

Indice

1. Introduzione	2
2. Requisiti di Accesso limitato	2
3. Sicurezza generale delle Informazioni.....	2
4. Sicurezza del Personale di Terzi	12
5. Audit e Revisione della sicurezza	14
6. Diritto di Ispezione	14
7. Certificazioni di Sicurezza	15
8. Sicurezza fisica – Sede di BT	15
9. Sicurezza fisica – Sedi di terzi	16
10. Fornitura di un ambiente di Hosting per Apparecchiature BT	17
11. Sviluppo software sicuro	17
12. Deposito Fiduciario.....	18
13. Accesso ai Sistemi BT.....	18
14. Sistemi di Terzi contenenti Informazioni BT	18
15. Terze parti che custodiscono Informazioni BT	21
16. Sicurezza di rete – Rete propria di BT	21
17. Sicurezza di rete della Terza parte	24
18. Sicurezza nel Cloud.....	25
19. Servizi di telefonia mobile	26
20. Informazioni classificate come UFFICIALI o di livello superiore del Governo del Regno Unito	26
21. Termini definiti e Interpretazione	26
22. ALLEGATO 1, DOCUMENTO 1 – MODELLO DI “DICHIARAZIONE SUI DATI UFFICIALI SENSIBILI” ..	33
23. ALLEGATO 2, Telecommunications (Security) Act 2021 – Conversione da Codice di condotta a Requisiti di sicurezza	34

1. Introduzione

- 1.1 I clienti di BT si aspettano da BT e dai propri fornitori la fornitura di servizi mediante sistemi di gestione per la sicurezza delle informazioni (ISMS) secondo gli standard del settore. Il vostro ISMS deve pertanto coprire l'infrastruttura, le reti, le apparecchiature e i sistemi informatici in modo tale da proteggere i servizi forniti e le informazioni sui clienti BT/BT relative ai servizi. Il presente documento definisce la policy sui Requisiti di sicurezza di BT e si applica a tutte le terze parti che operano per o per conto del Gruppo BT, compresi Openreach, EE e Plusnet, di seguito indicati come 'BT'. Sarà reso noto quali serie di controlli di sicurezza sono applicabili al servizio fornito a BT.
- 1.2 Questi Requisiti di sicurezza si aggiungono a qualsivoglia altro obbligo stipulato nel Contratto a cui la Terza parte deve adempiere, senza pregiudicarne la validità.

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 abbia accesso a Informazioni BT, essa dovrà:
- 2.2 Assicurarsi che le Informazioni BT non vengano divulgate o rese accessibili a membri del Personale della Terza parte, salvo che ciò sia 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 (i) distruzione accidentale o illecita, e (ii) perdita, alterazione, divulgazione non autorizzata delle, o Accesso alle, Informazioni BT conformemente alle best practice di settore in materia di sicurezza.

3. Sicurezza generale delle Informazioni

- 3.1 Previa ragionevole richiesta, la Terza parte renderà disponibili a 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 potrà predisporre una modifica al Contratto durante il relativo periodo di validità, se fosse necessario modificare le serie di controlli di sicurezza applicabili. La Terza parte dovrà conformarsi alla modifica al Contratto concordata in tempi ragionevoli, considerata la natura della modifica e il rischio per BT.
- 3.3 In caso di modifiche sostanziali apportate ai Servizi o alle modalità di fornitura degli stessi, la Terza parte dovrà rivedere i Requisiti di sicurezza contenuti in questa policy per accertarsi che essi siano ancora conformi a tutti i controlli di sicurezza applicabili.
- 3.4 Se la Terza parte subappalta obblighi previsti dal Contratto, tale Terza parte dovrà assicurarsi che tutti i Contratti con i Subappaltatori interessati e i Subappaltatori di questi ultimi includano condizioni scritte che obblighino i Subappaltatori a rispettare le

- sezioni applicabili dei presenti Requisiti di sicurezza o di requisiti di sicurezza equivalenti di Terze parti.
- 3.5 Qualora venga utilizzata una quarta parte per la prestazione del servizio, e detta parte abbia accesso o elabori Informazioni BT, la Terza parte dovrà concordare con lo Stakeholder BT quali informazioni potranno essere condivise. La Terza parte deve verificare l'esistenza di un rapporto contrattuale con la quarta parte e deve altresì assicurarsi che detta quarta parte operi in accordo con un quadro di riferimento per la sicurezza secondo gli standard di settore.
 - 3.6 Le Informazioni BT possono essere conservate per il tempo necessario a dare esecuzione al Contratto, dopodiché potranno essere conservate per un periodo massimo di due anni, a meno che non sia stato concordato un periodo di conservazione diverso tra BT e la Terza parte, e fatto salvo quanto richiesto da eventuali leggi applicabili.
 - 3.7 Se i Servizi vengono forniti a supporto diretto di un Contratto con il governo britannico, la Terza parte dovrà operare nel pieno rispetto della versione corrente del Cyber Essentials Plus – <https://www.cyberessentials.ncsc.gov.uk/>
 - 3.8 Nel caso in cui le informazioni BT vengano trattate o conservate all'estero, la Terza parte deve informare BT delle relative localizzazioni geografiche, e BT si riserva il diritto di rifiutare le localizzazioni ritenute ad alto rischio.

Gestione delle Informazioni BT

Salvo diversa indicazione da parte dello stakeholder BT, tutte le informazioni di BT sono classificate come "Riservate" (Confidential). Se dati personali o dati personali sensibili rientrano nell'ambito di applicazione, è necessario consultarsi con il proprio team esperto di protezione dei dati e privacy per verificare la necessità di controlli aggiuntivi.

I seguenti controlli di sicurezza sono " requisiti per la gestione delle informazioni discusse a voce" il cui ambito è limitato alle comunicazioni verbali.

- 3.9 Se è necessario discutere, mostrare o scambiare informazioni BT utilizzando uno strumento di collaborazione, ad esempio Teams
 - Assicurarsi che siano presenti solo le persone che hanno necessità di acquisire le informazioni.
 - Se è coinvolta una terza parte o un contractor esterno, è necessario un contratto sottoscritto con voi o un accordo di non divulgazione (NDA) predisposto prima dell'inizio della condivisione.
 - Occorre verificare l'identità di chi partecipa alla conferenza prima dell'inizio.
- 3.10 Se Informazioni BT devono essere discusse con un interlocutore di persona, mediante un telefono cellulare o una linea telefonica standard.
 - Tali conversazioni non devono coinvolgere né essere ascoltate da chiunque non abbia necessità di esserne a conoscenza.
 - Se la conversazione deve coinvolgere una terza parte o un contractor esterno, è necessario un contratto sottoscritto con voi o un accordo di non divulgazione (NDA) predisposto prima dell'inizio della conversazione.
 - Informazioni riservate o strettamente confidenziali non devono essere trasmesse tramite messaggi audio.

I seguenti controlli di sicurezza sono "requisiti per la gestione scritta" e il loro ambito di applicazione prevede materiale conservato in formato cartaceo. Ciò comprende, a titolo esemplificativo ma non esaustivo, comunicazioni scritte a mano, verbali, note e promemoria. Include anche materiale elettronico una volta stampato, come documenti di lavoro e relazioni in formato cartaceo.

3.11 Se si conservano copie cartacee delle informazioni BT presso strutture di Terze parti, quando non in uso queste devono essere protette, riponendole in ambienti chiusi a chiave, con accesso limitato esclusivamente a coloro che hanno necessità di visionare il materiale. La documentazione non deve essere lasciata incustodita.

3.12 Se è necessario stampare, fotocopiare o duplicare Informazioni BT, sono applicabili i seguenti controlli di sicurezza:

- Utilizzare esclusivamente i servizi di stampa o copia presso la propria sede.
- Le fotocopie o le stampe non devono essere lasciate incustodite nel luogo di stampa e devono essere ritirate al momento stesso della creazione.
- Nel caso in cui la stampante o la fotocopiatrice disponga di capacità di memoria che consenta di richiamare e ristampare il materiale copiato, occorrerà effettuare un riavvio per cancellare la memoria non appena possibile.

3.13 Se è necessario rimuovere copie delle Informazioni BT da strutture di Terze parti:

- Salvo quanto già concordato nell'ambito della prestazione, è necessario ottenere il consenso comprovato dello stakeholder di BT.
- Se approvate, le informazioni non devono essere identificabili in transito e devono essere contenute in una cartella, borsa o custodia anonima o neutra.
- Il materiale non deve essere lasciato incustodito e deve rimanere sotto il diretto controllo della persona incaricata del trasporto, soprattutto su mezzi pubblici.

3.14 Quando non sono più necessarie, le copie cartacee delle Informazioni BT devono essere smaltite come segue:

- Le copie cartacee non devono essere gettate insieme ai rifiuti generici.
- Se si utilizza un trituratore per documenti, lo standard minimo richiesto è P4 DIN66399.
- Se non sono disponibili trituratori per documenti approvati, le informazioni devono essere smaltite in appositi contenitori per rifiuti idonei a documenti riservati.

Alle "Informazioni strettamente confidenziali" si applica inoltre quanto segue.

- Le informazioni devono essere smaltite esclusivamente in contenitori per rifiuti idonei a documenti riservati dopo triturazione.
- Per le informazioni da distruggere in loco da parte del fornitore è richiesto al fornitore un attestato di distruzione.

I seguenti controlli di sicurezza si riferiscono a Informazioni BT in formato elettronico.

3.15 Quando si memorizzano informazioni BT su PC o laptop di Terze parti, si applicano i seguenti controlli:

- La procedura è consentita solo su dispositivi con crittografia dell'hard disk, ad esempio Bitlocker.

