Indice

1. Introduzione e ambito di applicazione

1.1 Nel presente documento viene presentato l'insieme dei requisiti di sicurezza di base di BT relativi all'ambito dei lavori intrapresi da un fornitore. Tali requisiti vengono classificati secondo 3 livelli.

I requisiti del 1º livello, di cui alla sezione 2, fanno riferimento ai fornitori che eseguiranno i lavori essendo in possesso di informazioni BT limitate e di un accesso limitato ai sistemi amministrativi e alle reti di BT. I fornitori che rientrano in questa categoria non saranno tenuti a conformarsi agli altri requisiti disposti nel presente documento.

Le sezioni 3-6 del 2º livello sono obbligatorie per tutte le altre tipologie di lavori.

Per quanto riguarda il 3º livello, a seconda dell'ambito dei lavori potrebbero essere applicabili uno o più requisiti contenuti nelle sezioni 7-18. In caso di dubbio, rivolgersi al proprio rappresentante dell'approvvigionamento BT.

Alcuni requisiti potrebbero rinviare ad uno degli allegati elencati di seguito in quanto contenenti ulteriori informazioni utili. :

Allegato 1 Classificazione delle informazioni
Allegato 2 Formazione obbligatoria
Allegato 3 Trasmissione di richieste di chiarimenti/problemi ad un referente di BT Security
Allegato 4 Accesso a siti ed edifici BT da parte di organizzazioni non BT – Solo Regno Unito
Allegato 5 Requisiti di sicurezza per servizi di hosting esterni

1.2 I presenti requisiti di sicurezza non alterano in alcun modo gli altri obblighi del fornitore disposti nel contratto (inclusi, senza intento limitativo, i suo obblighi di cui alle condizioni intitolate “Riservatezza”, “Tutela dei dati personali” e controlli pre-impiego (PECs, Pre-employment Checks)), ma ne costituiscono una integrazione.

2. Sicurezza delle informazioni in caso di accesso limitato

L'osservanza della sezione 2 costituisce l'unico requisito applicabile nel caso in cui il fornitore esegua lavori che comportino un accesso limitato alle informazioni BT e possano comportare un accesso limitato ai sistemi amministrativi di BT, ad esempio alle reti iSupplier e BT (rientrano in questa tipologia di lavori, senza intento limitativo, cancelleria, gestione degli impianti degli edifici, sopralluoghi, programmi di voucher e prodotti con sconto dipendenti, provider di contenuti televisivi per BT e titolari di diritti).

Fatti salvi gli obblighi di riservatezza a cui possa essere soggetto, laddove il fornitore o personale temporaneo accedano alle informazioni di BT o dei clienti di BT (inclusi i dati personali) correlate a BT o ai clienti di BT, il fornitore dovrà:
(a) fare in modo che tali informazioni (inclusi i dati personali) non vengano divulgate né consultate da personale temporaneo non impiegato direttamente nei lavori BT;
(b) mantenere (e provvedere affinché tutto il personale temporaneo interessato mantenga) tali informazioni (inclusi i dati personali) in condizioni di sicurezza e riservatezza (ad esempio, senza intento limitativo, mettendo in atto i sistemi e le procedure necessari per salvaguardare la sicurezza di tutte le informazioni appartenenti a, o sotto il controllo di, BT nella misura in cui siano in possesso o sotto il controllo del fornitore in conformità alle migliori prassi di settore e implementare tali sistemi e processi in modo rigoroso).

Le sezioni dalla 3 alla 6 incluse sono applicabili a tutti gli impegni dei fornitori nei confronti di BT (con l'eccezione dei fornitori che effettuano unicamente forniture con accesso limitato).

3. Sicurezza delle informazioni generali

3.1 Il fornitore avrà cura di trasmettere prontamente a BT gli estremi del proprio referente per la sicurezza ed ogni eventuale variazione degli stessi.

3.2 All'inizio del contratto, il fornitore provvederà a comunicare per iscritto al referente di BT Security, a mezzo dell'allegato 3, le aree geografiche in cui vengono erogati i servizi principali, viene assegnato il personale temporaneo interessato o vengono trattate o archiviate le informazioni BT. Durante il contratto, il fornitore dovrà inoltre comunicare ogni proposta di modifica dell'area geografica al referente di BT Security a mezzo dell'allegato 3, affinché BT possa valutare nuovamente gli eventuali rischi a carico delle informazioni di BT o dei clienti di BT.

3.3 Il fornitore provvederà affinché tutti i contratti con i subappaltatori interessati includano clausole scritte che impongano il rispetto, da parte dei subappaltatori stessi, dei requisiti di sicurezza per i fornitori di BT, nella misura in cui risultino applicabili. Queste condizioni devono essere stipulate tra il fornitore e il suo subappaltatore prima che quest'ultimo o un suo addetto possano accedere ai sistemi BT e alle informazioni BT.

3.4 Il fornitore non potrà avvalersi delle informazioni BT per finalità diverse da quelle per cui tali informazioni gli sono state trasmesse da BT e unicamente nella misura necessarie per consentirgli di dare esecuzione al contratto. Il fornitore avrà l'obbligo di trattare o utilizzare le informazioni BT secondo modalità coerenti con i requisiti contenuti nell'allegato 1 dei presenti requisiti di sicurezza, nonché in conformità alla legislazione vigente in materia.

3.5 Il fornitore avrà cura di informare il referente di BT Security a mezzo dell'allegato 3, qualora si trovi ad essere soggetto a procedure di fusione, acquisizione o cambiamento di proprietà, affinché ci sia possibile valutare nuovamente gli eventuali rischi a carico di BT, delle informazioni BT o delle informazioni dei clienti di BT.

3.6 Con cadenza almeno annuale e ogni volta che sopraggiungano variazioni alle forniture o alla modalità con cui vengono fornite, il fornitore dovrà riesaminare i presenti requisiti di sicurezza al fine di accertarne la conformità a tutti i requisiti di sicurezza applicabili.

3.7 Il fornitore dovrà gestire in condizioni di sicurezza tutti i Beni materiali BT e/o gli articoli BT assegnatigli dalla stessa BT.

- Quando inutilizzati, i beni materiali BT e gli Articoli BT dovranno essere immagazzinati in condizioni di sicurezza. Tali materiali includono, senza intento limitativo, token di accesso remoto, computer portatili BT, apparecchiature di rete, server e documentazione.

- I beni materiali BT non potranno essere allontanati dal luogo di lavoro senza previa autorizzazione.

3.8 In relazione all'approvvigionamento delle forniture, il fornitore dovrà attuare procedure formali di gestione degli incidenti riguardanti la sicurezza con responsabilità definite e trattamento “riservato” di tutte le informazioni relative a tali incidenti. Il fornitore provvederà ad informare il referente di BT Security a mezzo dell'allegato 3, entro un ragionevole lasso di tempo da quando giunga a conoscenza di un qualsiasi incidente:

i) che comporti perdite materiali, corruzione, danneggiamento o uso improprio di informazioni BT, Beni materiali BT, articoli BT oppure un accesso improprio o non autorizzato ai sistemi BT e alle informazioni BT, oppure una violazione degli obblighi del fornitore ai sensi dei presenti requisiti di sicurezza;
ii) che abbia come conseguenza l'incapacità di effettuare le forniture in conformità al contratto;
iii) causato da azioni che violano i requisiti del presente documento sulla sicurezza.

Dietro ragionevole richiesta, il fornitore trasmetterà sollecitamente a BT una relazione scritta contenente un piano di ripristino che includa un calendario e le misure da porre in atto al fine di evitare il reiterarsi dell'incidente.

3.9 Il fornitore dovrà garantire un pronto intervento a fronte di ogni rischio identificato a carico della riservatezza, integrità o disponibilità delle informazioni BT o dei processi o sistemi del fornitore.

3.10 BT avrà facoltà di condurre valutazioni dei rischi relativamente a qualsiasi aspetto pertinente del servizio (ad esempio i subappaltatori coinvolti nel servizio) allo scopo di identificare ulteriori rischi a carico di BT per effetto dell'approvvigionamento delle forniture, a seconda dei casi. BT potrà quindi precisare le opportune contromisure aggiuntive atte a contrastare tali rischi. Gli eventuali costi associati all'attuazione delle contromisure saranno oggetto di accordo tra le parti.

