter stellen vertraglich sicher, dass die Administratoren von Drittanbietern Sicherheitsfunktionen an der Grenze zwischen dem Netzwerk der Administratoren von Drittanbietern und dem Netzwerk des Anbieters implementieren und durchsetzen.	16.14
M10.28	Anbieter stellen vertraglich sicher, dass die Administratoren von Drittanbietern technische Kontrollen durchführen, um das Potenzial für Benutzer oder Systeme zu begrenzen, sich negativ auf mehr als einen Anbieter auszuwirken.	16.14
M10.29	Anbieter stellen vertraglich sicher, dass Administratoren von Drittanbietern logisch unabhängige privilegierte Zugriffsarbeitsplätze pro Anbieter implementieren.	16.14
M10.30	Anbieter stellen vertraglich sicher, dass die Administratoren des Drittanbieters unabhängige administrative Domänen und Konten pro Anbieter implementieren.	16.14
M10.33	Der Anbieter stellt vertraglich sicher, dass der Administrator des Drittanbieters die Aktivitäten der Belegschaft des Administrators des Drittanbieters beim Zugriff auf das Netzwerk des Anbieters überwacht und prüft.	3.56, 3.57
M10.34	Der Anbieter fordert vertraglich vom Administrator des Drittanbieters alle Protokolle in Bezug auf die Sicherheit des Netzwerks des Administrators des Drittanbieters in dem Maß wie solche Protokolle sich auf den Zugriff auf das Netzwerk des Anbieters beziehen.	3.56, 3.57 und 16.23
M10.35	Anbieter fordern, dass Netzwerke vom Administrator des Drittanbieters, die den Anbieter beeinflussen könnten, demselben Prüfniveau unterliegen, das der Anbieter auf	16.18

	sich selbst anwendet (z. B. TBEST-Test als Set für den Anbieter durch Ofcom von Zeit zu Zeit).	
M10.36	Anbieter stellen vertraglich sicher, dass die Lieferanten der Netzausrüstung ihnen eine „Sicherheitserklärung“ darüber mitteilen, wie sie sichere Ausrüstungen herstellen, und sicherstellen, dass sie die Sicherheit der Ausrüstungen während ihrer gesamten Lebensdauer aufrechterhalten. Es wird empfohlen, dass eine solche Erklärung alle Aspekte abdeckt, die im Rahmen der Sicherheitsbewertung des Anbieters (VSA, Vendor Security Assessment) beschrieben werden (siehe Anhang B). Anbieter sollten ihre Lieferanten ermutigen, eine Antwort auf die Sicherheitsbewertung des Anbieters zu veröffentlichen.	16.15
M10.38	Anbieter stellen durch vertragliche Vereinbarungen sicher, dass die Sicherheitserklärung des Lieferanten der Netzausrüstung auf angemessener Führungsebene unterzeichnet wird.	16.15
M10.39	Wenn der Lieferant der Netzausrüstung behauptet, eine international anerkannte Sicherheitsbewertung oder Zertifizierung seiner Ausrüstung (wie Common Criteria oder NESAS) erhalten zu haben, müssen die Anbieter vertraglich von den Lieferanten der Ausrüstung verlangen, ihnen die vollständigen Erkenntnisse mitzuteilen, die diese Bewertung oder dieses Zertifikat belegen.	16.17
M10.40	Anbieter stellen vertraglich sicher, dass Lieferanten der Netzausrüstung einen Standard einhalten, der nicht niedriger ist als die „Sicherheitserklärung“ des Lieferanten der Netzausrüstung.	16.16
M10.41	Anbieter müssen vertraglich von Lieferanten der Netzausrüstung fordern, aktuelle Leitlinien für den sicheren Einsatz der Ausrüstung vorzulegen.	16.16
M10.42	Anbieter müssen vertraglich von Lieferanten der Netzausrüstung fordern, dass alle Geräte und alle Software- und Hardware-Teilkomponenten für die Dauer des Vertrages unterstützt werden. Die Dauer der Unterstützung von Hardware und Software wird im Vertrag festgeschrieben.	16.16
M10.43	Anbieter stellen vertraglich sicher, dass Lieferanten der Netzausrüstung Angaben (Produkt und Version) zu wichtigen Fremdkomponenten und Abhängigkeiten, einschließlich Open-Source-Komponenten sowie Zeitraum und Umfang der Unterstützung, machen.	16.16
M10.44	Soweit dies für die besondere Nutzung von Ausrüstungen durch einen Anbieter relevant ist, verlangen die Anbieter vertraglich von Drittanbietern, alle Sicherheitsprobleme, die ein Sicherheitsrisiko für das Netz oder den Dienst eines Anbieters darstellen, die in ihren Produkten entdeckt	16.16