- Tutti i documenti devono essere crittografati singolarmente.
 - Al documento deve essere applicato il sistema di sicurezza Information Rights Management (IRM).
 - Se fornita, le informazioni devono mantenere l'etichetta di classificazione BT.
- 3.16 Quando si salva un documento BT in una posizione di condivisione file interna per archiviazione generale, collaborazione o condivisione di file, si applicano i seguenti controlli di sicurezza:
- La posizione in cui viene salvato il materiale deve prevedere autorizzazioni di accesso per consentire solo a chi ha necessità di visionare o utilizzare il documento.
 - Se fornita, le informazioni devono mantenere l'etichetta di classificazione BT.
 - Tutti i documenti devono essere crittografati singolarmente.
 - Al documento deve essere applicato il sistema di sicurezza Information Rights Management (IRM).
 - Se rientrante nell'ambito del servizio fornito, il materiale relativo a standard PCI e carte di pagamento non deve essere mai salvato in siti di archiviazione di file.
 - Se sono richiesti account di tipo Guest per consentire l'accesso di una terza parte o un contractor esterno, è necessario un contratto sottoscritto con voi o un accordo di non divulgazione (NDA) predisposto prima di concedere l'accesso.
- 3.17 Se è necessario salvare le informazioni BT su supporti rimovibili di Terze parti, ad esempio una memory stick USB, si applicano i seguenti controlli di sicurezza:
- Il dispositivo deve essere crittografato secondo lo stesso livello del disco rigido.
 - In caso di smarrimento o furto, è necessario aprire una pratica di incidente di sicurezza.
 - È necessario disporre di evidenze dell'approvazione preventiva da parte dello Stakeholder BT per il trasferimento di materiale "strettamente confidenziale" su supporti rimovibili.
 - Se compresi nell'ambito del servizio, dati personali o materiale PCI non devono essere conservati su supporti rimovibili.
 - I dispositivi destinati al supporto e alla manutenzione non devono essere utilizzati per altri scopi.
- 3.18 Le Informazioni BT non devono essere archiviate su PC personali, laptop, supporti rimovibili o dispositivi mobili
- 3.19 Le Informazioni BT non devono essere inviate o inoltrate automaticamente dall'indirizzo e-mail aziendale a un proprio account e-mail personale o a un account e-mail esterno, salvo che non si tratti di una terza parte o di un contractor esterno che abbia sottoscritto con voi un contratto o un accordo di non divulgazione (NDA) e che tali informazioni siano utilizzate per fornire il servizio.
- 3.20 Per ridurre al minimo il rischio di attacco informatico e le opportunità di manipolazione dei comportamenti umani da parte di aggressori attraverso l'interazione con browser di internet e sistemi di posta elettronica, implementare processi per garantire che siano consentiti esclusivamente i browser e i client di posta elettronica integralmente supportati e disinstallare o disabilitare qualsiasi browser non autorizzato o plug-in di client di posta elettronica o applicazioni add-on.

- 3.21 La Terza parte deve disporre di misure di backup per ripristinare le Informazioni BT entro 3 giorni lavorativi in caso di danneggiamento, perdita o degrado.
- 3.22 In caso di eliminazione di dati e Informazioni BT, è necessario mantenere registri completi relativi alla conservazione e all'eliminazione dei dati, corredati di audit trail, evidenze e sistemi di monitoraggio. Tali registri devono comprendere:
- Prova dell'avvenuta distruzione e/o eliminazione (inclusa la data di presa in carico e il metodo utilizzato).
 - Audit log dei sistemi per l'eliminazione.
 - Certificati di avvenuta eliminazione dei dati.
 - Identità di chi si è occupato dell'eliminazione (compresi eventuali collaboratori/terzi o contractor addetti all'eliminazione)
 - La generazione di un report di distruzione e verifica a conferma dell'esito positivo o negativo della procedura di eliminazione / distruzione. (dal processo di sovrascrittura deve essere generato un report in cui sono indicati i settori che non è stato possibile cancellare).
- 3.23 Quando si smaltiscono apparecchiature in cui erano presenti dati/informazioni BT, è necessario fornire una pista di controllo (Audit Trail) per i seguenti tipi di apparecchiature:
- Supporti amovibili.
 - Unità disco.
 - Nastri per backup.
 - Componenti di computer.
 - È necessario conservare registri completi atti a fornire un *audit trail* che includa come minimo:
 - Il nome dell'applicazione o del servizio che ha utilizzato quell'apparecchiatura.
 - Il tipo di apparecchiatura, come un computer desktop, laptop, un server, un nastro, un router, ecc.
 - Il numero di hard drive contenuti nell'apparecchiatura (se applicabile).
 - L'apparecchiatura identificata dal numero di serie.
 - I componenti dell'apparecchiatura identificati dal numero di serie.
 - Un tracciamento delle risorse completo relativo a tutte le apparecchiature e ai componenti per l'intero ciclo di vita dell'apparecchiatura smaltita.
 - Prova dell'avvenuta distruzione e/o eliminazione (inclusa la data di presa in carico e il metodo utilizzato).
 - Dati relativi al soggetto che si è occupato dello smaltimento (compresi eventuali collaboratori addetti allo smaltimento/terzi/contractor addetti allo smaltimento rifiuti).
 - Report di avvenuta distruzione e verifica generati per confermare l'esito positivo o negativo della procedura di distruzione o riciclo/recupero dei rifiuti. Ad esempio, dal processo di sovrascrittura deve essere generato un report in cui vengono specificati i settori che non è stato possibile cancellare. Questi report devono includere la capacità, la marca, il modello e il numero di serie dei supporti.

Ruoli e responsabilità

3.24 Tutte le Terze parti devono conoscere e aver compreso i requisiti di questi controlli di sicurezza e a ciascuna spetta la responsabilità di garantire che tutti i soggetti coinvolti nella prestazione di un servizio a BT conoscano i requisiti applicabili del presente standard e li rispettino.

Governance

3.25 La Terza parte deve disporre di un quadro di sicurezza standard di settore, coerente e consolidato, in tema di governance della sicurezza informatica e delle informazioni, comprensivo di quanto indicato di seguito:

- Politiche e procedure appropriate sulla sicurezza informatica e delle informazioni, approvate e comunicate.
- Una strategia in tema di sicurezza delle informazioni.
- Requisiti giuridici e normativi pertinenti, in relazione alla sicurezza informatica e delle Informazioni (privacy inclusa), ben compresi e gestiti.
- Procedure per la gestione dei rischi e di governance specifiche per i rischi relativi alla sicurezza informatica.

3.26 La Terza parte deve assicurarsi che vengano definiti ruoli e responsabilità idonei in relazione alla Sicurezza informatica e delle Informazioni e che questi vengano implementati. Ciò comprende quanto segue:

- Un Responsabile della sicurezza delle informazioni a tempo pieno (o figura equivalente) che abbia un'anzianità sufficiente e sia responsabile del programma di sicurezza delle informazioni.
- Un gruppo di lavoro di alto livello, un comitato o un organo equivalente che coordini le attività di sicurezza delle informazioni presso la Terza parte, che sia presieduto da un membro sufficientemente anziano dello staff e che si riunisca regolarmente.
- Una figura specializzata in sicurezza delle informazioni con ruoli e responsabilità adeguati e ben definiti.

3.27 La Terza parte deve garantire la responsabilità individuale in merito alle informazioni e ai sistemi assicurandosi che la proprietà di ambienti, informazioni e sistemi aziendali critici sia affidata a soggetti idonei e competenti.

3.28 La Terza parte deve assicurarsi che BT sarà informata (per iscritto), nel più breve tempo possibile e nel rispetto della legge, nel caso in cui tale Terza parte dovesse essere oggetto di un'operazione di fusione, acquisizione o di qualsivoglia altro cambio di proprietà.

Gestione degli Incidenti

3.29 La Terza parte deve disporre di un quadro coerente e consolidato per la gestione degli incidenti, a garanzia che tali eventi vengano gestiti, contenuti e mitigati in maniera adeguata, e che copra i seguenti aspetti:

- Garantire che ogni membro del personale conosca il proprio ruolo e la procedura da implementare in caso sia richiesto un intervento.
- Garantire che gli incidenti vengano comunicati coerentemente con criteri prestabiliti.

- Garantire che venga compreso l'impatto dell'incidente.
 - Garantire che, in caso di necessità, verranno svolte adeguate indagini, internamente o ad opera di uno specialista.
 - Garantire che tutti gli apprendimenti derivanti dagli incidenti verificatisi vengano incorporate in una *best practice*.
 - Garantire che le informazioni correlate a un incidente che coinvolge BT vengano trattate come "Riservate".
- 3.30 La Terza parte adotterà ogni ragionevole misura per garantire che uno o più soggetti idonei vengano nominati responsabili e fungano da Punto di contatto per il rischio per la sicurezza, la gestione degli incidenti e la gestione della conformità. La Terza parte dovrà comunicare allo Stakeholder BT i dettagli di contatto del/dei soggetto/i e qualsiasi eventuale relativa modifica.
- 3.31 La Terza parte informerà BT via e-mail all'indirizzo security@bt.com o telefonicamente al numero +44 0800 321 999, entro tempi ragionevoli dal momento in cui sarà venuta a conoscenza di un eventuale incidente che ha un impatto sul servizio da rendere a BT o sulle Informazioni BT, e in ogni caso entro e non oltre ventiquattro (24) ore dal momento in cui l'Incidente è reso noto alla Terza parte.
- 3.32 Senza ritardi immotivati, la Terza parte adotterà misure correttive appropriate e tempestive per mitigare eventuali rischi e gli effetti collegati all'incidente allo scopo di ridurre la gravità e la durata di tale evento.
- 3.33 La Terza parte redigerà, entro 30 giorni dal verificarsi di un incidente, un rapporto per lo Stakeholder BT in relazione a qualsivoglia incidente che possa avere un impatto sul servizio da rendere a BT o sulle Informazioni BT. Detto rapporto dovrebbe comprendere perlomeno i seguenti dati:
data e ora, luogo, tipo di incidente, impatto, stato ed esito (comprese le raccomandazioni per la risoluzione o le azioni intraprese).
- 3.34 La Terza parte deve eseguire un'analisi della causa di base di tutti gli incidenti di sicurezza. I risultati di questa analisi devono essere inoltrati al livello di gestione appropriato nell'ambito della propria organizzazione.

Gestione delle Modifiche

- 3.35 La Terza parte deve assicurarsi che tutte le modifiche IT vengano approvate, registrate e testate, incluso il ritiro di modifiche non andate a buon fine, prima dell'implementazione, al fine di impedire l'interruzione del servizio o violazioni della sicurezza. Deve altresì assicurarsi che sia prevista una procedura per implementare aggiornamenti di emergenza in modo controllato.
- 3.36 La Terza parte deve garantire che le modifiche vengano riportate negli ambienti sia di Produzione che Disaster Recovery
- 3.37 La Terza parte deve garantire che le risorse organizzative verranno sottoposte a manutenzione e riparazione mediante l'uso di strumenti registrati, approvati e controllati.
- 3.38 La Terza parte deve assicurarsi che la manutenzione in remoto delle risorse aziendali venga approvata, registrata ed eseguita in modo tale da prevenire accessi non autorizzati.

Gestione delle Minacce e dei Rischi informatici

3.39 La Terza parte deve assicurarsi che esista un quadro di valutazione delle minacce e dei rischi alla Sicurezza informatica sempre aggiornato, volto a garantire che il profilo di rischio per la Sicurezza informatica delle operazioni, risorse, sedi e risorse umane dell'organizzazione risulti ben compreso e gestito secondo le seguenti modalità:

- Valutazione delle vulnerabilità delle risorse.
- Individuazione delle minacce sia interne che esterne.
- Valutazione della sensibilità delle informazioni e dei dati in oggetto.
- Valutazione del potenziale impatto sulle attività aziendali.
- Per determinare il rischio si tiene conto delle minacce, vulnerabilità, probabilità e impatto.
- Garanzia che il quadro di gestione delle minacce e dei rischi informatici sia accettato e condiviso a un livello adeguato nell'ambito dell'organizzazione.

