Allegato [XX] – Requisiti di sicurezza per i fornitori di BT

Indice

SEZIONE 1: INTRODUZIONE 2
1 Introduzione 2
SEZIONE 2: REQUISITI IN CASO DI ACCESSO LIMITATO 2
2 Requisiti in caso di accesso limitato 2
SEZIONE 3: REQUISITI DI SICUREZZA GENERALI 2
3 Sicurezza generale delle informazioni 2
4 Sicurezza del personale temporaneo 6
5 Verifica e revisione della sicurezza 7
6 Accertamenti 7
SEZIONE 4: REQUISITI DI SICUREZZA SPECIFICI 8
7 Politica e requisiti generici di sicurezza 8
8 Sicurezza fisica - Strutture di BT 8
9 Sicurezza fisica - Strutture del fornitore 9
10 Predisposizione di un ambiente di hosting 11
11 Sviluppo dei servizi 11
12 DEPOSITO IN GARANZIA 12
13 Accesso ai sistemi di BT 12
14 Accesso alle informazioni di BT contenute nei sistemi del fornitore 13
15 Hosting delle informazioni di BT da parte del fornitore 14
16 Sicurezza di rete 14
17 Sicurezza di rete del fornitore 16
18 Sicurezza del cloud 17
19 Centro di contatto 17
SEZIONE 5: DEFINIZIONI 17

SEZIONE 1: INTRODUZIONE

1 INTRODUZIONE

1.1 Il presente documento illustra i requisiti di sicurezza richiesti da BT.

1.2 Nei presenti requisiti di sicurezza, saranno valide le definizioni contenute nella sezione 5, intitolata "**Definizioni**". Negli altri casi, ai presenti requisiti di sicurezza saranno applicabili i termini del contratto, e tutte le parole ed espressioni utilizzate nei presenti requisiti di sicurezza avranno lo stesso significato a loro attribuito nel contratto.

1.3 I presenti requisiti di sicurezza integrano e non alterano gli altri obblighi del fornitore disposti nel contratto (inclusi, senza intento limitativo, gli obblighi di cui alle condizioni intitolate "**Riservatezza**", "**Tutela dei dati personali**" e "**Conformità**").

SEZIONE 2: REQUISITI IN CASO DI ACCESSO LIMITATO

2 REQUISITI IN CASO DI ACCESSO LIMITATO

Questa sezione sarà considerata applicabile nel caso in cui il fornitore eroghi delle forniture che comportino un accesso limitato alle informazioni di BT o dei clienti di BT, oppure comportino un accesso a livello di utente ai sistemi amministrativi di BT. I fornitori che fanno parte di questa categoria non dovranno ottemperare ad alcuna altra parte del presente documento.

2.1 Fatti salvi gli obblighi di riservatezza a cui possa essere soggetto, laddove il fornitore o il personale temporaneo accedano alle informazioni di BT o dei clienti di BT, il fornitore dovrà:

2.2 fare in modo che le informazioni di BT non vengano divulgate né consultate dal personale temporaneo, tranne nei casi in cui ciò sia necessario per l'erogazione delle forniture; e

2.3 mettere in atto tutti i sistemi e le procedure (tecnici e organizzativi) necessari per salvaguardare la sicurezza e la riservatezza delle informazioni e dei sistemi di BT, conformemente alle buone prassi di sicurezza del settore.

SEZIONE 3: REQUISITI DI SICUREZZA GENERALI

Obbligatori nei casi in cui quanto disposto nella sezione 2: Requisiti in caso di accesso limitato, non sia considerato applicabile.

3 SICUREZZA GENERALE DELLE INFORMAZIONI

Sicurezza generale delle informazioni

3.1 Il Fornitore implementerà sistemi e processi (sia tecnici che organizzativi) al fine di:

3.1.1 salvaguardare la sicurezza e la riservatezza delle informazioni e dei sistemi di BT come previsto dai presenti requisiti di sicurezza; e

3.1.2 garantire la disponibilità, la qualità, l'integrità e una capacità adeguata di erogare le forniture senza interruzione, come previsto dalle buone prassi di sicurezza del settore.

3.2 Il fornitore implementerà un processo documentato di gestione delle modifiche informatiche in modo tale che qualunque cambiamento apportato ai processi e ai sistemi del fornitore sia implementato mantenendo la conformità ai presenti requisiti di sicurezza.