	wurden, innerhalb einer angemessenen Frist nach der Benachrichtigung zu beheben und in der Zwischenzeit regelmäßig über den Fortschritt zu informieren. Dies umfasst alle von der Sicherheitsanfälligkeit betroffenen Produkte und nicht nur das Produkt, für das die Sicherheitsanfälligkeit gemeldet wurde.	
M10.46	Anbieter stellen sicher, dass ihre Verträge die Weitergabe von Einzelheiten zu Sicherheitsfragen ermöglichen, soweit dies angemessen ist, um die Ermittlung und Verringerung der Risiken von Sicherheitseinbußen zu unterstützen, die in Bezug auf das öffentliche elektronische Kommunikationsnetz oder den öffentlichen elektronischen Kommunikationsdienst infolge von Handlungen oder Unterlassungen von Drittanbietern auftreten.	3.33 und 16.19
M10.47	Anbieter stellen vertraglich sicher, dass Lieferanten der Netzwerkausrüstung kritische Sicherheitspatches getrennt von Funktionsveröffentlichungen liefern, um die Geschwindigkeit, mit der der Patch bereitgestellt werden kann, zu maximieren.	14.1 und 16.12
M11.02	Alle persistenten Anmeldeinformationen und Geheimnisse (z. B. für den Zugang zu Break Glass) müssen geschützt werden und niemandem außer der/den verantwortlichen Person(en) im Notfall zur Verfügung stehen.	3.44
M11.03	Die zentrale Speicherung dauerhafter Anmeldeinformationen ist durch Hardware zu schützen. Zum Beispiel könnte auf einem physischen Host das Laufwerk mithilfe eines TPM verschlüsselt werden. Wenn ein virtueller Computer (VM) zur Bereitstellung eines zentralen Speicherdienstes verwendet wird, müssen diese VM und die darin enthaltenen Daten ebenfalls verschlüsselt sein, einen sicheren Bootvorgang verwenden und so konfiguriert sein, dass sichergestellt ist, dass sie nur in einer geeigneten Umgebung gebootet werden kann. Dadurch soll sichergestellt werden, dass Daten nicht aus der Betriebsumgebung entfernt und darauf zugegriffen werden kann.	3.45
M16.12	Protokolle für Netzwerkgeräte in sicherheitskritischen Funktionen müssen vollständig aufgezeichnet und 13 Monate lang für Audits zur Verfügung gestellt werden.	3.56, 3.57
M16.21	Anzeichen von potenziell anormaler Aktivität müssen unverzüglich bewertet, untersucht und angegangen werden.	3.56, 3.57
M21.02	Die vom Anbieter gemäß Regel 3 Absatz 3 Buchstabe f zu treffenden Maßnahmen sollten in der Regel darin bestehen – soweit dies nach vernünftigem Ermessen durchführbar ist – sicherzustellen, dass sich die Geräte, die die Netzaufsichtsfunktionen des Anbieters erfüllen, im Vereinigten Königreich befinden und mit im Vereinigten Königreich ansässigem Personal betrieben werden.	16.21

M21.03	Der Anbieter muss eine britisch-basierte technische Fähigkeit zur Bereitstellung Fachkompetenz zum Betrieb der Netzwerke des Anbieters im Vereinigten Königreich und den Risiken für die Netzwerke des Anbieters im Vereinigten Königreich beibehalten.	16.2, 16.20-16.22
M21.04	Werden Daten außerhalb gespeichert, muss der Anbieter eine Liste der Orte aufbewahren, an denen die Daten gespeichert werden. Das Risiko aufgrund der Speicherung der Daten an diesen Standorten, einschließlich aller Risiken im Zusammenhang mit dem lokalen Datenschutzrecht, wird im Rahmen der Risikomanagementprozesse des Anbieters verwaltet.	3.8