3.11 Il fornitore dovrà dotarsi di processi e politiche sulla sicurezza e mantenere una documentazione (di cui copie da mettere a disposizione in lingua inglese) che attestino la conformità ai presenti requisiti di sicurezza, mettendo inoltre a disposizione di BT l'accesso alle prove in ottemperanza alla sezione 7.

3.12 Il fornitore disporrà affinché siano in atto procedure e controlli atti a proteggere il trasferimento di informazioni BT tramite l'impiego di servizi di comunicazione e-mail, voce, fax e video (accertandosi ad esempio che durante le riunioni in videoconferenza tutti i partecipanti siano autorizzati a discutere di informazioni BT). Per ulteriori informazioni sul trattamento delle informazioni BT si veda l'allegato 1.

3.13 Il fornitore avrà l'obbligo di implementare procedure atte a contrastare le minacce alla sicurezza dirette o mirate a BT o contro un soggetto terzo operante al servizio di BT al fine di tutelare adeguatamente le informazioni BT.

3.14 Il fornitore provvederà affinché le attività lavorative remote e a domicilio aventi attinenza con informazioni BT e sistemi BT siano soggette a regolari controlli sulla sicurezza nell'ambito dell'organizzazione del fornitore stesso, quali, a titolo di esempio e senza intento limitativo, l'autenticazione avanzata da applicare all'accesso remoto da parte degli utenti.

3.15 Alla risoluzione o scadenza del contratto, il fornitore provvederà, e farà in modo che il personale temporaneo e i subappaltatori provvedano, a distruggere in sicurezza e in conformità all'allegato 1 dei presenti requisiti di sicurezza, tutte le informazioni BT possedute o controllate dal fornitore o dai suoi subappaltatori, salvo diversamente specificato da BT, o imposto in forza di un obbligo legislativo o regolamentare. Le informazioni archiviate devono essere poste al di fuori della possibilità di accesso nel corso delle attività aziendali correnti.

3.16 Il fornitore dovrà conservare le informazioni BT per tutto il tempo necessario a svolgere il servizio, ma non oltre un massimo di due anni, tranne che un diverso periodo di conservazione sia stato specificato da BT o sia imposto in osservanza di requisiti legislativi o regolamentari.

3.17 Il fornitore dovrà garantire la disponibilità, qualità, integrità e capacità adeguata di offrire la prestazioni di sistema richieste o le forniture con una disponibilità senza interruzioni, assicurando che:

- sia in atto un piano di backup;
- i dati di sistema critici siano protetti (se del caso);
- venga applicata una soluzione alternativa, se ciò costituisce un requisito concordato;
- il sistema o servizio possa essere ripristinato dopo un guasto o un incidente di grave entità;
- il piano venga messo in pratica almeno con cadenza annuale;
- le copie di backup delle informazioni e del software, a seconda dei casi, vengano effettuate e testate regolarmente in conformità ad una politica di backup concordata allo scopo di garantire il ripristino dei dati senza alterazioni.

4. Sicurezza del personale temporaneo

4.1 Il personale temporaneo interessato riceverà l'autorizzazione di Accesso unicamente previo completamento della formazione alla sicurezza di BT oggetto dell'allegato 2 dei presenti requisiti di sicurezza. Il corso BT sulla sicurezza delle informazioni potrà essere sostituito da una formazione equivalente organizzata dai fornitori sullo stesso tema, salvo approvazione da parte di BT Security. In seguito, la formazione obbligatoria dovrà essere oggetto di mantenimento come indicato dettagliatamente in allegato 2. Il fornitore avrà l'obbligo di conservare i registri della formazione, i quali saranno messi a disposizione per le verifiche condotte da BT.

4.2 Il fornitore provvederà affinché tutto il personale temporaneo firmi l'accordo di riservatezza del fornitore stesso prima di avviare i lavori negli edifici di BT o sui sistemi BT o

di accedere alle informazioni BT. Questi accordi di riservatezza devono essere conservati dal fornitore e messi a disposizione per le verifiche di BT nell'ambito delle procedure di audit.

4.3 Il fornitore si impegna ad intervenire in caso di violazioni alle politiche e procedure di sicurezza attraverso processi formali quali, se opportuno, azioni disciplinari.

4.4 Il fornitore dovrà attivare un servizio riservato di linea telefonica diretta, disponibile al suo intero personale, nella misura consentita dalla legge, che dovrà essere utilizzato dal personale temporaneo qualora riceva istruzioni di agire in modo incongruo rispetto ai presenti requisiti di sicurezza e in violazione degli stessi. Le relative relazioni dovranno essere trasmesse al referente di BT Security a mezzo dell'allegato 3.

4.5 Quando le forniture cessino di essere assegnate al personale temporaneo, il fornitore provvederà affinché l'accesso alle informazioni BT venga revocato e ogni bene, articolo o informazione di BT in possesso del personale temporaneo venga restituito al team operativo BT competente o distrutto ai sensi dell'allegato 1 dei presenti requisiti di sicurezza. Laddove possibile, il fornitore attiverà una procedura di uscita controllata che includa una richiesta scritta al responsabile operativo di BT per la rimozione degli accessi e dell'identità. Il personale temporaneo dovrà essere informato che l'accordo di riservatezza sottoscritto resta in vigore e che le informazioni BT acquisite tramite il lavoro sulle forniture non devono essere divulgate.

4.6 Nell'ambito della concessione dell'accesso, il fornitore dovrà conservare ed esibire i registri di tutto il personale temporaneo che necessita di accesso o che sta effettuando forniture BT, indicando nominativo, ubicazione dei lavori, indirizzo e-mail professionale e numero di telefono aziendale diretto e interno (se necessario) e/o numero di telefono cellulare, data di richiesta del numero di identificazione utente (UIN, User Id Number) (se posseduto), data di assegnazione del progetto BT, data di completamento della formazione obbligatoria, data in cui hanno lasciato il progetto BT e una dichiarazione di controllo preliminare all'assunzione. Il referente per la sicurezza del fornitore dovrà accertarsi in permanenza che l'autorizzazione venga rilasciata unicamente al personale temporaneo interessato.

5. Verifiche e revisioni della sicurezza

5.1 Il fornitore, in relazione alle forniture e fermo restando il rispetto della riservatezza delle informazioni riguardanti i suoi altri clienti, dovrà consentire (e fare in modo che tutto il personale temporaneo consenta), dietro ragionevole richiesta, a BT o ai suoi rappresentanti autorizzati, l'accesso alle strutture, ai sistemi e ai registri del fornitore e dei subappaltatori interessati, contenenti informazioni BT e dei clienti di BT (inclusi i dati personali) nei modi ragionevolmente necessari per accertare la conformità del fornitore ai presenti requisiti di sicurezza.

Ciò potrebbe includere una valutazione di tutti gli elementi dei controlli fisici e logici nonché la validazione dei sistemi del fornitore in cui sono contenute informazioni BT. Il fornitore dovrà facilitare tali accertamenti consentendo a BT di raccogliere, conservare e analizzare le informazioni riguardanti l'approvvigionamento delle forniture, se del caso, al fine di

individuare eventuali rischi per la sicurezza, oltre ad assecondare le ragionevoli richieste di BT di invio di relazioni e di partecipazione a riunioni.

Su richiesta di BT, il fornitore parteciperà ad un controllo di integrità on-line da remoto volto ad accertare la conformità di base alle clausole dei presenti requisiti di sicurezza.

6. Accertamenti

6.1 Qualora BT abbia motivo di sospettare che si sia verificata una violazione, da parte del fornitore di un subappaltatore, delle disposizioni dei presenti requisiti di sicurezza, tale da ripercuotersi sui sistemi BT e/o sulle informazioni BT, BT ne darà informazione al referente per la sicurezza del fornitore. Il fornitore si impegna a collaborare senza riserve con BT in ogni eventuale accertamento che ne consegua condotto da BT e/o dalle autorità preposte all'applicazione della legge, autorizzando ad esempio l'accesso alle informazioni BT presenti presso le strutture del fornitore, previo ragionevole preavviso.