3.3 Su richiesta scritta di BT, il fornitore metterà a disposizione di BT copie di ogni certificazione di sicurezza e dichiarazione di conformità relativa alle forniture al fine di dimostrare la propria conformità ai presenti requisiti di sicurezza.

3.4 Il fornitore adotterà ogni misura ragionevole per assicurare l'adeguatezza del soggetto o dei soggetti nominati e incaricati di agire come referenti per la gestione dei rischi alla sicurezza, degli incidenti e della conformità. Il fornitore fornirà al referente per la sicurezza di BT gli estremi di tale soggetto o di tali soggetti e lo informerà di ogni cambiamento ad essi relativo. Gli estremi dovranno comprendere:

nome, responsabilità, ruolo, indirizzo email e/o numero di telefono di gruppo

3.5 Il fornitore riconosce e accetta che, di tanto in tanto, BT possa apportare modifiche ragionevoli ai requisiti di sicurezza di BT, nel caso in cui:

3.5.1 il fornitore sia oggetto di fusione, acquisizione o di altri cambiamenti materiali inerenti alla proprietà o al controllo;

3.5.2 vengano modificati gli standard tecnologici o di sicurezza del settore; oppure

3.5.3 vengano modificate materialmente le forniture o le modalità di erogazione,

(ognuno di questi è una "**Variazione dei requisiti di sicurezza**").

Dopo essere stato informato per iscritto da BT della necessità di una variazione dei requisiti di sicurezza, il fornitore dovrà attuare tale variazione tempestivamente, e, in ogni caso, entro un periodo ragionevole (tale periodo ragionevole dovrà tenere conto del tipo di variazione e dei rischi che presenta per BT).

3.6 Almeno con cadenza annuale o quando vi siano variazioni materiali delle forniture o delle modalità di erogazione delle stesse, il fornitore dovrà riesaminare i presenti requisiti di sicurezza al fine di accertarne la conformità a tutti i requisiti di sicurezza applicabili.

3.7 In caso di utilizzo da parte del fornitore, ai sensi del contratto, di subappaltatori, il fornitore dovrà fare in modo che tutti i contratti disposti con i subappaltatori contengano termini scritti che obbligano i subappaltatori alla conformità ai requisiti di sicurezza per i fornitori di BT, nella misura in cui essi sono applicabili. Tali termini dovranno essere predisposti tra fornitore e subappaltatore prima che il subappaltatore o qualunque membro del suo personale possa avere accesso ai sistemi e alle informazioni di BT.

Utilizzo delle informazioni di BT

3.8 Il fornitore non potrà utilizzare le informazioni di BT per alcun scopo che non sia quello per il quale tali informazioni sono state date al fornitore e comunque solo nella misura necessaria a mettere il fornitore nelle condizioni di eseguire il contratto. Laddove il fornitore effettui il trattamento di dati personali, non potrà utilizzare alcun dato personale che faccia parte delle informazioni di BT per alcun scopo che non sia quello specificato nell'allegato sul trattamento.

3.9 Le informazioni di BT potranno essere conservate per tutto il tempo necessario all'esecuzione del contratto, dopo di che dovranno essere conservate per non più di due anni, a meno che un diverso periodo di conservazione sia stato convenuto da BT e dal fornitore, o nel caso in cui sia richiesto dalla legislazione in vigore. Per fugare ogni dubbio, nel caso in cui il fornitore tratti dati personali, non potrà conservare alcun dato personale che faccia parte delle informazioni di BT per periodi più lunghi di quelli indicati nell'allegato sul trattamento o nella clausola "**Protezione dei dati personali**".

3.10 Il fornitore dovrà attenersi alle politiche e alle norme applicabili indicate su:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

3.11 Nel caso in cui le forniture siano a sostegno diretto di un contratto stipulato con il governo del Regno Unito, il fornitore dovrà osservare quanto disposto dalla versione più aggiornata di Cyber Essentials Plus.

