Indice

1. Introduzione

1.1 Il presente documento definisce i Requisiti di sicurezza di BT e si applica a tutte le terze parti che lavorano per o per conto del Gruppo BT, compresi Openreach, EE e PlusNet, di seguito indicati come 'BT'.

1.2 Questi Requisiti di sicurezza si aggiungono a qualsivoglia altro obbligo stipulato nel Contratto a cui le terze parti devono adempiere, senza pregiudicarne la validità.

1.3 Tutti gli standard a cui si fa riferimento nel presente documento si trovano nella seguente posizione. Standard di terzi

2. Requisiti di Accesso limitato

2.1 Fatto salvo qualsiasi altro obbligo di riservatezza che la terza parte potrebbe essere tenuta a rispettare, qualora il Personale di detta Terza parte potesse accedere alle Informazioni BT, la terza parte deve:

2.2 Assicurarsi che le Informazioni BT non vengano divulgate ai membri del Personale della Terza parte, i quali non dovranno accedervi, se non necessario per la prestazione del Servizio; e

2.3 Implementare qualsiasi sistema e processo, sia tecnico che organizzativo, necessario a proteggere le Informazioni BT da una (i) distruzione accidentale o illecita, e (ii) perdita, alterazione, divulgazione non autorizzata delle, o Accesso alle, Informazioni BT conformemente alle *best practice* per la sicurezza di settore.

3. Sicurezza delle Informazioni generali

3.1 Previa ragionevole richiesta, la terza parte metterà a disposizione di BT copie delle certificazioni di sicurezza e delle dichiarazioni di conformità relative al Servizio per fornire prova della conformità ai presenti Requisiti di sicurezza.

3.2 In caso di importanti modifiche alla tecnologia o agli standard di sicurezza di settore, o qualora venissero apportate modifiche sostanziali ai Servizi o alla modalità di fornitura degli stessi, BT potrebbe predisporre una Modifica al Contratto durante il suo periodo di validità, nel caso in cui fosse necessario modificare i Requisiti di sicurezza applicabili. La terza parte dovrà rispettare la Modifica al Contratto concordata in tempi ragionevoli, considerando la natura della modifica e il rischio per BT.

3.3 La terza parte deve, almeno una volta all'anno o in caso di modifiche sostanziali ai Servizi o alle relative modalità di fornitura, riesaminare questi Requisiti di sicurezza e gli standard associati per garantire che essi siano ancora conformi a tutti i controlli di sicurezza applicabili.

3.4 Se una terza parte subappalta degli obblighi di cui al Contratto, tale terza parte dovrà assicurarsi che tutti i Contratti con i relativi Subappaltatori e i rispettivi Subappaltatori includano condizioni scritte che obblighino i Subappaltatori a rispettare le sezioni applicabili di questi Requisiti di sicurezza o di requisiti di sicurezza equivalenti di terzi.

3.5 Le Informazioni BT possono essere conservate per il tempo necessario a eseguire il Contratto, dopo il quale non dovrebbero essere conservate per più di un massimo di due anni, a meno che non sia stato concordato un periodo di conservazione diverso tra BT e la terza parte, o non sia richiesto da eventuali leggi applicabili.

3.6 Se i Servizi vengono resi a supporto diretto di un Contratto con il governo britannico, la terza parte deve operare nel pieno rispetto della versione corrente del Cyber Essentials Plus.

3.7 La terza parte deve assicurarsi che le Informazioni BT vengano gestite nel rispetto dei controlli indicati nei seguenti standard:

- Standard relativo alla Classificazione delle Informazioni e Trattamento dei Dati per le Terze Parti V4.0
- Standard relativo ai controlli per le Terze Parti V1.1 – Sezioni

  Sezione 1 Ruoli e Responsabilità.

  Sezione 2 Governance.

  Sezione 3 Gestione degli Incidenti.

  Sezione 4 Gestione delle Modifiche.

  Sezione 5 Gestione delle Minacce e dei Rischi informatici

  Sezione 6 Gestione delle Identità e Controllo degli Accessi.

  Sezione 10 Classificazione e Protezione dei Dati.

  Sezione 12 Prevenzione della Fuga di Dati.

  Sezione 13 PCI-DSS (se rientra nell'ambito del Servizio).

