Inhalt

1. Einführung

1.1 Dieses Dokument legt die Sicherheitsanforderungen von BT fest und gilt für alle Drittanbieter, die für oder im Namen der BT Group einschließlich Openreach, EE und PlusNet arbeiten. Für den Rest des Dokuments werden diese als „BT“ bezeichnet.

1.2 Diese Sicherheitsanforderungen gelten zusätzlich zu und unbeschadet aller anderen Verpflichtungen des Drittanbieters im Vertrag.

1.3 Alle Standards, auf die in diesem Dokument Bezug genommen wird, finden Sie an folgender Stelle. Standards für Drittanbieter

2. Anforderungen für eingeschränkten Zugang/Zugriff

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 Good Industry Security Practices der Branche zu schützen.

3. Allgemeine Informationssicherheit

3.1 Auf angemessene 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 Dienstleistungen oder der Art und Weise, wie sie erbracht werden, geben, kann BT während der Laufzeit einen Vertragszusatz herausgeben, 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 Der Drittanbieter muss mindestens einmal jährlich oder bei wesentlichen Änderungen der Dienstleistungen oder der Art und Weise, wie sie erbracht werden, diese Sicherheitsanforderungen und die damit verbundenen Standards überprüfen, um sicherzustellen, dass er weiterhin alle geltenden Sicherheitskontrollen erfüllt.

3.4 Wenn der Drittanbieter Verpflichtungen aus dem Vertrag an Subunternehmer vergibt, muss der Drittanbieter 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.

3.5 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 dem Drittanbieter vereinbart oder dies ist durch geltende Gesetze vorgeschrieben.

3.6 Wenn die Dienste direkt einen Vertrag mit der britischen Regierung unterstützen, muss der Drittanbieter die aktuellste Version von Cyber Essentials Plus einhalten.

3.7 Der Drittanbieter muss sicherstellen, dass die BT-Informationen gemäß den Sicherheitsvorgaben in den folgenden Standards behandelt werden:

- Datenklassifizierungs- und Datenverarbeitungsstandard für Drittanbieter V4.0
- Unser Standard für Drittanbieter-Sicherheitsmaßnahmen

  Abschnitt 1 Rollen und Verantwortlichkeiten.

  Abschnitt 2 Governance.

  Abschnitt 3 Incident Management.

  Abschnitt 4 Änderungsmanagement.

  Abschnitt 5 Cyber-Risiko- und Bedrohungsmanagement.

  Abschnitt 6 Identitätsmanagement und Zugangskontrolle.

  Abschnitt 10 Datenklassifizierung und Datenschutz.

  Abschnitt 12 Verhinderung von Datenlecks.

  Abschnitt 13 PCI-DSS (wenn Teil des Dienstleistungsumfangs).

  Abschnitt 19 Schwachstellen Management.

  Abschnitt 22 Sicherheit, Protokollierung und Überwachung.

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 Sicherheitsmaßnahmen und -standards des Drittanbieters und von BT durch formelle Verfahren und Disziplinarmaßnahmen vorgehen. Dies kann bedeuten, dass:

4.2.1 dem Mitarbeiter der Zugriff auf BT-Systemen oder BT-Informationen entzogen wird, oder

4.2.2 der Mitarbeiter von Arbeiten, die mit der Bereitstellung des Dienstes verbunden sind, ausgeschlossen wird.

Darüber hinaus sollte der Drittanbieter sicherstellen, 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, soweit dies gesetzlich zulässig ist, eine vertrauliche Möglichkeit, 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.

- Wenn der Mitarbeiter des Drittanbieters dem Dienst nicht mehr zugewiesen wird, sollten nach Wahl von BT alle physischen Vermögenswerte oder Informationen von BT, die sich im Besitz des Mitarbeiters des Drittanbieters befinden, entweder: an das entsprechende operative Team von BT zurückgegeben werden;
- oder in Übereinstimmung mit dem Datenklassifizierungs- und Datenverarbeitungsstandard für Drittanbieter V4.0 vernichtet werden.