3.40 La Terza parte deve garantire che a tutti i rischi e alle minacce identificati in fase di valutazione delle minacce e dei rischi alla Sicurezza informatica venga data la giusta priorità e che vengano prese le dovute misure per mitigare tali rischi entro tempi ragionevoli.

3.41 La Terza parte dovrà informare lo Stakeholder BT qualora non fosse in grado di porre rimedio a, o ridurre, eventuali aree sostanziali di rischio che potrebbero avere un impatto sul servizio reso.

Gestione delle Identità e Controllo degli Accessi

3.42 La Terza parte deve implementare un quadro coerente e consolidato per la gestione in sicurezza delle identità e delle credenziali da parte di personale autorizzato:

- Concedendo, riabilitando, modificando e disabilitando i diritti di accesso esclusivamente in base ad autorizzazioni documentate e approvate.
- Garantendo che gli account inattivi vengano disabilitati.
- Disabilitando gli account dei membri del personale che non sono più dipendenti dell'azienda.
- Implementando processi e strumenti per tracciare, controllare, prevenire e correggere l'uso, l'assegnazione e la configurazione di privilegi amministrativi su computer, reti e applicazioni.
- Tramite analisi periodiche degli accessi che garantiscano che ogni accesso sia idoneo allo scopo.
- Prevedendo il (rinnovo) della certificazione per l'accesso degli account utente almeno su base annuale e degli account con privilegi almeno ogni trimestre.
- Garantendo che le credenziali e i dati confidenziali permanenti (ad esempio, per l'accesso di emergenza di tipo "break glass" in caso di necessità) siano custoditi all'interno di un archivio protetto da hardware e siano resi disponibili solo al o ai responsabile/i in caso di emergenza.

3.43 L'archiviazione centrale delle credenziali permanenti deve essere protetta da sistemi hardware. Ad esempio, su un host fisico l'unità potrebbe essere crittografata utilizzando un Trusted Platform Module (TPM), come definito nell'allegato A del Codice di condotta

sulla sicurezza delle telecomunicazioni. Nel caso in cui venga utilizzata una macchina virtuale (VM) per fornire un servizio di archiviazione centrale, anche tale VM e i dati in essa contenuti devono essere crittografati, con utilizzo di avvio protetto (secure boot) e di una configurazione tale da garantire la possibilità di avviamento solo all'interno di un ambiente appropriato. La Terza parte deve garantire che l'accesso remoto venga gestito in modo che solo i soggetti autorizzati possano connettersi in remoto ai Sistemi della Terza parte e che le connessioni siano protette e non consentano la fuga di dati. Dovrà altresì garantire l'applicazione di un sistema di controllo degli accessi adeguato, come l'autenticazione a più fattori.

- L'autenticazione a due fattori dovrebbe essere ottenuta usando un ID utente, una password e uno dei seguenti metodi:
- Un generatore di password monouso - che richieda un codice PIN/password specifico dell'utente per visualizzare la password monouso.
- Una smart card con chip conforme alla norma ISO 7816 e un software e lettore di schede associato. Le smart card contactless non sono consentite.
- Autenticazione basata su certificato emesso nel rispetto della propria politica sui certificati Infosec.

Per fugare ogni dubbio, se l'accesso con privilegi a scopo di assistenza viene fornito tramite accesso in remoto, ciò dovrà avvenire mediante una connessione protetta e l'autenticazione a due fattori.

- 3.44 La Terza parte deve assicurarsi che i permessi e le autorizzazioni di accesso per tutti i sistemi (compresi gli strumenti, le applicazioni, i database, i sistemi operativi, gli hardware, ecc.) vengano gestiti integrando i principi dei privilegi minimi e della separazione dei compiti.
- 3.45 La Terza parte deve assicurarsi che ogni transazione possa essere ricondotta esclusivamente a un unico soggetto identificabile; in caso di credenziali condivise, che siano stati implementati adeguati controlli di compensazione (incluse le procedure per gli accessi in caso di emergenza). Non sono consentite credenziali condivise per l'accesso privilegiato.
- 3.46 La Terza parte deve assicurarsi che tutte le autenticazioni vengano gestite in modo proporzionale al rischio della transazione, ovvero utilizzando password di lunghezza e complessità adeguata, modificando le password a intervalli regolari, usando l'autenticazione a più fattori, tramite una gestione sicura delle credenziali di accesso e mediante altre misure di controllo. L'accesso privilegiato deve avvenire tramite account dotati di autenticazione a più fattori. Gli account utente con privilegi per l'accesso di emergenza di tipo "break-glass" devono disporre di credenziali sicure e univoche per ciascun punto di accesso dell'apparecchiatura di rete.
- 3.47 Devono altresì essere implementate delle misure di controllo adeguate per la gestione delle autenticazioni non andate a buon fine, comprese le notifiche a schermo, login negati e blocco di utenti.
- 3.48 Devono essere implementati processi e misure di controllo per la gestione e l'autorizzazione di account guest e di assistenza.

Classificazione e Protezione dei Dati

3.49 La Terza parte deve implementare uno schema/quadro per la gestione e la classificazione delle informazioni coerente e consolidato (in linea con le best practice del settore e i requisiti BT) comprensivo dei seguenti elementi:

- Linee guida per la gestione delle informazioni.
- Le informazioni devono essere protette in linea con il livello di classificazione assegnato.
- Garanzia che tutto lo staff sia al corrente che le Informazioni BT non dovranno essere utilizzate per scopi diversi da quelli per cui sono state fornite.

Prevenzione della fuga di dati

3.50 La Terza parte deve disporre di un quadro coerente e consolidato per garantire la protezione dei dati da fughe accidentali assicurandosi che detta protezione includa (senza limitarsi a) i seguenti vettori:

- E-mail, Internet / Web Gateway (inclusa l'archiviazione online e la webmail), USB, porte ottiche e altre tipologie di porte/archiviazione portatile ecc., Mobile Computing e BYOD, servizi di accesso remoto, meccanismi di condivisione di file e social media.
- I dispositivi non autorizzati devono essere disconnessi dalla rete (dalla rete aziendale del vendor o dai sistemi/reti di BT) oppure utilizzati per accedere a informazioni non pubbliche.

PCI DSS

3.51 La Terza parte deve garantire che, qualora fosse coinvolta nella gestione di dati relativi alle Carte di pagamento, opererà secondo quanto indicato nel PCI-DSS. Inoltre, la Terza Parte deve registrare le attività relative alle carte di pagamento presso il PCI Governance & Assurance Team tramite invio di e-mail all'indirizzo della Group PCI Compliance group.pci.compliance@bt.com.

Gestione delle Vulnerabilità.

3.52 La Terza parte deve disporre di un quadro coerente e consolidato per la gestione delle vulnerabilità comprensivo dei seguenti aspetti:

- Politiche e procedure di processo.
- Ruoli e responsabilità definiti.
- Strumenti idonei come quelli per il rilevamento delle intrusioni e di scansione delle vulnerabilità.

3.53 Il quadro di gestione delle vulnerabilità della Terza parte deve garantire il monitoraggio regolare di quanto segue, per rilevare potenziali attacchi alla sicurezza informatica:

- Sistemi e risorse chiave.
- Connessioni non autorizzate.
- Software / applicazioni non autorizzati.
- Attività di rete.

3.54 Il quadro di gestione delle vulnerabilità della Terza parte deve garantire che:

- Siano stati predisposti dei processi per ricevere, analizzare e rispondere alle vulnerabilità dell'organizzazione, derivanti da fonti interne ed esterne (ad esempio, test interni, bollettini sulla sicurezza o ricercatori in materia di sicurezza).
- Devono essere consentiti esclusivamente strumenti, tecnologie e utenti autorizzati.
- Le vulnerabilità individuate vengono mitigate o documentate come rischi accettati.

Monitoraggio e Analisi della Sicurezza.

3.55 La Terza parte deve garantire di disporre di un quadro coerente e consolidato per la gestione di audit e log che preveda sistemi e applicazioni chiave per la registrazione di eventi chiave (compresi gli accessi con privilegi e l'attività del personale). Le registrazioni risultanti devono essere conservate per un periodo minimo di 13 mesi. Le registrazioni delle apparecchiature di rete presenti nelle Funzioni critiche per la sicurezza devono essere integralmente disponibili per l'audit per 13 mesi. Come minimo, la Terza parte deve garantire che i log (ove appropriato) contengano i seguenti eventi:

- Un audit consolidato e coerente e punti di inizio e fine del processo registrato.
- Modifiche al tipo di evento analizzato, in base a quanto richiesto dall'*audit trail* (ad esempio, i parametri di avvio e le eventuali modifiche ad essi apportate).
- Avvio e spegnimento del sistema.
- Login avvenuti con successo.
- Tentativi di login non andati a buon fine (ad esempio, inserimento di ID utente o password errati).
- Creazione, modifica ed eliminazione di account utente.
- Risorsa alla quale i soggetti hanno avuto accesso (ad esempio, dati).
- Il punto dal quale è avvenuto l'accesso alla risorsa (ad esempio, indirizzo IP).
- Quando (ad esempio, data e ora).

3.56 Il quadro di gestione delle attività di audit e log deve prevedere i seguenti aspetti:

- I log degli eventi principali vengono rivisti da un soggetto indipendente almeno una volta al mese per rilevare eventuali attività non autorizzate, metodi e target degli attacchi.
- Le eccezioni osservate vengono studiate fino alla relativa risoluzione.
- I log vengono raccolti da più fonti e sensori, messi in correlazione tra loro, archiviati in una posizione sicura e a prova di manomissione per poter procedere alla ricostruzione degli eventi.
- L'impatto degli eventi viene determinato in base a delle soglie di allerta incidente prestabilite, che prevedono un'azione tempestiva determinata dalla criticità dell'allarme.

4. Sicurezza del Personale

4.1 La Terza parte dovrà assicurarsi che tutto il Personale abbia sottoscritto accordi di riservatezza prima di iniziare il lavoro presso le sedi 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.

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

- Accesso ai Sistemi BT o alle Informazioni BT; o
- Esecuzione di lavori connessi alla prestazione del Servizio.

Inoltre, la Terza parte deve assicurarsi di aver implementato procedure idonee a garantire che qualsiasi membro del suo Personale così escluso non possa effettivamente accedere ai Sistemi BT, alle Informazioni BT né svolgere operazioni connesse alla prestazione del Servizio.

4.3 Nei limiti consentiti dalla legge, la Terza parte dovrà prevedere un canale riservato che il suo 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.

4.4 Quando il Personale della Terza parte non sarà più assegnato a un Servizio, a discrezione di BT, ogni risorsa fisica o Informazione BT in possesso del Personale della Terza parte dovrà essere: restituita alla squadra operativa di BT interessata, oppure distrutta in sicurezza come da controlli di sicurezza 3.22 e 3.23.