  Sezione 19 Gestione delle Vulnerabilità.

  Sezione 22 Monitoraggio e Analisi in continuo.

4. Sicurezza del Personale delle Terze Parti

4.1 La terza parte dovrà assicurarsi che tutto il relativo Personale abbia sottoscritto gli accordi di riservatezza prima di iniziare a lavorare presso gli edifici di BT o sui Sistemi BT o prima di accedere alle Informazioni BT. Tali accordi di riservatezza devono essere conservati dalla terza parte e resi disponibili per l'esame da parte di BT durante gli audit.

4.2 La terza parte dovrà occuparsi delle violazioni commesse dalla terza parte stessa e degli standard e controlli di sicurezza applicabili di BT, tramite processi formali comprensivi di misure disciplinari che potrebbero includere l'esclusione del soggetto dalle seguenti attività:

4.2.1 Accesso ai Sistemi BT o alle Informazioni BT; o

4.2.2 Esecuzione di lavori connessi alla prestazione del Servizio.

In più, la terza parte dovrebbe assicurarsi di aver implementato delle procedure idonee a garantire che qualsivoglia membro del suo Personale escluso non possa effettivamente accedere ai Sistemi BT, alle Informazioni BT o non possa svolgere lavori connessi alla prestazione del Servizio.

4.3 Nei limiti consentiti dalla legge, la terza parte dovrà prevedere un ambiente riservato che il relativo Personale potrà utilizzare per segnalare in modo anonimo eventuali casi in cui gli sia stato richiesto di agire in modo non conforme ai presenti Requisiti di sicurezza. I relativi report dovranno essere comunicati a BT.

- Quando il Personale della Terza parte non sarà più assegnato a un Servizio, a discrezione di BT, qualsivoglia risorsa fisica o Informazione BT in possesso del Personale della Terza parte dovrebbe essere: restituita alla squadra operativa di BT pertinente; o

- distrutta secondo quanto stabilito dallo Standard relativo alla Classificazione dell'Informazione e Trattamento dei Dati per le Terze Parti V4.0

4.4 La terza parte deve garantire l'esistenza di procedure appropriate affinché il proprio Personale conosca e implementi i controlli indicati nei seguenti standard:

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

  Sezione 15 Social Media

  Sezione 23 Sensibilizzazione e Formazione.

5. Audit e Revisione della sicurezza

5.1 Fatto salvo qualsiasi altro diritto di verifica che BT potrebbe detenere, al fine di valutare la conformità della terza parte ai presenti Requisiti di sicurezza e agli standard associati, la terza parte fornirà a BT, o ai suoi rappresentanti, l'Accesso e l'assistenza necessari e idonei per consentire l'esecuzione di revisioni di sicurezza su base documentale o di audit in loco. Prima di poter svolgere un audit di routine in loco, la terza parte dovrà essere avvertita con un preavviso minimo di 30 giorni lavorativi.

L'obiettivo dell'audit sarà quello di analizzare tutti gli aspetti che riguardano le politiche, i processi e il o i sistemi della terza parte (fermo restando che la terza parte dovrà proteggere la riservatezza di qualsivoglia informazione non collegata alla prestazione del Servizio a BT) che sono in qualche modo attinenti al Servizio prestato.

5.2 La terza parte lavorerà con BT per mettere in pratica le raccomandazioni concordate e implementare eventuali azioni correttive ritenute necessarie a seguito di una revisione di sicurezza su base documentale o di un audit in loco entro 30 giorni dalla ricezione della comunicazione da parte di BT o un periodo stabilito dalle parti, a spese della terza parte.

5.3 Qualora BT dovesse svolgere un audit indipendente della terza parte e la terza parte dovesse rivelarsi non conforme ai principi e alle prassi di cui alla norma ISO/IEC 27001:2013, la terza parte dovrà, a sue spese, prendere tutte le misure necessarie per poter raggiungere lo stato di conformità richiesto e dovrà rimborsare interamente eventuali costi sostenuti da BT nel corso di detto audit.

6. Diritto di Ispezione

6.1 La terza parte deve concedere a BT il diritto di ispezione conformemente a quanto indicato in:

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

  Sezione 24 Diritto di Ispezione.