4.4 Der Drittanbieter muss sicherstellen, dass geeignete Verfahren in Bezug auf das Personal des Drittanbieters vorhanden sind, um die Kontrollen gemäß den folgenden Standards durchzuführen:

- Unser Standard für Drittanbieter-Sicherheitsmaßnahmen V1.1 – Abschnitte

  Abschnitt 5 Soziale Medien

  Abschnitt 23 Schulung und Bewusstsein

5. Prüfung und Sicherheitsüberprüfung

5.1 Unbeschadet aller anderen Prüfungsrechte, die BT möglicherweise hat, gewährt der Drittanbieter, um die Einhaltung dieser Sicherheitsanforderungen und der damit verbundenen Standards durch den Drittanbieter zu beurteilen, 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 Benachrichtigung durch BT oder innerhalb eines zwischen den Parteien vereinbarten Zeitraums auf Kosten des Drittanbieters durchzuführen.

5.3 Sollte BT eine unabhängige Prüfung des Drittanbieters durchführen müssen und der Drittanbieter sich als nicht konform mit den Grundsätzen und Praktiken der ISO/IEC 27001:2013 erweisen, muss der Drittanbieter auf eigene Kosten die Maßnahmen ergreifen, die erforderlich sind, um die erforderliche Konformität zu erreichen, und alle Kosten, die BT durch die Durchführung einer solchen Prüfung entstehen, in voller Höhe erstatten.

6. Recht auf Überprüfung

6.1 Der Drittanbieter muss BT ein Recht auf Überprüfung gewähren, und zwar in Übereinstimmung mit:

- Unserem Standard für Drittanbieter-Sicherheitsmaßnahmen V1.1 – Abschnitt

  Abschnitt 24 Recht auf Überprüfung.

7. Sicherheitszertifikate

7.1 Die Systeme, Dienstleistungen, zugehörigen Dienste, Prozesse und physischen Standorte des Drittanbieters müssen mit der Norm ISO/IEC 27001:2013 (oder Zertifizierungen, die gleichwertige Kontrollen nachweisen, unterstützt durch einen unabhängigen Prüferbericht) und jeder geänderten oder zukünftigen Version des Standards konform sein und diese kontinuierlich erfüllen. Diese Compliance muss gewährleistet werden, entweder durch:

7.1.1 die Zertifizierung des ISMS des Drittanbieters durch ein UKAS oder eine international gleichwertige zugelassene Zertifizierungsstelle, wenn der Geltungsbereich und die Erklärung der Anwendbarkeit von BT validiert wurde; oder

7.1.2 ein von BT spezifiziertes bilaterales Prüf- und Testverfahren.

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

7.3 Sollte sich der Geltungsbereich des Zertifikats oder der Erklärung zur Anwendbarkeit zu irgendeinem Zeitpunkt ändern, muss der Drittanbieter diese Änderungen zur erneuten Validierung mit Hilfe des Änderungskontrollverfahrens (oder, falls es kein Änderungskontrollverfahren gibt, durch den Änderungsprozess) einreichen. Der Drittanbieter muss BT innerhalb von 2 Arbeitstagen über jede größere Nichtkonformität informieren, die von der Zertifizierungsstelle oder dem Drittanbieter festgestellt wird.

8. Physische Sicherheit - BT-Räumlichkeiten

8.1 Wenn der Drittanbieter in den Räumlichkeiten von BT arbeitet, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Unser Standard für Drittanbieter-Sicherheitsmaßnahmen V1.1 – Abschnitt

Abschnitt 25 Physische Sicherheit - BT-Räumlichkeiten

9. Physische Sicherheit in den Räumlichkeiten von Drittanbietern

9.1 Wenn Drittanbieter-Räumlichkeiten für die Erbringung der Leistung genutzt werden, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Unser Standard für Drittanbieter-Sicherheitsmaßnahmen V1.1 – Abschnitt

Abschnitt 9. Physische Sicherheit in den Räumlichkeiten von Drittanbietern **mit Ausnahme** der Sicherheitsmaßnahmen 9.10 und 9.11 für die Bereitstellung der Hosting-Umgebung für BT-Geräte.

10. Bereitstellung einer Hosting-Umgebung für BT-Geräte.

10.1 Wenn Drittanbieter-Räumlichkeiten für die Bereitstellung einer Hosting-Umgebung für BT-Geräte genutzt werden, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitt

Abschnitt 9. Physische Sicherheit in den Räumlichkeiten von Drittanbietern mit Ausnahme der Sicherheitsmaßnahmen 9.10 und 9.11 für die Bereitstellung der Hosting-Umgebung für BT-Geräte.