Trattamento delle informazioni

3.12 Il fornitore avrà e seguirà procedure di trattamento delle informazioni che siano materialmente coerenti con quanto disposto nelle specifiche per la classificazione e il trattamento delle informazioni di terze parti e che garantiscano come minimo che il fornitore:

3.12.1 implementi procedure volte a evitare la distribuzione non autorizzata delle informazioni di BT in qualunque forma, compreso per email, fax, social media, stampa o posta (ad esempio, implementando una politica di blocco dei computer e pulizia dello spazio di lavoro, e assicurandosi che le informazioni strettamente riservate non vengano inviate tramite fax o email);

3.12.2 non discuta delle informazioni di BT durante le riunioni, tranne nel caso in cui tutti i partecipanti: (i) siano autorizzati a partecipare alla riunione; (ii) abbiamo necessità di conoscere le informazioni oggetto di discussione; e (iii) siano a conoscenza e prendano in considerazione i loro obblighi in materia di riservatezza;

3.12.3 non archivi le informazioni di BT:

3.12.3.1 nel cloud o tramite servizi internet che comprendono, senza intento limitativo, Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin o Facebook, salvo se previamente concordato per iscritto con BT;

3.12.3.2 su portatili o altri dispositivi, a meno che non siano protetti con un sistema completo di crittografia del disco (ad esempio, BitLocker) che rispetti gli standard illustrati al paragrafo 3.15; oppure

3.12.3.3 cancelli o cessi di utilizzare le informazioni di BT per le normali attività aziendali in modo sicuro.

Controllo degli accessi

3.13 Il fornitore effettuerà il controllo degli accessi ai propri sistemi in modo adeguato all'ambiente e alla natura delle forniture erogate a BT, per fare in modo che, ove applicabile:

3.13.1 tutti gli utenti, compresi gli utenti con il grado di amministratore, siano in possesso di identificativi unici;

3.13.2 le password siano regolarmente modificate (almeno ogni 90 giorni);

3.13.3 dopo tentativi di accesso non riusciti, siano implementate misure di protezione adeguate per evitare attacchi di tipo "brute force";

3.13.4 gli account non utilizzati siano automaticamente disattivati;

3.13.5 siano usate password di potenza adeguata (con minimo 8 caratteri, tra cui tre elementi delle seguenti categorie: (i) lettere maiuscole; (ii) lettere minuscole; (iii) numeri; e (iv) caratteri non alfanumerici) e sia implementata la storia delle password per impedire l'utilizzo di password già usate nei 12 mesi precedenti;

3.13.6 sia implementato un accesso ai sistemi del fornitore che si basa sul ruolo con, come minimo, controlli dell'accesso più stringenti per gli amministratori; e

3.13.7 siano effettuate revisioni e verifiche dell'accesso degli utenti.

Accesso remoto

3.14 Il fornitore non può consentire al personale temporaneo di effettuare l'accesso remoto alle informazioni classificate come 'strettamente riservate', salvo previo accordo scritto stipulato con BT. Laddove è consentito l'accesso remoto, il fornitore dovrà assicurarsi che esso sia soggetto ad adeguati controlli di sicurezza all'interno dell'organizzazione del fornitore stesso, incluso, senza intento limitativo, assicurandosi che l'accesso remoto da parte degli utenti sia soggetto a un sistema forte di autenticazione a due fattori. In caso di utilizzo dell'accesso remoto tramite reti pubbliche per scopi di supporto, la connessione dovrà essere crittografata secondo le norme indicate al paragrafo 3.15.

Trasmissione dei dati

3.15 La trasmissione ordinaria di grossi quantitativi di informazioni di BT dovrà essere effettuata tramite PGP o con una piattaforma di trasferimento approvata dal settore.

Crittografia

3.16 Il fornitore dovrà assicurarsi che le informazioni di BT riservate e strettamente riservate siano crittografate (sia a riposo che in transito), conformemente alle buone prassi di sicurezza del settore, e assicurandosi che non siano usati standard disapprovati dal settore interessato. Gli attuali standard di crittografia approvati da BT alla data di inizio che rispettano i requisiti del presente paragrafo 3.15, sono illustrati nelle specifiche per la classificazione e il trattamento delle informazioni di terze parti.