7. Certificazioni di Sicurezza

7.1 I Sistemi, il Servizio e i Servizi associati, i processi e i luoghi fisici della Terza parte devono essere conformi alla norma ISO/IEC 27001:2013 (o a eventuali certificazioni che dimostrino controlli equivalenti, supportate dalla relazione di una società di revisione indipendente) e a qualsivoglia versione futura o modificata dello standard pubblicato. Detta conformità deve essere garantita mediante:

7.1.1 certificazione dell'ISMS della Terza Parte da parte di un UKAS o di un ente di certificazione internazionale equivalente approvato, il cui ambito di applicazione e la cui dichiarazione di applicabilità dovranno essere convalidate da BT; o

7.1.2 un processo di verifica e un audit bilaterale specificati da BT.

7.2 La terza parte deve presentare un certificato valido all'inizio del Rapporto contrattuale e ogniqualvolta verrà ricertificata.

7.3 Qualora l'oggetto del certificato o della dichiarazione di applicabilità dovesse cambiare, la terza parte dovrà presentare tali modifiche per una nuova convalida implementando la procedura di controllo delle modifiche (o, in assenza di una procedura di controllo delle modifiche, attraverso il processo delle variazioni). La terza parte deve informare BT, entro 2 giorni lavorativi, di eventuali major non-conformance che saranno state individuate dall'ente certificatore o dalla terza parte.

8. Sicurezza fisica – Sedi di BT

8.1 Se la terza parte lavora nelle sedi di BT, si applicano i controlli indicati nel seguente standard:

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 25. Sicurezza fisica – Sede di BT

9. Sicurezza fisica – Sedi della Terza Parte

9.1 Se vengono usate le sedi della terza parte per la prestazione del Servizio, si applicano i controlli indicati nel seguente standard.

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 9. Sicurezza fisica presso la Sede di una Terza parte **esclusi** i controlli 9.10 e 9.11 per la Fornitura di un ambiente per la custodia delle apparecchiature BT.

10. Fornitura di un ambiente per la custodia delle apparecchiature BT

10.1 Se viene usata la sede della terza parte per fornire un ambiente di hosting per le apparecchiature, si applicano i controlli indicati nel seguente standard.

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 9. Sicurezza fisica presso la Sede di una Terza parte - controlli 9.10 e 9.11 per la Fornitura di un ambiente di hosting per apparecchiature BT.

11. Sviluppo software sicuro

11.1 Se la terza parte fornisce software o sistemi, si applicano i controlli indicati nel seguente standard.

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 17. (17.1 e 17.2) Sviluppo software sicuro

12. ESCROW

12.1 Se si richiede un ESCROW a tutela di tutte le parti, si applicano i controlli indicati nel seguente standard.

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 17. (solo 17.3) Sviluppo software sicuro

13. Accesso ai Sistemi BT

13.1 Se i Sistemi della Terza parte o i membri del suo Personale richiedono l'Accesso/la connessione a Sistemi di BT, si applicano i controlli indicati nel seguente standard.

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 8. Accesso ai Sistemi BT

14. Sistemi di Terze Parti in cui sono contenute le Informazioni BT

14.1 Se vengono utilizzati i Sistemi di una Terza parte per contenere le Informazioni BT, si applicano i controlli indicati nel seguente standard:

Standard relativo alla Classificazione dell'Informazione e Trattamento dei Dati per le Terze Parti V4.0

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 7 Gestione degli Asset informativi.

Sezione 11. Crittografia.

Sezione 16 Configurazione di Sistema.

Sezione 18 Protezione anti-malware**.**

Sezione 21. Mitigazione dei casi di "Denial of Service".

15. Terze parti che custodiscono (hosting) le Informazioni BT

15.1 Se una terza parte custodisce le informazioni di BT, la relativa sede deve possedere un certificato ISO/IEC 27001 valido per la gestione della sicurezza (o una o più certificazioni che dimostrino controlli equivalenti, supportate dalla relazione di una società di revisione indipendente).

15.2 Si applicheranno i controlli indicati nei seguenti standard:

- Standard relativo alla Classificazione dell'Informazione e Trattamento dei Dati per le Terze Parti V4.0
- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 7 Gestione degli Asset informativi.

Sezione 11. Crittografia.

Sezione 16 Configurazione di Sistema.

Sezione 18 Protezione anti-malware**.**

Sezione 21. Mitigazione dei casi di "Denial of Service".