11. Sichere Software-Entwicklung

11.1 Wenn der Drittanbieter Software oder Systeme zur Verfügung stellt, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitt

Abschnitt 17 (17.1 und 17.2) Sichere Software-Entwicklung

12. ESCROW

12.1 Wenn zum Schutz aller Parteien eine ESCROW-Hinterlegung erforderlich ist, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitt

Abschnitt 17 (nur 17.3) Sichere Software-Entwicklung

13. Zugriff auf BT-Systeme

13.1 Wenn Systeme von Drittanbietern oder Personal von Drittanbietern Zugang/Anschluss an BT-Systeme erfordern, gelten die Sicherheitsmaßnahmen des folgenden Standards.

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitt

Abschnitt 8 Zugriff auf BT-Systeme

14. Drittanbieter-Systeme, die BT-Informationen speichern

14.1 Wenn Drittanbieter-Systeme verwendet werden, gelten die Sicherheitsmaßnahmen des folgenden Standards:

Datenklassifizierungs-und Datenverarbeitungsstandard für Drittanbieter V4.0

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitte

Abschnitt 7 Verwaltung von Informationsbeständen.

Abschnitt 11 Kryptographie.

Abschnitt 16 Systemkonfiguration.

Abschnitt 18 Anti-Malware-Schutz.

Abschnitt 21 Minderung von Denial of Service.

15. Drittanbieter-Systeme, die BT-Informationen hosten

15.1 Wenn der Drittanbieter die Informationen von BT hosted, müssen die Räumlichkeiten über ein gültiges ISO/IEC 27001-Zertifikat für das Sicherheitsmanagement verfügen (oder über eine oder mehrere Zertifizierungen, die gleichwertige Kontrollen nachweisen, die durch einen unabhängigen Prüfbericht unterstützt werden).

15.2 Es gelten die in den folgenden Standards:

- Datenklassifizierungs- und Datenverarbeitungsstandard für Drittanbieter V4.0
- Unser Standard für Drittanbieter- V1.1 – Abschnittr

  Abschnitt 7 Verwaltung von Informationsbeständen.

  Abschnitt 11. Kryptographie.

Abschnitt 16 Systemkonfiguration.

Abschnitt 18 Anti-Malware-Schutz.

Abschnitt 21 Minderung von Denial of Service.

16. Netzwerksicherheit – eigenes Netzwerk von BT

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

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitt

  Abschnitt 26 Netzwerksicherheit – eigenes Netzwerk von BT.

17. Sicherheit des Netzwerks von Drittanbietern

17.1 Wenn das eigene Netzwerk des Drittanbieters genutzt wird, um auf BT-Informationen zuzugreifen, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitte

  Abschnitt 16 Systemkonfiguration.

  Abschnitt 20 Netzwerkintegrität.

18. Cloud-Sicherheit

18.1 Wenn der Drittanbieter BT Cloud-Services zur Verfügung stellt, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Unser Standard für Drittanbieter- Sicherheitsmaßnahmen V1.1 – Abschnitt

  Abschnitt 14 Cloud / Online-Computing.

19. Contact Center

19.1 Wenn der Drittanbieter BT Contact Center-Services zur Verfügung stellt, gelten die Sicherheitsmaßnahmen des folgenden Standards:

- Standard für Drittanbieter-Contact-Centre V1.0

20. Von HMG als „OFFICIAL“ oder höher eingestufte Informationen

20.1 Die zusätzlichen Sicherheitsanforderungen, die in Anhang 1 dieser Sicherheitsanforderungen aufgeführt sind, gelten für alle Drittanbieter, die als „Official Sensitive“ eingestufte Informationen in Übereinstimmung mit dem von Zeit zu Zeit aktualisierten Klassifikationsschema der Regierung Ihrer Majestät speichert, verarbeiten oder übermitteln.

20.2 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.

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**“ bedeutet 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“ sind 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 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.

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

„**Cyber Essentials Plus**“ bedeutet ein von der britischen Regierung unterstütztes Programm, das Unternehmen dabei helfen soll, sich gegen die üblichen Cyber-Angriffe zu schützen.

“**Escrow**” bedeutet 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).

„**Gute Sicherheitspraxis in der Industrie - Good Industry Security Practice**“ bedeutet in Bezug auf jedes Unternehmen und alle Umstände die Umsetzung der Sicherheitspraktiken, -richtlinien, -standards und -werkzeuge, die vernünftigerweise und normalerweise von einer qualifizierten und erfahrenen Person erwartet werden, die unter gleichen oder ähnlichen Umständen mit derselben Art von Tätigkeit befasst ist.