Nel corso degli accertamenti, il fornitore avrà l'obbligo di collaborare con BT, fornendo l'opportuna assistenza e le strutture necessarie per l'indagine della violazione. BT avrà facoltà di richiedere che il fornitore isoli a scopo di valutazione eventuali beni materiali o immateriali appartenenti al fornitore per favorire gli accertamenti. Il fornitore non potrà in tal caso opporsi alla richiesta o prorogarne i tempi di risposta senza un ragionevole motivo.

Relativamente alle clausole delle sezioni 7 -18, la descrizione di ciascuna sezione specifica il tipo di fornitura a cui si applicano le clausole stesse.

7. Politica e requisiti generici di sicurezza

L'osservanza delle clausole contenute nella sezione 7 ha carattere vincolante se il fornitore ha accesso a "informazioni sensibili" (come da definizione), oppure svolge funzioni di sviluppo, installazione, manutenzione e supporto di reti o fornisce servizi professionali di IT.

7.1 Il fornitore dovrà essere in possesso di certificazione ISO27001 o conformarsi ai requisiti di sicurezza della certificazione ISO27001 o di politiche di sicurezza allineate alla ISO27001 e/o avere avviato la procedura di ottenimento della certificazione ISO27001 entro un lasso di tempo concordato con BT.

7.2 Se previsto, BT potrà periodicamente aggiornare politiche, linee guida e requisiti correlati alla sicurezza e altre disposizioni obbligatorie. BT integrerà gli aggiornamenti in questione nell'ambito di una versione riveduta dei presenti requisiti di sicurezza mediante una richiesta di modifica contrattuale notificata per iscritto al fornitore da BT. Gli eventuali costi associati all'introduzione dei nuovi requisiti di sicurezza saranno oggetto di accordo tra le parti.

7.3 Il fornitore metterà a disposizione di BT copie delle Certificazioni di sicurezza e una dichiarazione di applicabilità relativa ai servizi erogati a sostegno delle prove di messa in conformità rispetto a questo piano

8. Sicurezza fisica - Strutture di BT

L'osservanza delle clausole contenute nella sezione 8 ha carattere vincolante se il fornitore effettua forniture presso le Strutture di BT.

8.1 Tutti i membri del personale temporaneo impegnato presso le strutture di BT dovranno essere in possesso di una tessera che li identifichi come “fornitore autorizzato” o altro documento analogo fornito da BT. Questa tessera dovrà essere utilizzata permanentemente da ciascun membro del personale temporaneo come strumento di verifica dell'identità presso le strutture di BT e dovrà includere una immagine fotografica chiaramente visibile e fedelmente rappresentativa del suo portatore. Il personale temporaneo potrà essere ugualmente dotato di una scheda di accesso elettronico e/o di una tessera per visitatori a durata limitata, che dovranno essere utilizzate nel rispetto delle istruzioni vigenti localmente.

8.2 Solo server conformi agli standard BT, PC Webtop BT e dispositivi terminali altamente affidabili potranno essere connessi direttamente (mediante inserimento di cavo nella porta LAN o connessione wireless) ai domini BT. Il fornitore non potrà (e, quando opportuno, disporrà affinché il personale temporaneo non possa) collegare un’apparecchiatura non approvata da BT a un qualsiasi dominio BT senza l'autorizzazione preliminare del referente di BT Security (a mezzo dell'allegato 3). Il referente di BT Security fornirà l'autorizzazione scritta contestualmente all'avvio del processo di concessione della politica di sicurezza interna di BT da parte del referente BT del fornitore.

8.3 Nessuna informazione BT potrà essere rimossa dalle strutture BT e nessuna apparecchiatura o nessun software potranno essere rimossi o installati presso le strutture BT senza l'autorizzazione preliminare di BT.

8.4 Le linee guida in materia di protezione fisica e di lavori all'interno delle Strutture di BT dovranno essere rigorosamente rispettate, ad esempio predisponendo un accompagnamento in caso di attraversamento delle zone protette. Ogni ulteriore ordine o istruzione impartito da BT ad un rappresentante del fornitore si intenderà trasmesso direttamente al fornitore.

8.5 Laddove il fornitore sia autorizzato a concedere al personale temporaneo un accesso non accompagnato alle aree interne alla proprietà di BT, il firmatario autorizzato non BT e il personale temporaneo dovranno aderire a tutte le raccomandazioni impartite da BT. Inoltre, il firmatario autorizzato BT e il personale temporaneo dovranno essere sottoposti a controlli pre-impiego di livello minimo L2.

9. Sicurezza fisica - Strutture del fornitore

L'osservanza delle clausole contenute nella sezione 9 ha natura vincolante se il fornitore effettua le forniture da strutture non BT e include l'insieme di personale temporaneo, subappaltatori e dipendenti, subappaltatori e agenti del fornitore.

9.1 L'accesso alle strutture non BT (siti, edifici o aree interne) in cui vengono effettuate le forniture o in cui vengono archiviate o trattate le informazioni BT dovrà avvenire mediante una tessera di identificazione fornita da un fornitore autorizzato. Questa tessera dovrà essere utilizzata permanentemente da ciascun individuo come strumento di verifica dell'identità presso le strutture in questione e dovrà includere una immagine fotografica chiaramente visibile e fedelmente rappresentativa del suo portatore. I singoli individui potranno essere provvisti di una tessera di accesso elettronico autorizzato al solo scopo di accedere alle strutture di interesse o, in alternativa, di un accesso di sicurezza tramite tastiera con procedure di controllo delle autorizzazioni e della distribuzione e di modifica dei codici *ad hoc* o periodica.

9.2 Il fornitore provvederà affinché l'accesso ai siti, agli edifici o alle aree interne in cui vengono eseguite le forniture o in cui vengono archiviate o trattate le informazioni BT, venga avvenga tramite autorizzazione e aderisca ai processi e procedure di sicurezza. Tale obbligo si intende esteso ai subappaltatori con accesso fisico a queste aree (ad esempio, società di controllo ambientale, manutenzione e vigilanza).

9.3 Su richiesta dell'azienda BT o del proprietario del progetto BT, il fornitore disporrà affinché il personale temporaneo interessato venga isolato in maniera sicura dal resto del personale del fornitore.

9.4 Le zone protette all'interno delle strutture del fornitore (ad esempio le sale per comunicazioni di rete), saranno segregate e protette mediante adeguati controlli all'ingresso per fare in modo che possa accedervi unicamente il personale temporaneo autorizzato. L'accesso effettuato a queste aree da parte del personale temporaneo deve essere sottoposto a regolari verifiche e la concessione dei diritti d'accesso a queste aree deve essere rinnovata almeno con cadenza annuale.

9.5 Il fornitore dovrà fare uso di sistemi di sicurezza CCTV e relativi supporti di registrazione sia in risposta a incidenti di sicurezza come strumento di videosorveglianza o come deterrente, sia come ausilio nella possibile cattura di individui colti nell'atto di commettere un reato. Le immagini CCTV registrate (su nastro o in formato digitale) dovranno essere conservate per almeno 20 giorni. Questo periodo potrà tuttavia essere prorogato nelle situazioni seguenti:
i) laddove le prove video CCTV debbano essere conservate per accertamenti peritali o indagini penali;
ii) se previsto come requisito necessario di ottemperanza ad una legge.

Tutti i nastri utilizzati per la registrazione delle immagini riprese dalle videocamere CCTV devono essere riposti in un armadio chiuso, con la chiave conservata e controllata in condizioni di sicurezza. L'accesso all'armadio deve essere limitato unicamente al personale autorizzato.
Tutti i registratori video e video digitali CCTV devono essere ubicati in punti appartati per evitare l'accesso non autorizzato e la possibilità di visioni “casuali” dei relativi schermi CCTV.