16. Sicurezza di rete – Rete propria di BT

16.1 Se la terza parte dovrà installare delle attrezzature, configurare, mantenere, riparare o monitorare la rete di BT, si applicheranno i controlli indicati nei seguenti standard:

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

Sezione 26. Sicurezza di rete – Rete propria di BT.

17. Sicurezza di rete della terza parte

17.1 Se viene usata la rete della terza parte per accedere alle Informazioni BT o per prestare il Servizio, si applicano i controlli indicati nel seguente standard:

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

  Sezione 16 Configurazione di Sistema.

  Sezione 20 Integrità di Rete

18. Sicurezza nel Cloud

18.1 Se la terza parte fornisce a BT Servizi cloud, si applicano i controlli indicati nel seguente standard:

- Standard relativi ai sistemi di controlli di terzi V1.1 – Sezioni

  Sezione 14. Cloud / Online Computing.

19. Contact Centre

19.1 Se la terza parte fornisce a BT Servizi di Contact Centre, si applicano i controlli indicati nel seguente standard:

- Standard di terzi relativo al Contact Centre V1.0

20. Informazioni classificate come OFFICIAL o di livello superiore dal Governo del Regno Unito

20.1 I Requisiti di sicurezza aggiuntivi di cui all'Allegato 1 dei presenti Requisiti di sicurezza si applicheranno a ogni terza parte che archivierà, elaborerà o trasmetterà le informazioni classificate come 'Official sensitive' in linea con lo Schema di classificazione di sicurezza del Governo del Regno Unito e successive modifiche.

20.2 La Terza parte garantirà che i sistemi e le infrastrutture utilizzati per la prestazione dei Servizi siano contenuti in una rete logica dedicata. Tale rete deve essere costituita unicamente dai sistemi dedicati alla fornitura di una struttura di trattamento dati sicura.

21. Termini definiti e Interpretazione

21.1 Se non diversamente indicato di seguito, i termini e le espressioni utilizzati nei presenti Requisiti di sicurezza avranno lo stesso significato di cui al Contratto:

Per "**Accesso**" si intende l'elaborazione, la gestione o l'archiviazione delle Informazioni BT secondo uno o più dei seguenti metodi:

a. Mediante interconnessione con i Sistemi BT;
b. Fornite in formato cartaceo o non elettronico;
c. Informazioni BT sui Sistemi del Fornitore; o
d. Mediante media mobili

e/o l'Accesso alle sedi di BT per la consegna delle Forniture, ad esclusione della consegna di hardware e la partecipazione a riunioni.

Per "**Informazioni BT**" si intendono tutte le Informazioni che riguardano BT o un Cliente BT fornite al Fornitore e tutte le Informazioni che vengono trattate o gestite dal Fornitore per conto di BT o di un Cliente BT nell'ambito del Contratto.

Per "**Sistemi BT**" si intendono i Servizi e le varie componenti dei Servizi, i prodotti, le reti, i server, i processi, i sistemi basati su carta o quelli IT (in tutto o in parte) di proprietà di e/o utilizzati da BT o qualsiasi altro sistema che possa trovarsi presso la sede di BT.

Per "**Contratto**" si intende il Contratto stipulato tra le Parti per la fornitura di beni, software o Servizi che fa riferimento ai presenti Requisiti di sicurezza.

Per "**Cyber Essentials Plus**" si intende lo schema appoggiato dal governo britannico per aiutare le imprese a proteggersi dagli attacchi informatici più comuni.

Per "**Escrow**" si intende l'accordo di deposito del codice sorgente stipulato conformemente al Contratto per usare, copiare, mantenere e modificare tale codice sorgente per lo svolgimento delle attività commerciali con BT (incluso il diritto di compilare tale codice sorgente).

Per "**best practice di sicurezza di settore**" si intende, relativamente a qualsivoglia iniziativa e in tutte le circostanze, l'implementazione di pratiche, politiche, standard e l'uso di attrezzature di sicurezza che ci si potrebbe ragionevolmente aspettare da una persona qualificata e competente coinvolta nello stesso tipo di attività, in circostanze uguali o simili.

Per "**Sicurezza di rete**" si intende la sicurezza dei nodi e dei percorsi di comunicazione di interconnessione che connettono in modo logico le tecnologie dell'utente finale tra di loro e ai sistemi di gestione associati.