Patch

3.17 Il fornitore dovrà avere e seguire una procedura documentata di gestione delle patch, che dovrà assicurare come minimo che il fornitore:

3.17.1 applichi le patch rispettando le seguenti tempistiche:

Tipo di patch	Descrizione	Tempistica
Patch critiche	Patch necessarie per far fronte alle vulnerabilità zero day	Appena possibile e, in ogni caso, entro 14 giorni da quando la patch diventa disponibile
Patch importanti	Per vulnerabilità classificate come alte, con un punteggio di 7.0 - 8.9 sulla scala di gravità qualitativa del Common Vulnerability Scoring System (CVSS)	Entro 30 giorni da quando la patch diventa disponibile
Altre patch	Tutte le patch che non sono importanti o critiche	Entro 8 settimane da quando la patch diventa disponibile

3.17.2 monitori l'emissione delle patch da parte dei venditori pertinenti;

3.17.3 utilizzi patch ottenute: direttamente dai venditori per i sistemi proprietari e patch che siano (i) dotate di firma digitale o (ii) verificate tramite l'utilizzo di un hash del venditore (non si devono usare hash MD5) per il pacchetto di aggiornamento, in modo che la patch possa essere identificata come proveniente da una comunità di supporto affidabile per il software open source;

3.17.4 testi tutte le patch su sistemi che rappresentino con precisione la configurazione dei sistemi di produzione obiettivo prima dell'applicazione della patch ai sistemi di produzione stessi e che, dopo l'installazione di una patch, verifichi il corretto funzionamento del servizio dotato di patch; e

3.17.5 Provveda alla manutenzione e all'aggiornamento dei sistemi del fornitore per assicurarsi che vengano applicate le vendor patch più aggiornate.

3.18 Se il fornitore non può applicare una patch a un sistema, dovrà informare BT per iscritto. Dopo la ricezione di tale informazione, BT analizzerà i rischi per BT e le informazioni di BT associati all'uso continuo del sistema da parte del fornitore, e BT potrebbe richiedere al fornitore di adottare ogni ragionevole misura per affrontare tali rischi (a spese del fornitore).

Gestione delle vulnerabilità

3.19 Il fornitore dovrà avere e seguire una procedura di gestione delle vulnerabilità, che dovrà assicurare come minimo che il fornitore:

3.19.1 adotti le azioni opportune per individuare le vulnerabilità (ad esempio, con lo scanning);

3.19.2 effettui regolarmente prove di penetrazione; conservi i verbali di tali prove; e

3.19.3 reagisca a eventuali notifiche di vulnerabilità implementando piani di intervento atti ad attenuare le vulnerabilità note, conformemente ai paragrafi 3.22-3.27.

Prove di penetrazione

3.20 Il fornitore dovrà:

3.20.1 consentire a BT (o ai subappaltatori autorizzati da BT) di effettuare ragionevoli prove di penetrazione con un preavviso ragionevole; e

3.20.2 fornire a BT l'accesso ai verbali relativi alle prove di penetrazione effettuate dal fornitore e alle forniture erogate.

Controllo e registrazione

3.21 Il fornitore dovrà avere e seguire una procedura di controllo e registrazione che assicuri come minimo che il fornitore registri, se del caso, i seguenti eventi:

3.21.1 i punti iniziali e finali della procedura registrata;

3.21.2 variazioni del tipo di eventi registrati, come richiesto dalla pista di audit (ad esempio, i parametri di avvio ed eventuali variazioni degli stessi);

3.21.3 avvio e arresto dei sistemi del fornitore;

3.21.4 login riusciti;

3.21.5 tentativi di login non riusciti (ad esempio, per identificativo utente o password errati);

3.21.6 tutte le operazioni effettuate dagli utenti privilegiati (ad esempio, gli utenti con accesso potente alle utilità o applicazioni di sistema);

3.21.7 privilege escalation riuscita o non riuscita;

3.21.8 tutti gli accessi o le operazioni effettuate dal fornitore a dal suo personale temporaneo sulle informazioni strettamente riservate; e

3.21.9 creazione, modifica e cancellazione degli account utenti.

3.22 Per ogni evento oggetto di audit, il fornitore dovrà conservare una pista di audit a prova di manomissione che consenta di ricostruire tali eventi.

3.23 Tenuto conto della criticità del componente o dei dati, il fornitore dovrà regolarmente ispezionare e analizzare i log di audit al fine di rilevare comportamenti sospettosi o anomali, per poi prendere gli opportuni provvedimenti e/o lanciare un allarme.

3.24 Tutti gli allarmi dovranno essere documentati e dovranno essere presi provvedimenti secondo le tempistiche determinate dalla criticità dell'allarme.