9.6 L'area locale che circonda le strutture del fornitore utilizzate per i prodotti e/o i servizi, a seconda dei casi, dovrà essere regolarmente ispezionata dal fornitore per verificare l'assenza di rischi e minacce.

9.7 Il fornitore dovrà verificare il livello di protezione dei cavi di alimentazione e telecomunicazione che trasmettono i dati o supportano i servizi informativi o i servizi radio/satellitari utilizzati nell'approvvigionamento delle forniture al fine di evitare l'interruzione delle operazioni aziendali. Dovranno essere implementate le seguenti misure di tutela della sicurezza fisica commisurate alla criticità aziendale delle rispettive operazioni:
i) le sedi stradali, le schermature dei cavi, i passi d'uomo o le scatole da incasso a marciapiede attraversati da cavi di importanza critica per l'azienda devono essere protetti;
ii) l'accesso al vano cavi o agli armadi delle risalite cavi all'interno degli edifici operativi deve essere limitato mediante l'uso di appositi lettori di controllo elettronici o una efficace gestione delle chiavi;
iii) i collegamenti per le comunicazioni computerizzate e le relative apparecchiature poste all'interno degli impianti informatici devono essere protetti a livello fisico e ambientale;
iv) i collegamenti per comunicazioni radio e satellitari e le relative apparecchiature devono essere protetti adeguatamente.

9.8 A completamento delle misure di sicurezza elettronica e fisica presso le sedi dei fornitori si reputa necessario integrare servizi di sicurezza presidiati nelle seguenti circostanze:

- la sede ha una particolare importanza operativa;
- le informazioni BT trattate possono avere conseguenze sul marchio e sulla reputazione;
- elevato volume di informazioni BT trattate (ad esempio, esternalizzazione di processi aziendali);
- requisiti contrattuali dei clienti;
- presenza di rischi/minacce specifici del sito;
- il fornitore è in possesso di informazioni BT con un elevato livello di sensibilità.

9.9 Per tutelare le apparecchiature BT (quali, ad esempio, server o switch) installate presso le strutture dei fornitori da minacce e pericoli di natura ambientale, nonché dal rischio di accessi non autorizzati, tali apparecchiature devono essere collocate in un'area protetta e segregata dalle apparecchiature utilizzate da qualsiasi sistema di organizzazioni non BT. Il livello di segregazione deve far sì che la sicurezza delle apparecchiature BT non possa essere compromessa né deliberatamente, né accidentalmente, per effetto di un accesso accordato a organizzazioni non BT e potrebbe ad esempio, assumere la forma di pareti divisorie, armadi con chiusura a chiave o ingabbiature metalliche.

9.10 Misure di prevenzione e rilevamento dovranno essere adottate allo scopo di prevenire guasti agli impianti causati dall'interruzione di servizi essenziali o altri fattori di influenza ambientali:

- incendi;
- gas;
- nubifragi;
- interruzioni di energia.

Per consentire il rilevamento delle seguenti circostanze dovranno essere installati appositi allarmi, collegati ad una postazione presidiata in permanenza:

- incendi;
- gas;
- interruzioni di energia;
- guasto al gruppo di continuità (UPS);
- guasto al sistema di controllo di umidità e temperatura/aria condizionata.

9.11 A protezione delle zone contenenti informazioni BT e strutture di elaborazione delle informazioni dovranno essere eretti perimetri di sicurezza (barriere quali pareti, recinzioni, cancelli ad apertura mediante tessera o reception presidiata).

9.12 Per evitare l'accesso non autorizzato o aggressioni deliberate, i punti d'accesso come le zone di consegna e di carico e altri punti da cui potrebbero entrare nei locali persone non autorizzate dovranno essere controllati e se possibile isolati dalle installazioni informatiche.

9.13 Assicurarsi che l'accesso fisico alle aree da cui si accede alle informazioni BT avvenga unicamente mediante carte di prossimità o a microprocessore (o sistemi di sicurezza equivalenti) e che il fornitore conduca verifiche interne periodiche per accertare il rispetto di tali disposizioni.

9.14 Il fornitore disporrà il divieto di scattare fotografie o acquisire in altro modo immagini delle informazioni BT o delle informazioni dei clienti di BT. In circostanze eccezionali per cui possa presentarsi la necessità per motivi aziendali di acquisire tali immagini, sarà necessario ottenere dal referente di BT Security l'esenzione temporanea da questa clausola in forma scritta a mezzo dell'allegato 3.

9.15 A tutela delle informazioni BT, il fornitore dovrà mettere in atto una politica aziendale di blocco dei computer e pulizia dello spazio di lavoro per i dipendenti che lasciano la propria postazione.

10. Predisposizione di un ambiente di hosting

L'osservanza delle clausole contenute nella sezione 10 ha carattere vincolante se il fornitore predispone un ambiente di hosting destinato ad apparecchiature di BT o dei clienti di BT.

10.1 Nel caso in cui predisponga un'area ad accesso protetto alle proprie strutture per l'hosting di apparecchiature di BT o di clienti BT ("Sito del fornitore"), il fornitore dovrà:
(a) assicurarsi che tutto il personale temporaneo che accede al sito del fornitore sia in possesso di una tessera di identificazione o di una tessera elettronica di controllo dell'accesso. Questa tessera dovrà essere utilizzata permanentemente da ciascun individuo come strumento di verifica dell'identità presso il Sito del fornitore e dovrà includere una immagine fotografica chiaramente visibile e fedelmente rappresentativa del membro del personale temporaneo; e
(b) aver attivato procedure atte a contrastare le minacce alla sicurezza dirette contro le apparecchiature di BT o dei clienti di BT o contro un soggetto terzo al servizio di BT al fine di salvaguardare le informazioni di BT e dei clienti di BT presso il Sito del fornitore; e
(c) fare uso di sistemi di sicurezza CCTV e relativi supporti di registrazione presso il Sito del fornitore sia in risposta a incidenti di sicurezza come strumento di videosorveglianza e come deterrente, sia come ausilio nella possibile cattura di individui colti nell'atto di commettere un reato. Il fornitore dovrà assicurare 20 giorni di registrazione mediante CCTV in virtù di un possibile utilizzo come efficace strumento investigativo;
(d) fornire a BT una pianta dei locali con lo spazio assegnato nell'area protetta del sito del fornitore;

(e) disporre affinché gli armadi di BT e del cliente di BT presso il Sito del fornitore siano tenuti chiusi a chiave e aperti unicamente dal personale autorizzato di BT, dai rappresentanti di BT approvati e dal personale temporaneo interessato;
(f) introdurre un processo di gestione sicura delle chiavi presso il sito del fornitore;
(g) ispezionare regolarmente l'area locale circostante il sito del fornitore per verificare l'eventuale presenza di rischi e minacce; e
(h) documentare e conservare procedure operative (nella lingua del Paese da cui hanno avuto origine i lavori BT) per assolvere ai requisiti di sicurezza enunciati nel presente paragrafo 12 e, su richiesta, fornire a BT l'accesso a tale documentazione.

10.2 BT avrà l'obbligo di trasmettere le seguenti informazioni al fornitore:
(a) un registro dei beni materiali di BT o del cliente di BT presenti presso il Sito del fornitore; e
(b) estremi dei dipendenti, subappaltatori e agenti di BT che hanno necessità di accedere (continuativamente) al sito del fornitore.

11. Sviluppo delle forniture

L'osservanza delle clausole contenute nella sezione 11 ha carattere vincolante se il fornitore si occupa dello sviluppo di forniture per uso da parte di BT o dei clienti di BT (sono inclusi "componenti standard", configurazioni del software e componenti di fabbricazione relativi alle forniture).

11.1 Il fornitore avrà l'obbligo di attuare misure di sicurezza concordate in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle forniture agendo nel modo seguente:

(i) conservando l'opportuna documentazione (nella lingua del Paese da cui hanno avuto origine i lavori BT) relativamente all'attuazione delle misure di sicurezza e farà in modo che sia la documentazione che la sicurezza siano conformi alle migliori prassi del settore;
(ii) contenendo al minimo il rischio che soggetti non autorizzati (ad esempio, pirati informatici) accedano ai sistemi BT e informazioni BT, reti BT o servizi BT, e
(iii) contenendo il rischio di uso improprio dei sistemi BT e informazioni BT, reti BT o servizi BT tale da causare potenziali perdite di proventi o interruzioni di servizio.