Per "**Official Sensitive Declaration**" **(Dichiarazione dati Official Sensitive)** si intende la dichiarazione scritta che il Fornitore deve presentare relativamente ai ruoli individuati dal Fornitore che avranno Accesso alle informazioni classificate come "Official Sensitive" o che hanno privilegi elevati relativamente alle infrastrutture in cui vengono archiviate, elaborate o trasmesse le informazioni classificate come "Official Sensitive" (cfr. Allegato 1 contenente un modello).

Per "**Requisiti di sicurezza**" si intende il presente documento e successive modifiche.

Per "**Subappaltatore**" si intende un Subappaltatore del Fornitore che si occupa della o è coinvolto nella consegna delle Forniture o che impiega o ingaggia soggetti coinvolti della consegna delle Forniture.

Per "**Personale della Terza parte**" si intende qualsiasi soggetto coinvolto dal Fornitore o dai suoi Subappaltatori nell'adempimento degli obblighi del Fornitore ai sensi del Contratto.

Per "**Servizio**" si intendono tutti i "**Beni**", i "**Software**" o i "**Servizi**" definiti nel Contratto.

Per "**Sistemi di Terzi**" si intende qualsiasi sistema di rete, applicazione o computer di proprietà del Fornitore usato per accedere alle, archiviare o elaborare le Informazioni BT o coinvolti nella consegna delle Forniture.

Interpretazione

21.2 Tutti i termini che seguono espressioni come "comprensivo di", "che include", "in particolare", "per esempio" o espressioni simili saranno interpretati come esemplificativi ma non limitativi del significato delle parole, delle descrizioni, delle definizioni, delle frasi o dei termini che precedono tali espressioni.

21.3 Nei casi in cui il diritto o l'obbligo di un Terzo viene espresso come diritto o obbligo che "**potrebbe**" esercitare o adempiere, la scelta di esercitare o di adempiere a tale obbligo o diritto sarà a discrezione esclusiva della Parte.

21.4 Nei casi in cui viene fatto riferimento a un collegamento ipertestuale ("**URL**"), tale riferimento sarà da ricollegare a detta risorsa online accessibile tramite URL o qualsivoglia altro URL sostitutivo, come di volta in volta comunicato alla parte applicabile.

ALLEGATO 1 – Requisiti di sicurezza aggiuntivi

Se la Terza parte ha necessità di Accedere a, conservare, elaborare o trasmettere informazioni 'Official Sensitive per il Governo del Regno Unito', la Terza parte dovrà operare nel rispetto dei presenti Requisiti di sicurezza e, in più, dei requisiti indicati nel presente Allegato 1; dovrà altresì fornire a BT una "Dichiarazione dati Official Sensitive" (Official Sensitive Declaration) debitamente compilata prima della sottoscrizione del Contratto. In tutti i casi, il controllo di livello superiore avrà la precedenza sui requisiti documentati altrove nei presenti Requisiti di sicurezza per i Servizi e i sistemi indicati nella "Dichiarazione dati Official Sensitive".

1. DIPENDENTI

1.1. Tutti i ruoli identificati dalla Terza parte come autorizzati ad accedere alle informazioni classificate come "Official Sensitive" o aventi privilegi elevati relativamente alle infrastrutture in cui vengono archiviate, elaborate o trasmesse le informazioni classificate come "Official Sensitive" saranno indicati nella "Dichiarazione dati Official Sensitive".

1.2. Il Personale della Terza parte che occupa le posizioni indicate nella "Dichiarazione dati Official Sensitive ":

1.2.1. deve essere almeno sottoposto a dei controlli preliminari all'assunzione conformemente al Baseline Personnel Security Standard (BPSS);

1.2.2. deve sottoscrivere una dichiarazione ai sensi dell'Official Secrets Act; e

1.2.3. se non è riuscito a ottenere i nulla osta di sicurezza necessari, deve essere bloccato dall'accesso alle informazioni o ai sistemi.