4.5 La Terza parte deve disporre di un quadro coerente e consolidato relativo all'uso accettabile di social media personali e aziendali. Detto quadro deve comprendere la garanzia che il personale:

- non pubblichi alcunché di diffamatorio, osceno o offensivo nei confronti dell'organizzazione e dei suoi clienti;
- non utilizzi loghi dell'organizzazione o dei clienti senza autorizzazione;
- non diffonda informazioni non pubbliche relative all'organizzazione o ai clienti senza consenso;
- non pubblichi opinioni relative all'organizzazione e ai suoi clienti che potrebbero ragionevolmente essere interpretate come commenti ufficiali dell'organizzazione o dei suoi clienti;
- non divulghi qualsivoglia Informazione BT contrassegnata come "Riservata" o "Strettamente confidenziale".

4.6 La Terza parte deve garantire che tutti i membri del suo personale che operano sotto il suo controllo partecipino ai corsi di formazione obbligatori sulla Sicurezza delle informazioni, che devono comprendere le best practice in tema di sicurezza informatica e la protezione dei dati personali. Detti corsi devono essere frequentati entro un mese dall'inizio del rapporto lavorativo e devono prevedere aggiornamenti una volta all'anno, compresi, ove appropriato:

- Utenti con privilegi
- Stakeholder di Terzi (ad esempio, subappaltatori, clienti, partner)
- Alta dirigenza
- Personale addetto alla Sicurezza fisica e informatica

- 4.7 La Terza parte deve garantire l'esistenza di un test atto a verificare che l'utente abbia compreso le nozioni apprese durante le attività di sensibilizzazione e formazione.

5. Audit e Revisione della sicurezza

- 5.1 Fatto salvo qualsiasi altro diritto di verifica spettante a BT, al fine di valutare la conformità della Terza parte ai controlli di sicurezza della presente policy sui Requisiti di sicurezza, 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 dello svolgimento di un audit in loco di routine, 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) attinenti al Servizio prestato.
- 5.2 La Terza parte collaborerà 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 entro un periodo stabilito dalle parti, a spese della Terza parte.
- 5.3 Qualora BT dovesse svolgere un audit indipendente relativo alla Terza parte e la Terza parte dovesse rivelarsi non conforme ai principi e alle prassi di cui alla norma ISO/IEC 27001, la terza parte dovrà, a sue spese, adottare 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 consentire a BT di svolgere un'ispezione dell'ambiente di controllo in cui vengono sviluppati, realizzati o prestati i servizi, affinché possa eseguire delle prove e/o valutazioni di conformità ai requisiti di sicurezza dietro ragionevole richiesta (o subito dopo un incidente).
- 6.2 I costi sostenuti per rimediare a eventuali punti deboli nel sistema di sicurezza individuati da BT saranno in capo alla Terza parte, che dovrà provvedere nelle tempistiche stabilite dalle due Parti.
- 6.3 In caso si verifichi un incidente grave, la Terza parte dovrà collaborare appieno con BT ad eventuali indagini conseguenti svolte da BT, un'autorità normativa e/o un'autorità incaricata dell'applicazione della legge, garantendo l'accesso e l'assistenza necessari e appropriati per lo svolgimento delle dovute indagini. BT potrebbe dover richiedere la collocazione in isolamento della Terza parte per valutare eventuali risorse pertinenti appartenenti alla Terza parte e facilitare le indagini; la Terza parte non dovrà negare o ritardare tale richiesta senza giustificazione.

7. Certificazioni di Sicurezza

- 7.1 I Sistemi, il Servizio e i Servizi associati, i processi e le localizzazioni fisiche della Terza parte devono essere conformi alla norma ISO/IEC 27001 (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. Tale conformità deve essere garantita dalla certificazione dell'ISMS della Terza parte da parte di un servizio di accreditamento del Regno Unito (UKAS) o di un organismo di certificazione approvato internazionalmente equivalente, il cui ambito e dichiarazione di applicabilità comprendano i servizi forniti nelle sedi da cui verranno forniti.
- 7.2 La Terza parte deve presentare un certificato valido all'inizio del rapporto contrattuale e ogniqualvolta verrà ricertificata.
- 7.3 Se l'ambito della certificazione o della dichiarazione di applicabilità viene modificato durante il periodo di validità del contratto in modo tale da non coprire più tutti i servizi forniti nelle localizzazioni dalle quali sono forniti, la Terza parte deve informare BT entro un periodo di tempo ragionevole. La Terza parte deve informare BT, entro due giorni lavorativi, di eventuali non conformità di entità sostanziale che saranno state individuate dall'ente certificatore o dalla Terza parte, e che rappresentino un rischio per i servizi forniti.

8. Sicurezza fisica – Sede di BT

- 8.1 La Terza parte dovrà operare nel rispetto di tutte le istruzioni rilevanti che le verranno fornite relativamente all'accesso ai locali BT e ai sistemi di accesso all'edificio. Tutto il Personale della Terza parte operativo presso le sedi BT dovrà essere in possesso di, e mostrare chiaramente, una tessera identificativa fornita da BT o dalla Terza parte, la quale deve essere corredata di una fotografia chiara e che raffiguri in modo veritiero il Personale della Terza parte.
- 8.2 BT può anche fornire al Personale della Terza parte una tessera di accesso elettronica e/o una tessera per visitatori a durata limitata da utilizzare secondo le istruzioni di emissione e revoca locali.
- 8.3 La Terza Parte è responsabile di informare BT entro 24 ore nel caso in cui un soggetto della Terza Parte non necessiti più di accedere all'edificio di BT e/o ai sistemi di accesso BT.
- 8.4 Solo i server con una configurazione approvata da BT, i Webtop PC di BT e gli End Device affidabili possono essere connessi direttamente (con connessione a una porta LAN o con connessione Wireless) ai domini BT. Senza autorizzazione scritta di BT, la Terza parte non potrà collegare nessuna apparecchiatura non approvata da BT a Domini BT.
- 8.5 I criteri di protezione fisica e le linee guida per lavorare presso le sedi di BT dovranno essere rispettati e dovranno includere, a titolo esemplificativo ma non esaustivo, l'accompagnamento del Personale della Terza parte e l'adozione di pratiche di lavoro appropriate all'interno delle aree protette.
- 8.6 Qualora la Terza parte sia autorizzata a fornire al suo Personale accesso senza accompagnamento a determinate aree all'interno della proprietà di BT, il firmatario autorizzato della Terza parte e il Personale della Terza parte dovranno attenersi alle

indicazioni contenute nel documento [Accesso ai siti di BT da parte dei Fornitori - Guida obbligatoria alla sicurezza](#) [Vendite a BT](#).

9. Sicurezza fisica – Sedi di terzi

- 9.1 La Terza parte deve disporre di un processo di accesso fisico che comprenda le autorizzazioni e i metodi di accesso alle sedi della stessa Terza parte (impianti, edifici e aree interne) in cui vengono prestati i servizi, o in cui sono conservate e trattate le Informazioni BT. Il metodo di accesso deve comprendere uno o più dei seguenti elementi:
- Una tessera identificativa della Terza parte autorizzata, munita di foto chiaramente visibile e riconducibile al suo proprietario.
 - Una tessera elettronica di accesso autorizzato per accedere alle zone applicabili della sede in oggetto.
 - Un accesso di sicurezza tramite tastierino, dotato delle seguenti funzioni: autorizzazione, divulgazione della modifica di codice (obbligatoria almeno una volta al mese), modifiche di codice speciali.
 - Riconoscimento biometrico.
- 9.2 La Terza parte deve disporre di processi e procedure per il controllo e il monitoraggio di visitatori e altri soggetti esterni, incluse Terze parti autorizzate ad accedere fisicamente ad aree protette o a scopo di controllo ambientale, gestione degli allarmi e pulizie.
- 9.3 Le aree protette presso le sedi di Terze parti utilizzate per la prestazione del servizio (ad esempio, locali per le comunicazioni di rete) dovranno essere separate dalle aree ad accesso generale e protette mediante appropriati sistemi di controllo degli ingressi tali da garantire l'accesso al solo personale autorizzato. L'accesso a tali aree deve essere verificato regolarmente e, almeno una volta all'anno, deve essere condotta una valutazione per confermare o meno i diritti di accesso a tali aree.
- 9.4 La Terza parte dovrà disporre di sistemi di sicurezza TVCC nei luoghi in cui le Informazioni BT vengono conservate o gestite. Tutte le registrazioni del sistema TVCC e i registratori devono essere collocati in un luogo sicuro per evitare modifiche, cancellazioni o visione casuale degli schermi TVCC. L'accesso alle registrazioni deve essere controllato e limitato solo ai soggetti autorizzati. Le registrazioni del sistema TVCC devono essere conservate per un massimo di 5 giorni.
- 9.5 La Terza parte deve aver implementato appropriate misure per garantire la sicurezza fisica con riferimento a quanto segue:
- Misure di prevenzione antincendio tra cui, a titolo esemplificativo ma non esaustivo, allarmi e attrezzature di rilevazione ed estinzione.
 - Condizioni climatiche, tenendo in considerazione aspetti quali temperatura, umidità ed elettricità statica, e relativa gestione, monitoraggio e risposta a condizioni estreme (come lo spegnimento automatico o gli allarmi).
 - Attrezzature di controllo tra cui, a titolo esemplificativo ma non esaustivo, climatizzazione e rilevamento acqua.
 - Prevenzione di danni dovuti all'acqua, posizionamento dei serbatoi dell'acqua, delle tubature, ecc. presso la sede.

- 9.6 La Terza parte deve assicurarsi che l'accesso fisico alle aree in cui sono conservate le Informazioni BT venga effettuato con smart card o carte di prossimità (o sistemi di sicurezza equivalenti o superiori), oltre a effettuare dei controlli con frequenza mensile per garantire che questo tipo di accesso sia consentito solo ai soggetti interessati.
- 9.7 La Terza parte deve garantire il divieto di fotografare e/o acquisire immagini di qualsivoglia Informazione BT. Qualora l'acquisizione delle immagini sia richiesta per motivi professionali, sarà necessario ottenere precedentemente l'autorizzazione scritta dello Stakeholder BT.

10. Fornitura di un ambiente di Hosting per Apparecchiature BT

- 10.1 Qualora fornisca un'area ad accesso sicuro presso la sua sede per la custodia delle apparecchiature di BT o dei clienti BT, la Terza parte deve:
- Fornire a BT una planimetria degli spazi assegnati nell'area sicura presso la sede.
 - Garantire che gli armadi di BT e dei clienti di BT presso la sede rimangano sempre chiusi e vi possa accedere solo il personale BT autorizzato, i rappresentanti approvati da BT e il personale della Terza parte interessato.
 - Mettere in atto una procedura sicura di gestione delle chiavi.
- 10.2 BT dovrà fornire alla Terza parte quanto segue:
- Un documento riportante le risorse fisiche di BT e/o dei clienti di BT conservate presso la sede della Terza parte.
 - I dettagli relativi ai dipendenti di BT, ai subappaltatori e agli agenti che hanno necessità di accedere alla sede della Terza parte (su base continuativa).