11.2 Il fornitore sarà tenuto a dimostrare, su richiesta, che ogni versione software o hardware (sia essa speciale o standard) fornita a BT è identica a quella concordata con BT. Il fornitore si impegna a preservare l'integrità delle versioni, inclusi gli aggiornamenti, i sistemi operativi e le applicazioni, dai reparti produttivi agli uffici.

11.3 Il fornitore dovrà dimostrare che lo sviluppo di sistemi destinati all'utilizzo da parte di BT o che la realizzazione e la manutenzione dell'hardware di proprietà di BT sono soggetti a protezione avanzata in linea con i requisiti di sicurezza di BT, se forniti dal team operativo di BT, oppure con le migliori prassi del settore.

11.4 Il fornitore farà in modo che gli ambienti di sviluppo e prova non contengano dati reali e siano segregati rispetto all'ambiente reale. I dati di prova forniti da BT dovranno essere eliminati al termine di un periodo stabilito dal proprietario dei dati BT.

11.5 Il fornitore garantisce che è stato compiuto ogni ragionevole sforzo al fine di assicurare che il software e/o l'hardware (unitamente alla documentazione consegnata in formato elettronico) non contengono il seguente software dannoso (elenco non esaustivo), in qualsiasi forma disponibile:

(i) "possesso elettronico" e "bombe logiche";
(ii) "virus" e "worm" eventualmente rilevati utilizzando il più recente (alla data di invio) software anti-virus disponibile sul mercato; e
(iii) "spyware", "adware" e altre forme di malware

(secondo il significato con cui tali espressioni vengono generalmente intese nell'industria informatica); al momento dell'accettazione e successivamente a questa, il fornitore garantisce che il software e/o l'hardware funzioneranno in conformità alle specifiche funzionali per l'intero periodo di garanzia, inoltre, il fornitore si avvarrà unicamente di materiali, tecniche e requisiti di sicurezza di elevato livello qualitativo nel dare esecuzione al contratto e applicherà sistematicamente i requisiti di sicurezza con la cura, abilità e diligenza richiesti dalle buone prassi informatiche e dalle metodologie di codifica sicure.

11.6 Il fornitore si impegna a collaborare con BT al fine di assicurare la conformità ai requisiti di sicurezza nell'ambito del quadro di sicurezza appropriato a spese del fornitore; ciò

potrebbe richiedere che le forniture vengano periodicamente testate di conseguenza in materia di sicurezza.

11.7 Ogni eventuale carenza nella sicurezza delle forniture individuata da BT o dal fornitore sarà rettificata a spese del fornitore nei tempi che BT avrà opportunamente cura di richiedere.

12. Accesso alle informazioni

Applicabile se specificato nei requisiti.

12.1 Entro 14 giorni dalla richiesta scritta di BT e a discrezione di BT:
(a) le parti, facendosi carico ciascuna delle proprie spese, sottoscriveranno e consegneranno alla controparte un accordo di accesso alle informazioni nella forma dell'accordo di accesso alle informazioni contenuto in appendice 3; oppure
(b) il fornitore, a proprie spese, sottoscriverà un accordo di deposito in garanzia sostanzialmente nella forma dell'accordo contenuto in appendice 21 relativamente a tutte le informazioni e documentazione aventi attinenza alle forniture (inclusi, senza intento limitativo, il software, tutto il codice sorgente, dati di collegamento, elenchi software, dati tecnici completi, note dei programmatori, il complesso delle informazioni e della documentazione correlate al software necessarie per aggiornare, modificare e correggere il software, nonché fornire ogni livello di supporto per il software) (di seguito, le "informazioni sul deposito di garanzia") e depositerà in garanzia presso NCC Escrow International Limited (di seguito, "agente depositario") una copia aggiornata delle informazioni sul deposito di garanzia. Il fornitore si adopererà affinché tali informazioni sul deposito di garanzia consentano a BT e/o a eventuali terzi competenti a nome di BT, di:

(i) adempiere agli obblighi pendenti del fornitore ai sensi del contratto, inclusi, senza intento limitativo, gli obblighi che sarebbero insorti (quali l'obbligo di evadere gli eventuali ordini che BT avrebbe potuto trasmettere in forza del contratto) qualora il contratto non fosse stato risolto da BT (salvo ai sensi del paragrafo 4 della clausola a titolo "risoluzione") prima dell'estinzione della sua durata normalmente prevista (nella quale sarà inclusa ogni eventuale proroga concessa nell'ambito della possibilità di BT di prolungare la durata iniziale); e
(ii) comprendere facilmente le informazioni sul deposito di garanzia, aggiornare (anche tramite upgrade), modificare, migliorare e correggere le informazioni sul deposito di garanzia e le forniture.

12.2 Il fornitore garantisce che le informazioni sul deposito di garanzia effettuato presso BT o presso l'agente depositario, a seconda dei casi, sono e saranno tenute opportunamente aggiornate in modo da consentire ad un programmatore o analista adeguatamente preparato di aggiornare o migliorare il software senza l'ausilio di altre persone o riferimenti. Il fornitore si impegna altresì a mantenere le informazioni sul deposito di garanzia perfettamente aggiornate per l'intera durata.

12.3 Qualora si verifichi un qualsiasi evento tale da consentire a BT o all'agente depositario, a seconda dei casi, di utilizzare e/o divulgare le informazioni sul deposito di garanzia, il fornitore sarà tenuto a fornire immediatamente a BT, per un periodo ragionevole, la consulenza, il supporto, l'assistenza, i dati, le informazioni, l'accesso al personale chiave del fornitore stesso o del suo concessore di licenza software nella misura

necessaria allo scopo di comprendere, aggiornare (anche tramite upgrade), migliorare, modificare e correggere in tutto o in parte le informazioni sul deposito di garanzia e/o il software.

12.4 Fermo restando ogni altro diritto che possa aver maturato, BT acquisirà automaticamente il diritto non esclusivo, perenne, irrevocabile e valido in tutto il mondo, di utilizzare le informazioni sul deposito di garanzia, dopo la loro divulgazione, al fine di mantenere e supportare le forniture, nonché il diritto non esclusivo, perenne, irrevocabile, valido nel mondo intero ed esente da qualsiasi pagamento, di utilizzare, copiare, aggiornare (anche tramite upgrade), modificare, adattare, migliorare e correggere le forniture e le eventuali forniture modificate, adattate, migliorate e/o corrette, nonché di concedere tali forniture a terzi (entro i limiti delle licenze concesse al fornitore), unitamente al diritto di autorizzare soggetti terzi ad agire come sopra a nome di BT.

12.5 La presente condizione sopravvivrà alla scadenza o risoluzione del contratto.

12.6 Se necessario allo scopo di garantire la conformità in materia di sicurezza, il referente per la sicurezza di rete BT (e/o i suoi addetti, nominati tra i dipendenti di BT) godranno di diritti analoghi (*mutatis mutandis*) se richiesto nell'ambito delle forniture, della familiarizzazione e della validazione (come da definizione contenuta nell'accordo di accesso alle informazioni) relativamente al materiale di base (come da definizione contenuta nell'accordo di accesso alle informazioni).

13. Accesso ai sistemi BT

L'osservanza delle clausole contenute nella sezione 13 ha carattere vincolante se il personale temporaneo del fornitore ha necessità di accedere ai sistemi BT per poter effettuare le forniture.

13.1 A propria discrezione assoluta e nella misura ritenuta opportuna, BT potrà consentire al fornitore l'accesso unicamente ai fini dell'approvvigionamento delle forniture.