ANHANG 3, NIS 2 Durchführungsverordnung - Umwandlung des Verhaltenskodex in die vertraglichen Sicherheitsanforderungen

Im Folgenden wird auf Bestimmungen des Anhangs der Durchführungsverordnung der Kommission zur Festlegung von Vorschriften für die Anwendung der Richtlinie (EU) 2022/2555 hinsichtlich der technischen und methodischen Anforderungen an Maßnahmen zum Cybersicherheitsrisikomanagement ("NIS-2-Durchführungsverordnung") verwiesen

Anhang der Durchführungsverordnung NIS 2	Anforderung	Klausel über die Sicherheitsanforderung von BT
5.1.4	Basierend auf der Sicherheitspolitik der Lieferkette und unter Berücksichtigung der Ergebnisse der durchgeführten Risikobewertung ... Die betreffenden Stellen stellen sicher, dass in ihren Verträgen mit den Lieferanten und Dienstleistern gegebenenfalls im Rahmen von Dienstleistungsvereinbarungen Folgendes festgelegt ist:	See below
5.1.4.a	Cybersicherheitsanforderungen an die Lieferanten oder Diensteanbieter, einschließlich der in Nummer 6.1 genannten Anforderungen an die Sicherheit beim Erwerb von IKT-Diensten oder -Produkten. 6.1 Erfordert: a) Sicherheitsanforderungen, die für die zu erwerbenden IKT-Dienste oder -Produkte gelten; b) Anforderungen an Sicherheitsupdates während der gesamten Lebensdauer der IKT-Dienste oder -Produkte oder deren Ersatz nach Ablauf des Supportzeitraums; c) Informationen über die Hardware- und Softwarekomponenten, die in den IKT-Diensten oder -Produkten verwendet werden; d) Informationen, die die implementierten Cybersicherheitsfunktionen der IKT-Dienste oder IKT-Produkte und die für ihren sicheren Betrieb erforderliche Konfiguration beschreiben; e) die Gewähr, dass die IKT-Dienste oder -Produkte die Sicherheitsanforderungen gemäß Buchstabe a erfüllen; f) geeignete Methoden zur Validierung, mit denen überprüft werden kann, ob die erbrachten IKT-Dienste oder -Produkte den angegebenen Sicherheitsanforderungen entsprechen, sowie die Dokumentation der Validierungsergebnisse..	5, 16.15, 16.16
5.1.4.b	Anforderungen an Fähigkeiten und Schulungen und gegebenenfalls Zertifizierungen, die von den	4.6, 7

	Mitarbeitern des Lieferanten oder Dienstleisters verlangt werden	
5.1.4.c	Anforderungen an die Überprüfung des Hintergrunds der Mitarbeiter der Lieferanten und Dienstleister	16.10, Portal für Lieferantenvereinbarungen und -richtlinienSelling to BT
5.1.4.d	eine Verpflichtung für Lieferanten und Diensteanbieter, die betroffenen Stellen unverzüglich über Sicherheitsvorfälle zu informieren, die ein Risiko für die Sicherheit des Netzes und der Informationssysteme dieser Einrichtungen darstellen	3.33
5.1.4.e	Bestimmungen über Reparaturzeiten	3.39, 14.1, 16.12
5.1.4.f	das Recht auf Audit oder das Recht, Auditberichte zu erhalten	5
5.1.4.g	eine Verpflichtung für Lieferanten und Diensteanbieter, mit Schwachstellen umzugehen, die ein Risiko für die Sicherheit des Netzes und der Informationssysteme der betreffenden Unternehmen darstellen	14.1, 16.12
5.1.4.h	Anforderungen an die Vergabe von Unteraufträgen und, sofern die betreffenden Stellen die Vergabe von Unteraufträgen zulassen, Cybersicherheitsanforderungen an Unterauftragnehmer im Einklang mit den in Buchstabe a genannten Cybersicherheitsanforderungen	3.4
5.1.4.i	Verpflichtungen der Lieferanten und Dienstleister bei Beendigung des Vertrags, wie z. B. das Abrufen und Beseitigen der Informationen, die die Lieferanten und Dienstleister bei der Ausübung ihrer Aufgaben erhalten haben	3.23, 3.24