11. Sviluppo software sicuro

- 11.1 La Terza parte deve garantire che gli ambienti produttivi e non vengano adeguatamente controllati, assicurandosi che siano adottate le seguenti misure:
- Segregazione degli ambienti dedicati alla produzione e non, con separazione dei compiti.
 - Nessun dato attivo deve essere utilizzato nell'ambito di test a meno che il titolare dei dati non abbia espresso il suo consenso e previa implementazione di controlli adeguati all'ambiente di produzione
 - Separazione dei compiti tra produzione e sviluppo non in produzione.
- 11.2 La Terza parte deve disporre di un quadro coerente e consolidato relativo allo Sviluppo dei sistemi per evitare vulnerabilità della sicurezza e violazioni della sicurezza informatica, comprensivo dei seguenti aspetti:
- I sistemi devono essere sviluppati in linea con le best practice di sviluppo sicuro (ad esempio, OWASP).
 - Il codice deve essere archiviato in modo sicuro e soggetto a misure di Garanzia della qualità.
 - Il codice deve essere adeguatamente protetto da modifiche non autorizzate successive all'approvazione delle prove e invio in produzione.

12. Deposito Fiduciario

12.1 Qualora sia necessario un deposito in garanzia (Escrow) per tutelare i beni di tutte le parti (Escrow della prima e della terza parte) (ovvero Proprietà intellettuale / Codice sorgente, ecc.), la Terza parte deve disporre di un quadro coerente e consolidato comprensivo dei seguenti aspetti:

- Stipulazione di un Escrow agreement con un Escrow agent che goda di buona reputazione, abbia una posizione neutrale e sia indipendente.
- Condivisione continua di aggiornamenti del codice sorgente con l'Escrow agent a garanzia del costante aggiornamento delle informazioni necessarie.
- Archiviazione sicura del codice sorgente e di altri materiali fino a che non vengano soddisfatte le condizioni di rilascio.
- Condizioni di rilascio adeguate.
- Aggiornamenti continui, pagamenti convenuti e revisioni dell'Escrow agreement.

13. Accesso ai Sistemi BT

13.1 La Terza parte dovrà operare nel rispetto di tutte le istruzioni rilevanti che le verranno fornite relativamente all'accesso ai Sistemi BT e al relativo utilizzo.

13.2 La Terza parte è tenuta a informare BT, entro 24 ore, quando un soggetto facente parte della sua organizzazione cessa di avere necessità di accedere alle risorse.

13.3 La Terza parte dovrà garantire che l'identificazione degli utenti, le password, i PIN, i token e l'accesso alle conferenze siano riferibili a singoli membri del personale della stessa Terza parte e che non vengano condivisi. I dettagli devono essere conservati in modo sicuro e distinto dal dispositivo utilizzato per accedere. Se una password viene resa nota a un'altra persona, tale password deve essere modificata immediatamente.

Connettività tra sistemi

13.4 Il collegamento tra domini ai Sistemi BT non è ammesso se non specificatamente approvato e autorizzato da BT.

13.5 La Terza parte deve compiere ogni ragionevole sforzo per garantire che nei Sistemi BT non vengano introdotti virus o malware (secondo il significato generalmente attribuito a tali espressioni nel settore informatico).

13.6 In caso di connettività tra i sistemi di BT e della Terza parte, tale connettività dovrà realizzarsi per mezzo di collegamenti sicuri in cui i dati saranno protetti mediante crittografia, secondo i controlli crittografici presentati nelle sezioni 14.9, 14.10, 14.11, 14.12 e 14.13.

13.7 La Terza parte deve garantire che i sistemi e le infrastrutture utilizzati siano contenuti in una rete logica dedicata. Tale rete deve essere costituita unicamente dai sistemi dedicati per la fornitura di una struttura di trattamento dati del cliente sicura.

14. Sistemi di Terzi contenenti Informazioni BT

14.1 La Terza parte deve garantire che vengano applicati i patch di sicurezza più recenti a sistemi / risorse / Reti / applicazioni in modo tempestivo a garanzia che:

- La Terza parte utilizzi i patch ottenuti direttamente dai vendor per i sistemi proprietari e patch che siano (i) firmati digitalmente o (ii) verificati tramite l'uso di un hash del vendor (gli hash MD5 non possono essere usati) per il pacchetto di aggiornamento, in modo tale che il patch possa essere identificato come proveniente da una community di supporto affidabile per i software open source.
 - La Terza parte effettui test su tutti i patch su sistemi che rappresentino in modo accurato la configurazione dei sistemi di produzione target prima dell'applicazione del patch sui sistemi di produzione, e che il funzionamento del servizio con patch venga verificato a seguito di tutte le attività di patching.
 - Monitoraggio di tutti i vendor applicabili e di altre fonti di informazioni rilevanti per indicazioni di allerta legate alle vulnerabilità.
 - Qualora sia impossibile applicare un patch a un sistema, adottare le contromisure necessarie.
 - La Terza parte fornirà patch di sicurezza critica separatamente alle varie versioni di una funzione per massimizzare la velocità di distribuzione della patch.
- 14.2 La Terza parte deve garantire che, almeno a cadenza annuale, verrà richiesta l'esecuzione di una valutazione della sicurezza IT o un *penetration test* sulle applicazioni e le infrastrutture IT della Terza parte utilizzate per prestare i servizi, compresi i siti di Disaster Recovery, per identificare vulnerabilità che potrebbero essere sfruttate per violare i dati/servizi, e per impedire la violazione della sicurezza mediante attacchi informatici. Su ragionevole richiesta, la Terza parte deve consentire a BT di accedere ai report dei *penetration test* relativi ai servizi prestati.
- 14.3 La Terza parte deve garantire che l'accesso alle porte di gestione e diagnostica, oltre che agli strumenti di diagnostica, sia controllato in modo sicuro.
- 14.4 La Terza parte deve garantire che l'accesso agli strumenti di audit sia limitato al personale del relativo fornitore e che l'uso di tali strumenti sia monitorato.
- 14.5 La Terza parte deve garantire che i server utilizzati per prestare il servizio non vengano distribuiti su reti non affidabili (rete non compresa nel proprio perimetro di sicurezza, esclusa dal proprio controllo amministrativo, ad es. per interazione con Internet) senza adeguati controlli di sicurezza.

Asset Management

- 14.6 La Terza parte deve tenere aggiornato un inventario preciso delle risorse informatiche, comprendente tutte le risorse tecnologiche potenzialmente in grado di archiviare o elaborare informazioni, in modo che solo i dispositivi autorizzati abbiano accesso e che i dispositivi non autorizzati e non gestiti vengano individuati e venga loro impedito l'accesso. Tale inventario deve includere tutte le risorse hardware, connesse o meno alla rete dell'organizzazione. Nota: Se applicabile, qualsiasi apparecchiatura BT ospitata in locali di Terze parti deve essere inclusa nell'inventario.
- 14.7 La Terza parte deve garantire che nell'inventario degli asset informatici venga catalogato quanto segue:
- Dispositivi e sistemi fisici, applicazioni e piattaforme software, sistemi informatici esterni.

- Alle risorse (ad esempio, hardware, dispositivi, dati, tempo e software) deve essere assegnato un diverso livello di priorità in base alla relativa classificazione, criticità e valore commerciale.
 - Flussi di dati relativi all'Organizzazione e alla Comunicazione, inclusi i flussi di Terzi/esterni.
 - Processi manuali nell'ambito dei quali vengono gestiti dati BT o relativi ai Clienti BT.
- 14.8 La Terza parte deve mantenere aggiornato un inventario preciso delle risorse software per tutto il software sulla rete, in modo che solo il software autorizzato sia installato e possa essere eseguito, e che il software non autorizzato e non gestito venga rilevato e ne venga impedita l'installazione o l'esecuzione.

Crittografia

- 14.9 La Terza parte deve garantire che le informazioni BT classificate come Riservate o con grado di confidenzialità superiore siano adeguatamente crittografate (in transito e a riposo) e che la crittografia sia integralmente eseguita con algoritmi crittografici e cifrari potenti e moderni, che impieghino solidi meccanismi di protezione dell'integrità e in conformità con gli standard di settore per la negoziazione di chiavi e protocolli e gestione delle chiavi in sicurezza. Le seguenti opzioni TLS non sono consentite per dati in transito: TLS v1.0, TLS v1.1, v6.0 e SSL (tutte le versioni). Le seguenti opzioni IPsec non sono consentite: IKE versione 1.
- 14.10 Le chiavi crittografiche devono avere una lunghezza pari o superiore a quella indicata di seguito:
- Le chiavi simmetriche (ad es. AES) devono avere una lunghezza pari ad almeno 256 bit.
 - Le chiavi asimmetriche (ad es. RSA) devono avere una lunghezza pari ad almeno 2048 bit.
 - Le chiavi a curva ellittica devono avere una lunghezza pari ad almeno 224 bit.
- 14.11 Qualora il NIST dovesse dichiarare che un certo algoritmo di crittografia non è più sicuro, questo non dovrà essere utilizzato per le nuove versioni. Le versioni esistenti che fanno ancora uso di algoritmi di crittografia obsoleti devono essere sottoposte a revisione e deve essere previsto un piano di migrazione per passare ad algoritmi più sicuri.
- 14.12 Per la crittografia simmetrica è possibile utilizzare i seguenti algoritmi: 3DES-168 (se non stabilito da uno standard internazionale), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed e ARIA.
- 14.13 Utilizzare hash sottoposti a salting per proteggere i dati archiviati, ovvero le password. L'hashing può essere utilizzato anche per anonimizzare i dati prima del trattamento, ad esempio gli MSISDN o i dati relativi ai pagamenti. I seguenti algoritmi di hashing non sono consentiti: MD2, MD4, MD5 e SHA-1.

Configurazione dei Sistemi

- 14.14 La Terza parte deve disporre di un quadro coerente e consolidato per la gestione a garanzia che i sistemi vengano configurati in maniera adeguata, compresi i seguenti aspetti:

- I sistemi e i dispositivi di rete sono configurati in modo da funzionare secondo i principi di sicurezza (ad esempio, principio di minima funzionalità e assenza di software non autorizzati).
- Garanzia che tutti i dispositivi siano settati sullo stesso orario corretto.
- I sistemi devono essere privi di software dannosi.
- Le build e i dispositivi vengono sottoposti a un controllo e monitoraggio appropriato per garantirne l'integrità.

Protezione dai malware.

14.15 La Terza parte deve garantire l'applicazione della protezione anti-malware più aggiornata possibile a tutte le risorse IT pertinenti al fine di evitare l'interruzione dei servizi o violazioni alla sicurezza, oltre a garantire l'attivazione di attività di sensibilizzazione degli utenti appropriate.