13.2 In relazione all'accesso, il fornitore provvederà (e, quando opportuno, disporrà affinché il personale temporaneo provveda) a quanto segue:

a) accertarsi che gli identificativi degli utenti, le password, i PIN, i token e l'accesso per le conferenze siano destinati ai singoli membri del personale temporaneo e non siano oggetto di condivisione. I dati devono essere archiviati in modo sicuro e tenuti separati dal dispositivo utilizzato per effettuare l'accesso. Se un'altra persona giunge a conoscenza di una password, questa dovrà essere cambiata immediatamente;

b) dietro ragionevole richiesta, trasmettere a BT i rapporti richiesti in merito al personale temporaneo autorizzato ad accedere ai sistemi BT;

c) impedire il collegamento interdominio ai sistemi BT se non specificamente approvato e autorizzato dal referente di BT Security a mezzo dell'allegato 3;

d) adoperarsi nella misura del possibile per far sì che non venga introdotto alcun virus o codice dannoso (secondo l'accezione generale di tali espressioni nell'industria informatica), riducendo pertanto il rischio di danneggiamento dei sistemi BT e delle informazioni BT;

e) adoperarsi nella misura del possibile per far sì che gli archivi personali contenenti informazioni, dati o materiali multimediali privi di attinenza con le forniture non vengano memorizzati nei server BT, nei computer portatili e desktop forniti da BT, nei sistemi di archiviazione centralizzati BT o nei sistemi BT.

13.3 Nel caso in cui BT abbia concesso al fornitore un accesso ad Internet/Intranet, il fornitore stesso accederà (e farà in modo che il personale temporaneo acceda) a tali reti in modo adeguato ai fini dell'approvvigionamento delle forniture. Sarà compito del fornitore accertarsi che le seguenti istruzioni in materia di utilizzo improprio di Internet e della posta elettronica vengano trasmesse al personale temporaneo interessato con cadenza almeno annuale.

Non è consentito l'accesso a materiale che potrebbe essere ritenuto: -

a. osceno, a sfondo sessuale, sessista o politicamente offensivo;
b. un atto suscettibile di ledere la reputazione di BT o di singole persone;
c. attinente alla gestione di un'attività privata;
d. una violazione di diritti d'autore;
e. telefonia o messaggistica tramite Internet, quale Skype;
f. in grado di superare il firewall o altri meccanismi di sicurezza di BT mediante operazioni di aggiramento o tunneling;
g. tale da contribuire alla pubblicazione di siti o dichiarazioni online che potrebbero essere ragionevolmente interpretate come il punto di vista di BT;
h. inaccettabile o pericoloso e tale pertanto da dover essere bloccato agli utenti.

13.4 Il fornitore contatterà immediatamente BT qualora un membro del personale temporaneo interessato non necessiti più dei diritti di accesso ai sistemi BT o cambi ruolo per qualsiasi motivo previsto dall'accordo, consentendo così a BT di disabilitare o modificare i diritti di accesso agli stessi sistemi BT.

14. Accesso alle informazioni BT contenute nei sistemi del fornitore

L'osservanza delle clausole contenute nella sezione 14 ha carattere vincolante se le informazioni BT sono archiviate o trattate nei sistemi del fornitore.

14.1 Nel caso in cui al personale temporaneo venga consentito l'accesso ai sistemi del fornitore relativamente alla consegna di prodotti e/o servizi a BT, il fornitore dovrà:

a) assicurarsi che ciascun individuo disponga di una password e di un identificativo utente univoci (in conformità alle buone prassi standard di settore) noti unicamente al detto individuo per proprio uso esclusivo nell'ambito del processo di log-in sicuro;
b) consentire l'accesso ai sistemi di proprietà del fornitore in cui sono contenuti sistemi BT o informazioni BT o da cui è possibile accedervi unicamente nella misura strettamente necessaria al fine di consentire al personale temporaneo di assolvere alle proprie mansioni ai sensi dell'accordo;
c) stabilire procedure formali di controllo dell'assegnazione, revisione, revoca e/o cessazione dei diritti di accesso;
d) assicurarsi che l'assegnazione e l'utilizzo dei privilegi avanzati e dell'accesso a strutture e strumenti sensibili nei sistemi del fornitore siano controllati e limitati unicamente agli utenti che ne hanno necessità per scopi aziendali. L'accesso alle console dei sistemi e il loro utilizzo devono aver luogo in un ambiente sicuro commisurato ai beni abitualmente gestiti. Misure appropriate di sicurezza fisica

devono essere messe in atto al fine di scongiurare ogni rischio di accesso non autorizzato;
e) assicurarsi che l'assegnazione delle password utente ai sistemi di proprietà del fornitore in cui sono contenute o da cui si accede alle informazioni BT sia controllata mediante un processo formale di gestione verificabile;
f) condurre revisioni periodiche dei diritti di accesso degli utenti;
g) assicurarsi che l'accesso fisico alle apparecchiature informatiche da cui si accede o in cui sono archiviate le informazioni BT avvenga unicamente mediante carte di prossimità o a microprocessore (o sistemi di sicurezza equivalenti) e che il fornitore conduca verifiche interne periodiche per accertare il rispetto di tali disposizioni;
h) dimostrare che gli utenti aderiscono a buone prassi di sicurezza nella gestione delle password;
i) introdurre un sistema di gestione delle password che preveda un dispositivo sicuro ed efficace tale da garantire la qualità delle password;
j) assicurarsi che le sessioni utente vengano interrotte allo scadere di un periodo predefinito di inattività;
k) assicurarsi che vengano generati e gestiti in condizioni di sicurezza registri di controllo in cui vengano riportate le attività degli utenti e gli eventi pertinenti in materia di sicurezza. I registri dovranno essere conservati per un periodo ragionevole al fine di agevolare eventuali accertamenti, essendo esclusa ogni possibilità per il fornitore di consentire l'accesso non autorizzato ai registri di controllo o la modifica degli stessi;
l) assicurarsi che il monitoraggio dei registri di controllo e degli eventi, unitamente ai rapporti di analisi relativi a comportamenti anomali e/o a tentativi di accesso non autorizzato venga effettuato da personale del fornitore indipendente dagli utenti soggetti a monitoraggio.

14.2 Il fornitore avrà l'obbligo di introdurre sistemi in grado di rilevare e registrare ogni tentativo di danneggiamento, modifica o accesso non autorizzato alle informazioni BT contenute nei sistemi del fornitore (ad esempio, sistemi di registrazione e controllo dei processi, IDS, IPS ecc.);

14.3 introdurre controlli atti a rilevare e contrastare malware e fare in modo che vengano attuate procedure adeguate di sensibilizzazione degli utenti;

14.4 provvedere affinché, con cadenza almeno mensile, l'eventuale software non autorizzato venga identificato e rimosso dai sistemi del fornitore che contengono, trattano o accedono a informazioni BT;

14.5 verificare che l'accesso alle porte di diagnosi e gestione, nonché gli strumenti diagnostici siano controllati in maniera sicura;

14.6 assicurarsi che l'accesso agli strumenti di controllo del fornitore sia limitato al personale temporaneo interessato e che l'utilizzo degli stessi sia monitorato;

14.7 disporre affinché un team indipendente dagli sviluppatori conduca riesami dei codici e prove di penetrazione sull'intero software di produzione interna utilizzato per trattare le informazioni BT.

14.8 I server utilizzati ai fini di approvvigionamento delle forniture non dovranno essere installati su reti non affidabili (poste al di fuori del perimetro di sicurezza o del controllo amministrativo, ad esempio esposti a Internet) senza adeguati controlli di sicurezza.

14.9 Ogni modifica apportata a singoli sistemi del fornitore che contengono o trattano informazioni BT e/o che vengono utilizzati per fornire prodotti e/o servizi a BT devono essere controllati e sottoposti a procedure formali di controllo delle modifiche.

14.10 Tutti i sistemi devono avere gli orologi interni sincronizzati rispetto a una fonte attendibile.

15. Hosting delle informazioni BT da parte del fornitore

L'osservanza delle clausole contenute nella sezione 15 ha carattere vincolante se il fornitore si affida a servizi esterni di hosting per le informazioni BT classificate almeno come riservate in un ambiente di servizi cloud, oppure in un ambiente server di fornitori o subappaltatori.