2. FORMAZIONE SULLA SICUREZZA

2.1. La Terza parte prescriverà la partecipazione a corsi di formazione sulla sicurezza al momento dell'assunzione e almeno a cadenza annuale. Tali corsi verteranno sui requisiti di gestione delle informazioni, nello specifico delle informazioni classificate come "Official" o "Official Sensitive" in linea con i requisiti di cui allo Schema di classificazione di sicurezza del Governo del Regno Unito, così come specificato nelle Linee guida per la protezione delle informazioni HMG da parte di BT per terzi

2.2. La Terza parte aggiornerà le *job description* relative ai suoli indicati della "Dichiarazione dati Official Sensitive" per prescrivere la partecipazione ai corsi di formazione indicati al precedente paragrafo 2.1. La Terza parte conserverà la documentazione relativa alla formazione che, su richiesta, dovrà essere messa a disposizione di BT.

3. CONTROLLO DEGLI ACCESSI

3.1. Se i dipendenti lasciano l'azienda o cambiano ruolo, i relativi diritti di Acceso dovranno essere revocati dai Sistemi della Terza parte rilevanti entro un (1) giorno lavorativo.

3.2. Se i dipendenti della Terza parte, compresi gli Appaltatori, i dipendenti con contratto a tempo determinato e quelli assunti tramite agenzia, hanno privilegi elevati relativamente alle infrastrutture di BT, la Terza parte deve comunicare a BT per iscritto entro 1 giorno lavorativo da quando il dipendente non avrà più necessità di Accedere ai Sistemi BT (ad esempio, se i dipendenti lasciano l'azienda o cambiano ruolo).

3.3. Se i dipendenti della Terza parte, compresi gli Appaltatori, i dipendenti con contratto a tempo determinato e quelli assunti tramite agenzia, hanno ricevuto una tessera per l'Accesso permanente alle sedi BT, la Terza parte deve comunicare a BT per iscritto entro 1 giorno lavorativo da quando il dipendente non avrà più necessità di Accedere alla sede BT (ad esempio, se i dipendenti lasciano l'azienda o cambiano ruolo).

4. VALUTAZIONE E CLASSIFICAZIONE DELLE RISORSE

4.1. La Terza parte implementerà delle procedure di gestione delle informazioni aggiuntive per soddisfare i requisiti di gestione delle informazioni "Official" o "Official Sensitive" in linea con i requisiti di cui allo Schema di classificazione di sicurezza del Governo del Regno Unito e successivi aggiornamenti

5. RISPOSTA IN CASO DI INCIDENTE E RENDICONTAZIONE – SERVICE LEVEL AGREEMENT

5.1. La Terza parte verrà informata in merito a dei *Service level agreement* specifici a supporto delle procedure di risposta in caso di incidente. Questi potrebbero avere la precedenza su eventuali accordi precedenti descritti nei presenti Requisiti di sicurezza.

6. AUDIT, TEST E MONITORAGGIO

6.1. Se richiesto da BT, la Terza parte implementerà un servizio di monitoraggio della sicurezza attivo 24 ore su 24, 7 giorni su 7.

6.2. Le infrastrutture della Terza parte sottoposte all'attività di monitoraggio della sicurezza attivo 24 ore su 24, 7 giorni su 7 saranno documentate nella "Dichiarazione dati Official Sensitive".

7. CONTINUITÀ OPERATIVA E DISASTER RECOVERY

7.1. La Terza parte produrrà un piano di continuità operativa e Disaster Recovery conformemente a quanto indicato nella norma BS ISO 22301 entro 30 giorni dalla sottoscrizione del Contratto.

8. LUOGO

8.1. Se non diversamente specificato da BT, il Servizio deve essere fisicamente ubicato entro i confini fisici del Regno Unito o, ove applicabile, dello SEE.

ALLEGATO 1, DOCUMENTO 1 – MODELLO DI "DICHIARAZIONE DATI OFFICIAL SENSITIVE"

1. Sistemi/Servizi in oggetto

Elencare i sistemi e i Servizi oggetto della fornitura a supporto del cliente HMG.

Sistema	Servizio

2. Ruoli della Terza parte che richiedono un livello di nulla osta di sicurezza.

Ruolo	Livello di nulla osta di sicurezza richiesto
* *ad esempio, DBA*	*SC*

3. Gestione delle Vulnerabilità

Sistema	Valutazione del tipo di vulnerabilità	Frequenza

4. Audit, test e monitoraggio

Sistemi da monitorare 24/7, come specificato da BT