Nota: L'anti-malware deve includere, a titolo esemplificativo e non esaustivo, il rilevamento di codice mobile non autorizzato, virus, spyware, software di registrazione delle chiavi, botnet, worm, trojan, ecc.

Mitigazione dei casi di "Denial of Service".

14.16 La Terza parte deve assicurarsi che i sistemi principali siano protetti da attacchi di tipo "Denial of Service" (DoS) e "Distributed Denial of Service" (DDoS).

15. Terze parti che custodiscono Informazioni BT

15.1 In aggiunta ai controlli della Sezione 14. Sistemi di Terze parti che custodiscono informazioni BT: se una terza parte custodisce informazioni di BT in un data center o in una soluzione cloud, 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).

16. Sicurezza di rete – Rete propria di BT

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

16.1 Su richiesta, la Terza Parte fornirà a BT i nomi, gli indirizzi e altri dettagli che BT ragionevolmente richiederà per tutto il personale della Terza parte che:

- sia di volta in volta direttamente coinvolto nell'implementazione, manutenzione e/o gestione del/i Servizio/i prima della rispettiva assunzione.
- collabori con BT relativamente al dibattito sulle vulnerabilità identificate da BT e/o da Terze parti nei Servizi.

16.2 In relazione alle sue attività di supporto localizzate nel Regno Unito, la Terza parte dovrà disporre di un team di addetti alla sicurezza qualificati, composto da almeno un cittadino britannico che dovrà essere disponibile per mantenere i rapporti con BT e partecipare alle riunioni che BT deciderà ragionevolmente di richiedere periodicamente.

- 16.3 La Terza parte dovrà fornire a BT un programma (opportunamente aggiornato secondo necessità) di tutti i componenti attivi compresi nel Servizio/i e le loro rispettive fonti.
- 16.4 La Terza Parte fornirà a BT tempestivamente (ossia, non appena possibile per consentire la correzione prima della pubblicazione) informazioni in relazione a qualsiasi vulnerabilità nel/i Servizio/i e si conformerà (a spese della Terza Parte) ai ragionevoli requisiti in materia di vulnerabilità che potranno essere notificati da BT.
- 16.5 La Terza parte dovrà garantire che tutti i componenti riferibili alla sicurezza compresi nel/i Servizio/i, così come identificati da o per BT, vengano, periodicamente e a spese della Terza parte, valutati esternamente a ragionevole soddisfazione di BT.
- 16.6 La Terza parte dovrà fornire prontamente, e in ogni caso entro 7 giorni lavorativi, a BT dettagli completi relativi a qualsivoglia caratteristica e/o funzionalità del/i Servizio/i (o che siano state pianificate nella Roadmap di ciascuno dei Servizi) che, di volta in volta:
- siano note alla Terza parte; o
 - BT ritenga ragionevolmente siano progettate, o possano essere utilizzate per intercettazioni illegali o altro tipo di intercettazione o traffico delle telecomunicazioni, e informi di conseguenza la Terza parte. Tali dettagli dovranno includere tutte le Informazioni ragionevolmente necessarie per consentire a BT di comprendere appieno la natura, la composizione e l'ambito di applicazione di tali caratteristiche e/o funzionalità.
- 16.7 Alla Terza parte non è consentito utilizzare strumenti di monitoraggio di rete in grado di visualizzare informazioni sulle applicazioni.
- 16.8 Il Personale di Terze parti addetto alla costruzione, sviluppo e/o supporto della rete di BT deve essere sottoposto come minimo a un controllo pre-assunzione L2. Controlli pre-assunzione L3 saranno richiesti per i ruoli identificati da BT.
- 16.9 La Terza parte consentirà a BT di installare software di sicurezza secondo le specifiche di BT, su qualsiasi infrastruttura virtuale della Terza parte (inclusi, a titolo esemplificativo ma non esaustivo, macchine virtuali e container) o sistema operativo installato da Terze parti e in esecuzione su Reti BT.

Telecommunications (Security) Act 2021 (TSA)
Laddove il servizio di Terze parti rientri nell'ambito del Telecommunications (Security) Act 2021(TSA), si applicano i seguenti controlli di sicurezza.

- 16.10 Nel caso in cui la Terza parte supporti più di un operatore, è necessario implementare controlli per impedire a un operatore o alla sua rete di impattare negativamente qualsiasi altro operatore o sua rete.
- 16.11 Nel caso in cui la Terza svolga una funzione amministrativa per più di un operatore, si applicano i seguenti controlli:
- Implementazione di separazione logica all'interno della rete di Terze parti per separare i dati e le reti dei clienti.
 - Implementazione di separazione tra ambienti di gestione di Terze parti utilizzati per reti di operatori diversi.
 - Implementazione e applicazione di funzioni di sicurezza al confine tra la rete di Terze parti e la rete dell'operatore.

- Implementazione di controlli tecnici per limitare la possibilità che utenti o sistemi abbiano un impatto negativo su più di un operatore.
 - Implementazione di Postazioni di lavoro ad accesso privilegiato logicamente indipendenti per ciascun operatore.
 - Implementazione di domini e account amministrativi indipendenti per ciascun operatore.
- 16.12 Quando si forniscono apparecchiature di rete, le Terze parti devono fornire a BT una "dichiarazione di sicurezza" relativamente alle modalità di produzione dell'apparecchiatura sicura e di garanzia di sicurezza dell'apparecchiatura per tutta la vita utile. Tale dichiarazione di sicurezza risponde ai requisiti della Valutazione della sicurezza del fornitore pubblicata nell'allegato B del Codice di condotta sulla sicurezza delle telecomunicazioni.
- 16.13 Se la Terza parte fornisce apparecchiature di rete, sono applicabili i seguenti controlli:
- La Terza parte garantisce che aderirà a uno standard non inferiore a quello della sua 'dichiarazione di sicurezza' pubblicata.
 - La Terza parte fornirà indicazioni aggiornate sulle modalità di distribuzione in sicurezza dell'apparecchiatura.
 - La Terza parte supporterà tutte le apparecchiature e tutti i sottocomponenti software e hardware per la durata del contratto.
 - La Terza parte fornirà dettagli relativi a tutti i principali componenti e dipendenze di terze parti, inclusi, a titolo esemplificativo ma non esaustivo, prodotto e versione, componenti open source, livello di supporto e periodo.
 - La Terza parte risolverà tutti gli eventuali problemi relativi alla sicurezza che rappresentano un rischio per la sicurezza della rete o del servizio di un fornitore rilevati all'interno dei propri prodotti entro un intervallo di tempo ragionevole dalla notifica, fornendo nel frattempo aggiornamenti regolari sui relativi progressi (tale intervallo tempo deve essere concordato tra BT e la Terza parte che dovranno entrambi comportarsi ragionevolmente). Ciò comprende tutti i prodotti interessati dalla vulnerabilità, e non soltanto il prodotto per il quale è stata segnalata la vulnerabilità.
- 16.14 Se la Terza parte ha ottenuto valutazioni o certificazioni di sicurezza delle apparecchiature riconosciute a livello internazionale (ad es. Common Criteria o NESAS), queste devono essere pubblicate includendo i risultati completi che comprovano tale valutazione o certificato.
- 16.15 Nel caso in cui la rete di una Terza parte possa avere un impatto sulle reti di BT, la Terza parte, come da istruzioni BT, sarà sottoposta allo stesso programma di test applicato da BT alle Reti di BT e potrà rimedio alle vulnerabilità identificate come concordato da entrambe le parti.
- 16.16 La Terza parte autorizza BT a condividere i dettagli di criticità relative alla sicurezza, se necessario ai fini della sicurezza della rete.
- 16.17 L'infrastruttura e i sistemi utilizzati per la manutenzione delle Reti di BT devono essere localizzati nel Regno Unito.

- 16.18 Nel caso in cui la Terza parte svolga Funzioni di supervisione della Rete di BT, le apparecchiature utilizzate per tale funzione devono essere localizzate nel Regno Unito e inoltre gestite da personale con sede nel Regno Unito.
- 16.19 Nel caso in cui la Terza parte sia responsabile della sicurezza della rete e dei registri di controllo, questi devono essere conservati nel Regno Unito e protetti in base al diritto del Regno Unito.

17. Sicurezza di rete della Terza parte

17.1 La Terza parte deve garantire che l'integrità di rete venga stabilita e mantenuta accertandosi che i seguenti elementi siano opportunamente verificati:

- Le connessioni esterne alla rete sono documentate, passano attraverso un firewall e sono verificate e approvate prima di essere create al fine di evitare violazioni della sicurezza dei dati.
- La rete è progettata in modo opportuno in base principio di "defense in depth" per ridurre al minimo le violazioni della Sicurezza informatica mediante l'implementazione di appropriati controlli, come la "segmentazione di rete", volti a prevenire eventuali attacchi intenzionali.
- La progettazione e l'implementazione della rete vengono riviste almeno una volta all'anno.
- Tutti gli accessi in modalità wireless alla rete sono soggetti a protocolli di autorizzazione, autenticazione, segmentazione e crittografia per prevenire violazioni alla sicurezza.
- Uso di comunicazioni sicure tra dispositivi e stazioni di gestione.
- Uso di comunicazioni sicure tra dispositivi secondo quanto appropriato, compresa la crittografia di tutti gli accessi di amministratore non tramite console.
- Uso di una potente architettura di rete, suddivisa in livelli e zone e dotata di un'efficace sistema di gestione delle identità e di una configurazione del sistema operativo che deve essere adeguatamente protetta e documentata.
- Mediante la disattivazione (ove applicabile) dei servizi, delle applicazioni e delle porte che non verranno utilizzati.
- Mediante la disattivazione o la rimozione degli account guest.
- Non autorizzando relazioni di trust tra server.
- Uso del principio di sicurezza del "privilegio minimo" delle best practice per lo svolgimento di una funzione.
- Garantendo l'applicazione di misure idonee al rilevamento di intrusioni e/o alla protezione contro di esse.
- Ove appropriato, monitorando l'integrità dei file in modo da rilevare eventuali aggiunte, modifiche o eliminazioni di dati o file di sistema critici.
- Modifica di tutte le password predefinite o fornite dai vendor prima dell'attivazione dei componenti di rete.

17.2 Nel caso in cui la Terza parte fornisca servizi soggetti al Telecommunications (Security) Act 2021, si applicano i seguenti controlli di sicurezza aggiuntivi:

- I sistemi rivolti verso l'esterno, esclusi i CPE (Customer Premises Equipment), vengono sottoposti a test di sicurezza ogni due anni o ogniqualvolta si verifichi un cambiamento significativo.
- I set di dati sensibili e le funzioni sensibili o critiche non sono ospitati su apparecchiature situate sul bordo esposto della rete (Exposed Edge).
- Se non è prevista la protezione crittografica, deve essere implementata la separazione fisica e logica tra il Bordo esposto e le funzioni sensibili o critiche.
- La separazione di sicurezza mediante funzioni di applicazione della sicurezza deve essere implementata tra il Bordo esposto e le funzioni sensibili o critiche.