15.1 In relazione alle forniture, il fornitore provvederà affinché gli ambienti in cui vengono gestite in hosting le informazioni BT siano conformi ai requisiti dell'allegato 5.

16. Sicurezza di rete

L'osservanza delle clausole contenute nella sezione 16 ha carattere vincolante se il fornitore realizza, sviluppa o supporta reti BT o infrastrutture di rete.

16.1 In relazione alle forniture, il fornitore avrà l'obbligo di attuare misure concordate di sicurezza in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle reti BT e/o delle infrastrutture 21CN. Il fornitore metterà a disposizione di BT la documentazione completa relativa all'implementazione della sicurezza di rete correlata alle forniture e si impegnerà al fine di:

(a) soddisfare ogni requisito legale e normativo;
(b) impedire al meglio delle proprie capacità che soggetti non autorizzati (ad esempio, pirati informatici) accedano a elementi di gestione della rete e ad altri elementi accessibili tramite le reti BT e/o 21CN;
(c) adoperarsi al meglio delle proprie capacità al fine di contenere il rischio di uso improprio delle reti BT e/o 21CN tale da causare perdite potenziali di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi;
(d) adoperarsi al meglio delle proprie capacità al fine di individuare le violazioni della sicurezza effettivamente perpetrate, attivando la rapida correzione degli eventuali problemi che ne conseguano, nonché l'identificazione degli individui che hanno ottenuto l'accesso e delle modalità seguite per ottenerle;
(e) ridurre al minimo il rischio di errata configurazione delle reti BT, ad esempio concedendo il numero minimo di autorizzazioni necessarie per adempiere al ruolo oggetto del contratto.

16.2 Il fornitore dovrà adottare tutte le misure ragionevoli allo scopo di mettere in sicurezza tutte le interfacce presenti nei componenti forniti, senza presupporre che questi vengano fatti funzionare in un ambiente sicuro.

16.3 Il fornitore avrà l'obbligo di comunicare al referente per la sicurezza di rete BT i nominativi, gli indirizzi (e altri dati che BT avrà facoltà di richiedere) di tutti i membri del personale temporaneo che di volta in volta sarà direttamente coinvolto nell'installazione, manutenzione e/o gestione delle forniture prima che intraprendano tali operazioni.

16.4 Relativamente alle attività di supporto svolte sul territorio del Regno Unito, il fornitore si affiderà ad un team specializzato in sicurezza composto da almeno un cittadino del Regno Unito disponibile per fungere da collegamento con il referente per la sicurezza di rete BT (o i suoi addetti) e per partecipare alle riunioni che il suddetto referente potrà richiedere periodicamente.

16.5 Il fornitore trasmetterà al referente per la sicurezza di rete BT un prospetto (opportunamente aggiornato) di tutti i componenti attivi contenuti nelle forniture con indicazione delle rispettive fonti.

16.6 Il fornitore comunicherà gli estremi dei membri del suo personale che assicurano il collegamento con il team per la gestione delle vulnerabilità (CERT) in relazione alla discussione sulle vulnerabilità individuate da BT e dal fornitore nelle forniture. Il fornitore comunicherà puntualmente a BT informazioni sulle vulnerabilità, e adempierà ai ragionevoli obblighi ad esso notificati di volta in volta dal referente per la sicurezza di rete BT, a proprie spese. Il fornitore informerà BT in ordine alle vulnerabilità con sufficiente anticipo, in modo da consentire l'introduzione di controlli di mitigazione prima che il fornitore stesso divulghi pubblicamente le vulnerabilità.

16.7 Il fornitore dovrà concedere al referente per la sicurezza di rete BT e a chi da esso di volta in volta designato un accesso completo e incondizionato alle strutture in cui le forniture vengono sviluppate, prodotte o fabbricate perché vi possano condurre test e/o valutazioni di conformità alla sicurezza. Il fornitore sarà peraltro tenuto a collaborare (e disporrà affinché l'intero personale temporaneo interessato faccia altrettanto) in tali verifiche della conformità.

16.8 Il fornitore dovrà accertarsi che tutti i componenti riguardanti la sicurezza contenuti nelle forniture, così come di volta in volta identificati da, o comunicati a BT, vengano valutati esternamente a spese del fornitore e con la ragionevole soddisfazione di BT.

16.9 In relazione alle informazioni trasmesse o ottenute da BT e accompagnate dalla dicitura “STRETTAMENTE RISERVATO” o la cui natura riservata sia facilmente riconoscibile, il fornitore dovrà provvedere affinché:

(a) l'accesso ad esse venga consentito unicamente al personale temporaneo appositamente autorizzato da BT per la visione e il trattamento e venga conservato un registro di tali accessi;
(b) esse vengano trattate, utilizzate e archiviate con estrema cura e criptate prima dell'archiviazione mediante PGP o WinZip 9 e in condizioni che assicurino un elevato grado di resistenza alla compromissione accidentale (ossia, adottando il più efficace

algoritmo di crittografia disponibile o utilizzando una valida password) e che rendano rilevabile con grande probabilità l'azione o il tentativo di compromissione;
(c) una volta trasmesse, esse vengano sottoposte a misure di sicurezza adeguate mediante crittografia con Secure Email, PGP o WinZip 9; e
(d) non vengano, salvo autorizzazione scritta di BT, esportate al di fuori dello spazio economico europeo.

16.10 Il fornitore dovrà comunicare sollecitamente, e in ogni caso entro il termine di 7 giorni lavorativi, al referente per la sicurezza di rete BT i dettagli completi delle caratteristiche e funzionalità proprie delle forniture (o che sono pianificate nella tabella di marcia per le forniture) progettate per, o che potrebbero essere progettate per, l'intercettazione legale o altre forme di intercettazione del traffico delle telecomunicazioni che di volta in volta:

(a) il fornitore conosce; o che
(b) il referente per la sicurezza di rete BT ritiene ragionevolmente di conoscere e ne dà pertanto comunicazione al fornitore. Tali dettagli dovranno includere tutte le informazioni ritenute ragionevolmente necessarie per consentire al referente per la sicurezza di rete BT di comprendere appieno la natura, composizione e portata di tali caratteristiche e/o funzionalità.

16.11 Allo scopo di mantenere abilitato l'accesso ai sistemi e/o alle reti BT, il fornitore dovrà comunicare immediatamente a BT ogni eventuale modifica apportata al proprio metodo di accesso tramite i firewall, fornendo ad esempio la traduzione degli indirizzi di rete.

16.12 Non è consentito l'utilizzo di strumenti di monitoraggio in grado di visualizzare informazioni relative alle applicazioni.

16.13 La funzionalità IPv6 inclusa nei sistemi operativi deve essere disabilitata sugli host (dispositivi degli utenti finali, server) collegati ai domini di rete BT e quando non necessaria.

16.14 Il fornitore è tenuto a rispettare, e disporrà affinché le forniture rispettino, le politiche BT eventualmente vigenti e i requisiti di sicurezza. Ogni inosservanza dovrà essere concordata all'atto della firma del contratto o in sede di controllo delle modifiche.

16.15 Il fornitore provvederà affinché il personale temporaneo venga sottoposto a controlli pre-impiego adeguati rispetto al livello di accesso
http://www.selling2bt.bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf

I fornitori che si occupano di realizzazione, sviluppo o supporto delle reti BT o delle Infrastrutture di rete dovranno accertarsi che tutti i membri del personale temporaneo vengano sottoposti a controlli pre-impiego di livello minimo L2. Per alcuni ruoli appositamente individuati dal referente per la sicurezza di rete BT sono previsti controlli pre-impiego di livello L3. Laddove il fornitore sia impossibilitato a selezionare direttamente personale temporaneo con nulla osta di sicurezza nell'ambito dei controlli L3, potrà richiedere a proprie spese l'assistenza di BT.

17. Sicurezza di rete del fornitore

L'osservanza delle clausole contenute nella sezione 17 ha carattere vincolante se la rete del fornitore verrà utilizzata ai fini dell'approvvigionamento delle forniture (sono incluse reti LAN, WAN, Internet, wireless e radio).