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

„**Official Sensitive Declaration** “ ist 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.

„**Sicherheitsanforderungen**“ sind die Anforderungen in diesem Dokument, welches von Zeit zu Zeit aktualisiert wird.

„**Subunternehmer**“ ist ein 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.

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

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

„**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 bezieht sich 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 ist.

ANHANG 1 – Zusätzliche Sicherheitsanforderungen

Wenn der Drittanbieter verpflichtet ist, auf „HMG Official Sensitive“ Informationen zuzugreifen, diese zu speichern, zu verarbeiten oder zu übermitteln, erfüllt der Drittanbieter diese Sicherheitsanforderungen und zusätzlich die in diesem Anhang 1 aufgeführten Anforderungen und BT stellt die ausgefüllte „Official Sensitive Declaration“ vor der Vertragsunterzeichnung zur Verfügung. In allen Fällen ersetzt die Sicherheitsanforderung auf höchster Ebene die an anderer Stelle in diesen Sicherheitsanforderungen für die in der offiziellen Sensibilitätserklärung aufgeführten Dienste und Systeme dokumentierten Anforderungen.

1. MITARBEITER

1.1. Alle vom Drittanbieter identifizierten Rollen, die Zugang zu als „Official Sensitive“ eingestuften Informationen oder erhöhte Privilegien für die Infrastruktur haben, die als „Official Sensitive“ eingestufte Informationen speichert, verarbeitet oder überträgt, werden in der Official Sensitive Declaration dokumentiert.

1.2. Mitarbeiter von Drittanbietern, die in der Official Sensitive Declaration genannten Rollen eingesetzt werden:

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

1.2.2. müssen eine Erklärung nach dem Official Secrets Act unterzeichnen; und

1.2.3. die nicht in der Lage sind, die erforderlichen Sicherheitsfreigaben zu erhalten, müssen am Zugriff auf Informationen oder Systeme gehindert werden.

2. SICHERHEITSTRAINING

2.1. Der Drittanbieter wird bei der Einstellung und mindestens jährlich eine Sicherheitsschulung in Auftrag geben, die die Anforderungen an den Umgang mit Informationen abdeckt, die als „Official “ oder „Official Sensitive“ eingestuft sind, entsprechend den Anforderungen des „Her Majesty's Government Security Classifications Scheme“ ,wie in der BT-Anleitung zum Schutz von HMG-Informationen für Drittanbieter: detailliert beschrieben.

2.2. Der Drittanbieter aktualisiert die Stellenbeschreibungen für die in der Official Sensitive Declaration dokumentierten Rollen, 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 die Stelle verlassen oder die Rolle wechseln, müssen ihre Zugriffsrechte innerhalb eines (1) Werktags bei 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 die Stelle wechseln oder die Rolle wechseln).

4. BEWERTUNG UND KLASSIFIZIERUNG VON VERMÖGENSWERTEN

4.1. Der Drittanbieter führt zusätzliche Verfahren zur Handhabung von Informationen ein, um die Anforderungen an die Handhabung „Official“ oder „Official Sensitive“ Informationen in Übereinstimmung mit den Anforderungen des Her Majesty’s Government Security Classifications Scheme, das von Zeit zu Zeit aktualisiert wird, zu erfüllen.

5. INCIDENT RESPONSE UND BERICHTSWESEN – SERVICE LEVEL AGREEMENTS

5.1. Der Drittanbieter wird über spezifische Service-Level-Vereinbarungen informiert, 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 führt jeden Tag rund um die Uhr eine Sicherheitsüberwachung durch, sofern von BT spezifiziert.

6.2. Die Infrastruktur des Drittanbieters, die einer Sicherheitsüberwachung rund um die Uhr unterliegt, wird in der Official Sensitive Declaration dokumentiert.

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. ORT

8.1. Sofern von BT nicht anders angegeben, muss der Dienst physisch innerhalb der physischen Grenzen des Vereinigten Königreichs oder gegebenenfalls des EWR erbracht werden.

ANHANG 1, ANLAGE 1 -OFFICIAL SENSITIVE DECLARATION VORLAGE

1. Umfang Systeme/Dienstleistungen

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

System	Service

2. Drittanbieter-Rollen, die eine Sicherheitsfreigabestufe erfordern.

Rolle	Erforderliche Sicherheitsfreigabestufe
** z. B. DBA*	*SC*

3. Vulnerability Management

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.