17.3 La rete della Terza parte deve soddisfare tutti i requisiti normativi e di legge; e

- Evitare, al meglio delle proprie possibilità, che soggetti non autorizzati (ad es. hacker) accedano alla/e rete/i della Terza parte.
- Ridurre, al meglio delle proprie possibilità, il rischio di uso improprio della/e rete/i della Terza parte da parte di soggetti non autorizzati ad accedervi.
- Mettere in atto ogni ragionevole sforzo per rilevare eventuali violazioni della sicurezza, consentendo una veloce rettifica dei problemi e l'identificazione dei soggetti che hanno ottenuto l'accesso e della modalità con la quale tale accesso è stato ottenuto.

18. Sicurezza nel Cloud

18.1 La Terza parte deve essere certificata conforme all'ultima versione della norma ISO27017 oppure deve disporre di un quadro coerente e consolidato per garantire che tutti gli usi della tecnologia Cloud e i dati non pubblici archiviati nel Cloud siano approvati e sottoposti ad adeguati controlli equivalenti all'ultima versione del Cloud Controls Matrix (CCM) della Cloud Security Alliance.

18.2 Nei *Service Level Agreement* di rete e infrastruttura (in-house o in outsourcing) dovranno essere chiaramente documentati i controlli di sicurezza, i livelli di capacità e servizio e i requisiti dell'azienda o del cliente

18.3 La Terza parte deve implementare misure di sicurezza relative a tutti gli aspetti del servizio prestato, per tutelare la riservatezza, disponibilità, qualità e integrità riducendo al minimo la possibilità di accesso da parte di soggetti non autorizzati (ad es. altri clienti nel Cloud) alle Informazioni BT e ai servizi utilizzati da BT.

18.4 Nella misura in cui la Terza parte fornisce applicazioni o servizi di hosting a BT, sia a tenant singolo che a più tenant, inclusi software-as-a-service, platform-as-a-service, infrastructure-as-a-service e offerte simili, per acquisire, trasmettere, archiviare o elaborare in altro modo dati riservati, la Terza parte offrirà a BT la possibilità di:

- isolare logicamente tali Dati riservati dai dati di altri clienti della Terza parte;
- limitare, registrare e monitorare l'accesso a tali Dati riservati in qualsiasi momento, incluso l'accesso da parte di personale della Terza parte;
- creare, abilitare, disabilitare ed eliminare la chiave di crittografia al livello più alto (nota come Chiave gestita dal cliente) utilizzata per crittografare e decrittografare le chiavi successive, inclusa la chiave di crittografia dei dati al livello più in basso.

- limitare, registrare e monitorare l'accesso alla Chiave gestita dal cliente in qualsiasi momento; qualsiasi chiave di crittografia successiva - una chiave di cifratura in una gerarchia di chiavi inferiore alla Chiave gestita dal cliente - non dovrà mai essere archiviata nello stesso sistema di Dati riservati a meno che non sia crittografata dalla Chiave gestita dal cliente, condizione detta anche wrapping da parte della Chiave gestita dal cliente.

19. Servizi di telefonia mobile

19.1 Se la Terza parte fornisce Schede SIM, sono applicabili i seguenti controlli:

- Per le schede SIM a profilo fisso, la Terza parte garantirà che i dati sensibili della SIM vengano adeguatamente protetti dal produttore della scheda SIM.
- Per le schede SIM a profilo fisso, la Terza parte garantirà che l'integrità, la riservatezza e la disponibilità dei dati sensibili della SIM condivisi con il produttore delle schede SIM siano protetti in ogni fase del loro ciclo di vita.

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

20.1 Se al Fornitore è richiesto di accedere, archiviare, elaborare o trasmettere informazioni classificate come UFFICIALI del Governo del Regno Unito (HMG) o superiori, il Fornitore deve condurre una valutazione dei rischi per la sicurezza del personale su tutti i ruoli identificati nella Dichiarazione dei dati ufficiali sensibili, paragrafo 2, in linea con i requisiti stabiliti nel documento CPNI Guida al Nulla osta di sicurezza nazionale (4a edizione - giugno 2013 o successiva).

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

20.3 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 per la fornitura di una struttura di trattamento dati del cliente 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 rispetto al Contratto:

Per "Accesso" e "Accessi" si intendono il Trattamento, la gestione o l'archiviazione delle Informazioni BT secondo uno o più dei seguenti metodi:

- a. mediante interconnessione con i Sistemi BT;
- b. consegna in formato cartaceo o non elettronico;
- c. Informazioni BT sui Sistemi del Fornitore; oppure
- d. mediante media mobili

e/o 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 in base al Contratto.

“**Stakeholder (di) BT**” indica il rappresentante di BT che detiene la proprietà dell'ambito di lavoro in oggetto.

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

“**Reti di BT**” indica qualsiasi rete pubblica di comunicazioni elettroniche gestita da BT, come definita dalla sezione 32 del Communications Act 2003.

“**BYOD**” (Bring Your Own Device) significa utilizzo di un dispositivo proprio e non aziendale.

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.

“**Customer Premises Equipment**” indica l'apparecchiatura fornita ai clienti dal fornitore e gestita dal fornitore, che viene utilizzata o è destinata a essere utilizzata come parte della rete o del servizio. Da questa definizione sono esclusi dispositivi elettronici consumer come telefoni cellulari e tablet, mentre sono inclusi dispositivi come firewall edge, apparecchiature SD-WAN e kit di accesso wireless fisso. “”

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

La “**Sicurezza informatica**” è la modalità con la quale i singoli e le organizzazioni riducono il rischio di attacchi informatici. La funzione principale della Sicurezza informatica è proteggere i dispositivi che tutti utilizziamo (smartphone, laptop, tablet e computer) e i servizi a cui accediamo, sia da remoto che in presenza, da furti o danni.

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 le finalità aziendali di BT (incluso il diritto di compilare tale codice sorgente).

Le apparecchiature “**a Bordo esposto**” sono apparecchiature poste all'interno della sede del cliente, direttamente indirizzabili dall'apparecchiatura del cliente/utente, oppure fisicamente vulnerabili. Le apparecchiature fisicamente vulnerabili includono le apparecchiature negli armadi a bordo strada o fissati all'arredo urbano. Le apparecchiature a Bordo esposto comprendono CPE, apparecchiature per stazioni base, apparecchiature OLT e MSAN/DSLAM.

Per “**Best practice di sicurezza di settore**” si intende, relativamente a qualsivoglia iniziativa e in qualsiasi circostanza, l'implementazione delle pratiche, politiche, standard e sistemi di sicurezza che sarebbe ragionevolmente lecito aspettarsi da una persona qualificata e competente impegnata nello stesso tipo di attività, in circostanze uguali o simili.

“**NDA**” (Non Disclosure Agreement) indica un accordo di non divulgazione, un contratto vincolante tra due o più parti che impedisce la condivisione di informazioni sensibili con altri.

“**Risorsa di rete**” Indica un elemento che fa parte di un insieme di componenti interconnessi come computer, router, hub, cavi e controller per le telecomunicazioni, che costituiscono una rete.

"Funzione di supervisione della rete" indica i componenti della rete di BT che sovrintendono e controllano le funzioni critiche per la sicurezza, e che sono pertanto di vitale importanza per la sicurezza globale della rete. Sono essenziali per la comprensione, protezione o ripristino della rete da parte di BT.

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.

"NIST" indica il National Institute of Standards and Technology, un'unità del Dipartimento del Commercio degli Stati Uniti. Precedentemente noto come National Bureau of Standards, il NIST promuove e mantiene gli standard di misurazione. Dispone anche di programmi attivi per incoraggiare e assistere lo sviluppo e l'utilizzo di questi standard da parte dell'industria e della scienza.

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

Per **"Postazione di lavoro con accesso privilegiato (PAW)"** si intende una delle postazioni di lavoro attraverso le quali è possibile ottenere l'accesso privilegiato.

"Funzione critica per la sicurezza" indica qualsiasi funzione della rete o del servizio di BT il cui funzionamento potrebbe avere un impatto sostanziale sul corretto funzionamento dell'intera rete o del servizio o di una parte sostanziale di essi.

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

"SIM" indica un componente hardware o un token univoco e il software associato, utilizzato per autenticare l'accesso dell'utente alla rete. La SIM, utilizzata come descritto in questo documento, comprende l'hardware UICC/eUICC, le applicazioni SIM/USIM/ISIM, la funzionalità eSIM e RSP e qualsiasi applet SIM.

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

Per **"Transazione"** si intendono i dati/informazioni sulle transazioni acquisiti dalle transazioni, ad esempio i dati generati da varie applicazioni durante l'esecuzione o il supporto di processi aziendali quotidiani.

"Terza parte" indica un Fornitore di BT.

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.

"Rete di terzi" indica qualsiasi rete di fornitori.

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 coinvolto nel processo di consegna delle Forniture.

Interpretazione

- 21.2 Tutti i termini che seguono espressioni come “comprensivo di”, “che include”, “in particolare”, “per esempio” o 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 una Parte viene espresso come diritto o obbligo che essa “**può o 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.

Versione	Descrizione	Autore	Data
4.0	Nuovo	Karen Tanner	02/02/2020
4.1	Clausola aggiuntiva per il set di clausole HMG 20	Karen Tanner	20/02/2020
5.1	Legislazione del Telecommunications (Security) Act 2021 (TSA) e adozione del CIS da parte di BT	Jemma Turner	25/10/2022

ALLEGATO 1 – Requisiti di sicurezza aggiuntivi

Se la Terza parte ha necessità di Accedere a, conservare, elaborare o trasmettere informazioni ‘Ufficiali sensibili per il Governo del Regno Unito’, la Terza parte dovrà operare nel rispetto dei presenti Requisiti di sicurezza e, inoltre, dei requisiti indicati nel presente Allegato 1; dovrà altresì fornire a BT una “Dichiarazione sui dati ufficiali sensibili” debitamente compilata prima della sottoscrizione del Contratto. In tutti i casi, il controllo di livello superiore avrà la priorità sui requisiti documentati in altri punti dei presenti Requisiti di sicurezza per i Servizi e i sistemi indicati nella “Dichiarazione sui dati ufficiali sensibili”.