17.1 In relazione alle forniture, il fornitore avrà l'obbligo di attuare misure concordate di sicurezza in tutte le reti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle informazioni BT. Le misure dovranno:

(a) soddisfare ogni requisito legale e normativo;
(b) impedire nella misura del possibile che soggetti non autorizzati (ad esempio, pirati informatici) accedano alla rete;
(c) contenere nella misura del possibile il rischio di uso improprio delle reti tale da causare potenziali perdite di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi;
(d) individuare nella misura del possibile ogni violazione della sicurezza effettivamente perpetrata, attivando la rapida correzione degli eventuali problemi che ne conseguano, nonché l'identificazione degli individui che hanno ottenuto l'accesso e delle modalità seguite per ottenerle.

18. Sicurezza del cloud

L'osservanza delle clausole contenute nella sezione 18 ha carattere vincolante quando il fornitore presta a BT servizi correlati al cloud. Per una definizione di cloud si veda la pubblicazione NIST all'indirizzo http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf)

18.1 Il fornitore dovrà dimostrare con prove adeguate che i servizi cloud forniti soddisfano i requisiti di controllo CCM (Cloud Controls Matrix) dell'ente Cloud Security Alliance nella versione pubblicata più recente disponibile alla pagina https://cloudsecurityalliance.org , oltre a garantire la conformità all'allegato 5 dei presenti requisiti di sicurezza.

18.2 Le informazioni BT utilizzate nel commercio elettronico e circolanti nelle reti pubbliche dovranno essere protette in conformità all'allegato 1 sia in transito che a riposo (incluse le copie di backup) contro attività fraudolente e ogni tentativo non autorizzato di divulgazione, accesso e modifica.

18.3 Gli accordi sui livelli di servizio relativi a reti e infrastrutture (siano essi gestiti internamente o esternalizzati) dovranno documentare con chiarezza controlli, capacità e livelli di servizio in materia di sicurezza, oltre ai requisiti di business o del cliente.

18.4 Il fornitore dovrà consentire l'effettuazione di prove di penetrazione e/o l'accesso ai verbali delle prove di penetrazione già effettuate dal fornitore riguardanti le forniture effettuate. L'ambito di applicazione e i tempi delle prove saranno oggetto di accordo con BT.

18.5 Il fornitore avrà l'obbligo di attuare misure di sicurezza concordate in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e

integrità delle forniture contenendo al minimo il rischio che soggetti non autorizzati (ad esempio, altri clienti sul cloud) accedano ad informazioni BT e a servizi BT.

Glossario

Nei presenti requisiti di sicurezza trovano applicazione le definizioni riportate in appresso. In caso contrario, i termini del contratto si applicheranno ai presenti requisiti di sicurezza e tutte le parole ed espressioni ivi utilizzate avranno lo stesso significato loro assegnato nel contratto.

["**Accesso**": elaborazione, trattamento o archiviazione di informazioni BT mediante uno o più dei seguenti metodi:

- interconnessione con i sistemi BT;
- formato cartaceo o non elettronico;
- informazioni BT contenute nei sistemi del fornitore;
- supporti mobili;

e/o accesso agli edifici BT per l'erogazione di servizi (esclusa la consegna di componenti hardware e la partecipazione a riunioni).

[**Autorizzato**": BT ha approvato l'accesso nell'ambito del processo di interconnessione con i sistemi di BT o di un'autorizzazione scritta ricevuta dall'azienda BT o dal proprietario del progetto BT; il termine "**autorizzazione**" sarà interpretato di conseguenza. Il livello di accesso accordato sarà correlato e limitato a quanto necessario per l'approvvigionamento delle forniture.]

"**Articoli BT**": tutti gli articoli forniti da BT al fornitore e tutti gli articoli detenuti dal fornitore ma appartenenti a BT (ad es. chiavi di armadi, computer portatili, token, tessere di accesso, progetti, documenti di processo).

"**Referente per la sicurezza di rete BT**": addetto alla sicurezza delle informazioni di BT Security, contattato mediante compilazione e trasmissione dell'apposito modulo di richiesta contenuto in allegato 3, o altra persona la cui identità e i cui estremi di contatto possono essere di volta in volta notificati al referente commerciale del fornitore.

"**Beni materiali di BT**": tutti i beni materiali detenuti dal fornitore ma appartenenti a BT (ad es. router, switch, server o documentazione).

"**BT Security**": l'organizzazione di sicurezza operante in seno a BT.

"**Referente di BT Security**": addetto alla sicurezza delle informazioni di BT Security, contattato mediante compilazione e trasmissione dell'apposito modulo di richiesta contenuto in allegato 3.

"**Politica di BT Security**": politica vigente in materia di sicurezza di rete di BT fornita da BT.

"**Sistemi BT**": i servizi e componenti di servizi, prodotti, reti, server, processi, sistemi cartacei o sistemi informatici (parzialmente o integralmente) posseduti e/o gestiti da o per conto di BT, BT Group plc o qualsiasi entità di BT Group plc; oppure altri sistemi che potrebbero essere gestiti in hosting presso le strutture di BT (incluso iSupplier (secondo la definizione di "iSupplier" contenuta nella sezione dell'accordo intitolata "Pagamento e fatturazione") utilizzati nel contesto dell'"Accesso" (come sopra definito).

"**CCTV**": televisione a circuito chiuso.

"**Data di inizio**": ved. definizione nel contratto.

"**personale temporaneo**" "**personale temporaneo interessato"**: ved. definizioni nel contratto.

"**Informazioni**": informazioni disponibili in forma tangibile o in altro modo, inclusi, senza intento limitativo, specifiche, relazioni, dati, appunti, documentazione, disegni, software, politiche, procedure, processi, normative, elaborazioni computerizzate, progetti, schemi circuitali, modelli, schemi, campioni, invenzioni (brevettabili o meno) e know-how, unitamente ai supporti (se del caso) con i quali tali informazioni vengono fornite.
"**ISO 27001**": normativa internazionale sui sistemi di gestione della sicurezza pubblicata dalla Organizzazione internazionale per la standardizzazione (ISO) e dalla Commissione elettrotecnica internazionale (CEI).
"**Ordine**": ordine di forniture trasmesso da BT al fornitore ai sensi del contratto.
"**Sicurezza di rete**": sicurezza dei percorsi e nodi di comunicazione in interconnessione che collegano logicamente le tecnologie degli utenti finali le une alle altre e ai relativi sistemi di gestione.
"**Dati personali**": si intende con tale espressione il significato ad essa ascritto dalla Direttiva 95/46/CE o legislazione successiva promulgata in materia (la "Direttiva").
"Trattare", "Trattato" o "Trattamento": qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate alle informazioni BT, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione, la restituzione o la distruzione.
"**Informazioni sensibili**": informazioni BT classificate o contrassegnate almeno come "riservate", inclusi i dati personali.
"**Subappaltatore**": ved. definizione nel contratto.
"**Sistemi del fornitore**": qualsiasi computer, applicazione o sistema di rete di proprietà del fornitore utilizzato per accedere a, archiviare o trattare informazioni BT o coinvolti nell'approvvigionamento delle forniture.
"**Referente per la sicurezza del fornitore**": questa persona i cui estremi di contatto verranno comunicati di volta in volta dal fornitore a BT, sarà il referente unico per ogni questione attinente alla sicurezza.
"**Forniture**": insieme di componenti, materiali, impianti, strumenti, apparati di prova, documentazione, firmware, software, ricambi, parti e oggetti che dovranno essere forniti a BT in virtù del contratto, unitamente a tutte le informazioni e ai lavori che il contratto prevede vengano forniti a, o eseguiti per BT.
"**Trasferimento" o "Trasferito**": con tali espressioni si intende
(a) lo spostamento delle informazioni BT in possesso del personale temporaneo (inclusi, senza intento limitativo, i dati personali) da un luogo o individuo a un altro, tramite sistema fisico, vocale o elettronico; e
(b) la concessione dell'accesso alle informazioni BT in possesso del personale temporaneo (inclusi, senza intento limitativo, i dati personali) da parte di un luogo o individuo a un altro, tramite sistema fisico, vocale o elettronico.