1. DIPENDENTI

- 1.1. Tutti i ruoli identificati dalla Terza parte come autorizzati ad Accedere alle informazioni classificate come “Ufficiali sensibili” o aventi privilegi elevati relativamente alle infrastrutture in cui vengono archiviate, elaborate o trasmesse le informazioni classificate come “Ufficiali sensibili” saranno indicati nella “Dichiarazione sui dati ufficiali sensibili”.
- 1.2. Il Personale della Terza parte che occupa le posizioni indicate nella “Dichiarazione sui dati ufficiali sensibili”:
 - 1.2.1. deve essere sottoposto perlomeno 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 in caso di tentativo di 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 con cadenza almeno annuale. Tali corsi verteranno sui requisiti di gestione delle informazioni, nello specifico delle informazioni classificate come “Ufficiali” o “Ufficiali sensibili” in linea con i requisiti di cui allo Schema di classificazione di sicurezza del Governo del Regno Unito (HMG), così come specificato nelle [Linee guida BT per la protezione delle informazioni HMG da parte di terzi](#)
- 2.2. La Terza parte aggiornerà le *job description* relative ai ruoli indicati della “Dichiarazione sui dati ufficiali sensibili” 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 Accesso dovranno essere revocati dai Sistemi della Terza parte interessati 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 informare 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 informare 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 "Ufficiali" o "Ufficiali sensibili" in linea con i requisiti di cui allo [Schema di classificazione di sicurezza del Governo del Regno Unito](#) e successivi aggiornamenti
- 5. RISPOSTA E REPORTING IN CASO DI INCIDENTE – SERVICE LEVEL AGREEMENT**
- 5.1. La Terza parte verrà informata in merito a *Service level agreement* specifici a supporto delle procedure di risposta in caso di incidente. Questi potrebbero avere priorità 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 sui dati ufficiali sensibili".
- 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.

22. ALLEGATO 1, DOCUMENTO 1 – MODELLO DI “DICHIARAZIONE SUI DATI UFFICIALI SENSIBILI”

1. Sistemi/Servizi in oggetto

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

Sistema	Servizio

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

Ruolo	Livello di nulla osta di sicurezza previsto
* 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

23. ALLEGATO 2, Telecommunications (Security) Act 2021 – Conversione da Codice di condotta a Requisiti di sicurezza

Code of Practice Rif	Clausola di sicurezza BT Rif
M21.04 Nel caso in cui i dati siano archiviati all'estero, il fornitore deve tenere un elenco dei luoghi in cui sono conservati. Il rischio dovuto alla conservazione dei dati in detti luoghi, compreso qualsiasi rischio associato alla legislazione locale sulla protezione dei dati, deve essere gestito nell'ambito dei processi di gestione del rischio del fornitore.	3.8
M10.46 I fornitori devono accertarsi che i loro contratti consentano la condivisione di dettagli su problematiche di sicurezza in modo tale da contribuire all'identificazione e alla riduzione dei rischi di compromissione della sicurezza relativi alla rete pubblica di comunicazione elettronica o al servizio pubblico di comunicazione elettronica a causa di azioni o omissioni da parte di fornitori terzi.	3.31
M10.13 I fornitori dovranno contrattualmente richiedere ai fornitori terzi di individuare e segnalare la causa principale di qualsiasi incidente di sicurezza che potrebbe comportare una compromissione della sicurezza nel Regno Unito entro 30 giorni, e di rettificare eventuali punti deboli riscontrati.	3.33
M5.05 Oltre ai requisiti del CAF D.2, i fornitori sono tenuti a eseguire un'analisi della causa principale di tutti gli incidenti di sicurezza. I risultati di tale analisi devono essere sottoposti ai livelli superiori appropriati, fino ad arrivare al consiglio di amministrazione del fornitore.	3.34
M11.02 Eventuali credenziali e dati confidenziali permanenti (ad es. relativi ad accesso di emergenza) devono essere protetti e non resi disponibili a nessuno tranne che al/i responsabile/i in caso di emergenza.	3.42
M6.02 L'accesso privilegiato deve avvenire tramite account con ID utente e credenziali di autenticazione univoci per ciascun utente, che non devono essere condivisi.	3.45
M6.04 Tutti gli account utente con privilegi di accesso di emergenza devono disporre di credenziali univoche e sicure per ciascun dispositivo di rete.	3.46
M10.24 I fornitori devono richiedere contrattualmente che gli amministratori di terze parti implementino controlli tecnici per impedire a un particolare fornitore o alla sua rete di avere effetti negativi su qualsiasi altro fornitore o sulla sua rete.	16.10
M10.25 I fornitori devono richiedere contrattualmente che gli amministratori di terze parti implementino una separazione logica all'interno della rete dell'amministratore di terze parti per separare i dati e le reti dei clienti.	16.11
M10.26 I fornitori devono richiedere contrattualmente che gli amministratori di terze parti implementino una separazione tra gli ambienti di gestione degli amministratori di terze parti utilizzati per reti di provider diversi.	16.11
M10.27 I fornitori devono richiedere contrattualmente che gli amministratori di terze parti implementino e applichino funzioni di applicazione della sicurezza al confine tra la rete dell'amministratore di terze parti e la rete del fornitore.	16.11

M10.28 I fornitori devono richiedere contrattualmente che gli amministratori di terze parti implementino controlli tecnici per limitare la possibilità che utenti o sistemi abbiano un impatto negativo su più fornitori.	16.11
M10.29 I fornitori devono richiedere contrattualmente che gli amministratori di terze parti implementino postazioni di lavoro con accesso privilegiato logicamente indipendenti per ciascun fornitore.	16.11
M10.30 I fornitori devono richiedere contrattualmente che gli amministratori di terze parti implementino account e domini amministrativi indipendenti per ciascun fornitore.	16.11
M10.36 I fornitori devono richiedere contrattualmente ai fornitori di apparecchiature di rete di condividere una "dichiarazione di sicurezza" sulle modalità di produzione di apparecchiature sicure e accertarsi che tutelino la sicurezza delle apparecchiature per tutta la loro vita utile. È consigliabile che tale dichiarazione sia riferita a tutti gli aspetti descritti nella valutazione della sicurezza del fornitore (VSA) (vedere allegato B), e inoltre, i fornitori dovrebbero incoraggiare i propri fornitori a pubblicare una risposta alla VSA.	16.12
M10.38 I fornitori garantiranno, mediante accordi contrattuali, che la dichiarazione di sicurezza del fornitore di apparecchiature di rete sia approvata a un livello di governance appropriato.	16.12
M10.40 I fornitori devono richiedere contrattualmente al fornitore di apparecchiature di rete di aderire a uno standard non inferiore alla "dichiarazione di sicurezza" dello stesso fornitore di apparecchiature di rete.	16.13
M10.41 I fornitori devono richiedere contrattualmente ai fornitori di apparecchiature di rete di fornire indicazioni aggiornate su come l'apparecchiatura deve essere collocata in modo sicuro.	16.13
M10.42 I fornitori richiederanno contrattualmente ai fornitori di apparecchiature di rete di fornire assistenza per tutte le apparecchiature e tutti i sottocomponenti software e hardware per la durata del contratto. Il periodo di assistenza sia dell'hardware che del software deve essere indicato nel contratto.	16.13
M10.43 I fornitori devono richiedere contrattualmente ai fornitori di apparecchiature di rete di fornire dettagli (su prodotto e versione) dei principali componenti e dipendenze di terze parti, inclusi i componenti open source e il periodo e il livello di assistenza.	16.13
M10.44 Laddove rilevante per un utilizzo particolare delle apparecchiature da parte di un fornitore, i fornitori devono richiedere contrattualmente ai fornitori terzi di porre rimedio a tutte le problematiche di sicurezza che rappresentano un rischio per la sicurezza della rete o del servizio di un fornitore individuate nei loro prodotti entro un periodo di tempo ragionevole dalla notifica, fornendo nel frattempo regolari aggiornamenti sullo stato di avanzamento. Ciò comprende tutti i prodotti interessati dalla vulnerabilità, e non soltanto il prodotto per il quale è stata segnalata la vulnerabilità.	16.13
M10.39 Nel caso in cui il fornitore di apparecchiature di rete dichiari di aver ottenuto valutazioni o certificazioni di sicurezza riconosciute a livello internazionale per le proprie apparecchiature (come Common Criteria o NESAS), i fornitori richiederanno contrattualmente ai fornitori di apparecchiature di condividere con loro le risultanze complete che comprovino tali valutazioni o certificazioni.	16.14
M10.35 I fornitori devono richiedere che le reti dell'amministratore di terze parti che potrebbero avere effetti sul fornitore siano sottoposte allo stesso livello di test che il fornitore applica a se stesso (ad esempio test TBEST come stabilito per il fornitore da Ofcom di volta in volta).	16.15

M10.46 I fornitori devono accertarsi che i loro contratti consentano la condivisione di dettagli su problematiche di sicurezza in modo tale da contribuire all'identificazione e alla riduzione dei rischi di compromissione della sicurezza relativi alla rete pubblica di comunicazione elettronica o al servizio pubblico di comunicazione elettronica a causa di azioni o omissioni da parte di fornitori terzi.	16.16
M21.02 Le misure che devono essere adottate dal fornitore ai sensi del regolamento 3(3)(f) devono normalmente includere la garanzia, per quanto ragionevolmente possibile, che l'apparecchiatura che svolge le Funzioni di supervisione della rete del fornitore sia situata nel Regno Unito e gestita da personale con sede nel Regno Unito.	16.18
M21.02 Le misure che devono essere adottate dal fornitore ai sensi del regolamento 3(3)(f) devono normalmente includere la garanzia, per quanto ragionevolmente possibile, che l'apparecchiatura che svolge le Funzioni di supervisione della rete del fornitore sia situata nel Regno Unito e gestita da personale con sede nel Regno Unito. M16.07 I sistemi che raccolgono ed elaborano dati di registrazione e monitoraggio devono essere gestiti come le Funzioni di supervisione della rete.	16.18 e 16.19
M1.02 I test di sicurezza sui sistemi rivolti verso l'esterno, escluso il CPE, devono normalmente essere eseguiti almeno ogni due anni, e in ogni caso poco dopo il verificarsi di un cambiamento significativo.	17.2
M1.03 Le apparecchiature a bordo esposto non devono ospitare dati sensibili o funzioni critiche per la sicurezza.	17.2
M1.04 Deve essere implementata la separazione fisica e logica tra il bordo esposto e le Funzioni critiche per la sicurezza. (Si noti che questo requisito potrebbe non essere necessario una volta che i set di dati e le funzioni possono essere protetti crittograficamente da alterazioni)	17.2
M1.05 Devono esistere confini di sicurezza tra il bordo esposto e le funzioni critiche o sensibili per l'attuazione di misure di protezione.	17.2
M8.12 Per le schede SIM a profilo fisso, il fornitore deve accertarsi che i dati sensibili della SIM siano adeguatamente protetti durante tutto il loro ciclo di vita, sia dal fornitore della carta SIM che all'interno della rete dell'operatore, dato il rischio per la resilienza e la riservatezza della rete in caso di perdita di tali informazioni.	19.1
M8.13 Per le schede SIM a profilo fisso, l'integrità, riservatezza e disponibilità dei dati sensibili della SIM condivisi con il fornitore delle schede SIM dovranno essere protetti in ogni fase del loro ciclo di vita.	19.1