3.25 Il fornitore dovrà conservare i file di log per 3 mesi (tranne nel caso in cui debbano essere cancellati ai sensi della clausola "**Protezione dei dati personali**") e, su richiesta di BT, fornirà copie dei file di log oppure permetterà l'accesso agli stessi, in un formato concordato da entrambe le parti.

Gestione delle minacce e degli incidenti

3.26 Il fornitore dovrà avere e seguire una procedura formale di gestione degli incidenti di sicurezza che comprenda la definizione specifica delle responsabilità in caso di incidenti di sicurezza rilevanti. Tutte le informazioni relative agli incidenti di sicurezza rilevanti saranno da considerare **"riservate**".

3.27 Dopo essere venuto a conoscenza di un incidente di sicurezza rilevante, il fornitore dovrà informare il referente per la sicurezza e il referente commerciale di BT entro un lasso di tempo ragionevole; in ogni caso, non oltre le dodici (12) ore da quando è venuto a conoscenza dell'incidente di sicurezza rilevante.

3.28 Senza ritardi ingiustificati, il fornitore dovrà prendere provvedimenti correttivi adeguati e tempestivi per attenuare eventuali rischi ed effetti relativi all'incidente di sicurezza rilevante, al fine di ridurre la gravità e la durata dell'incidente stesso.

3.29 Il fornitore accetta di fornire tutte le informazioni ragionevolmente richieste da BT in relazione all'incidente di sicurezza rilevante, incluso, senza intento limitativo, quanto segue:

3.29.1 data e ora;

3.29.2 luogo;

3.29.3 tipo di incidente;

3.29.4 impatto;

3.29.5 classificazione delle informazioni interessate;

3.29.6 stato; e

3.29.7 risultato (comprese le raccomandazioni per la risoluzione o le azioni intraprese).

3.30 Il fornitore dovrà fare in modo di rettificare rapidamente i rischi individuati alla riservatezza, all'integrità o alla disponibilità delle informazioni di BT all'interno dei processi o dei sistemi del fornitore.

3.31 Nel caso in cui un incidente di sicurezza rilevante costituisca anche una violazione dei dati personali, il fornitore dovrà inoltre attenersi alle disposizioni indicate nella clausola "**Protezione dei dati personali**", oltre alle disposizioni contenute nei presenti requisiti di sicurezza. Per fugare ogni dubbio, il fornitore dovrà inoltre attenersi alle disposizioni indicate nella clausola "**Protezione dei dati personali**" in relazione a tutte le violazioni dei dati personali, indipendentemente dal fatto che la violazione costituisca o meno un incidente di sicurezza rilevante.

4 SICUREZZA DEL PERSONALE TEMPORANEO

4.1 Il personale temporaneo riceverà l'autorizzazione di accesso unicamente previo completamento della formazione alla sicurezza di BT disponibile su https://workingwithbt.extra.bt.com o tramite il sistema di apprendimento di BT, per il quale il personale temporaneo ha ricevuto un codice identificativo BT. La formazione alla sicurezza di BT dovrà essere regolarmente aggiornata, come indicato su https://workingwithbt.extra.bt.com. Il fornitore dovrà conservare la documentazione relativa alla formazione e metterla a disposizione di BT per le procedure di verifica.

4.2 Prima che il personale temporaneo inizi a lavorare negli edifici di BT o sui sistemi di BT, o prima che acceda alle informazioni di BT, il fornitore provvederà affinché tale personale temporaneo firmi accordi di riservatezza contenenti obblighi sostanzialmente simili a quelli imposti al fornitore nella sezione 2 di cui sopra. Questi accordi di riservatezza devono essere conservati dal fornitore e messi a disposizione per le verifiche di BT nell'ambito delle procedure di verifica.

4.3 Il fornitore si impegna ad intervenire in caso di violazioni alle politiche e procedure di sicurezza del fornitore e di BT, attraverso processi formali, comprese, se opportuno, azioni disciplinari che potrebbero comportare il divieto per il soggetto di:

4.3.1 accedere ai sistemi o alle informazioni di BT; oppure

4.3.2 svolgere le mansioni connesse all'erogazione delle forniture.

Inoltre, il fornitore dovrà predisporre procedure adeguate per fare in modo che al personale temporaneo che è stato rimosso non venga in seguito dato accesso ai sistemi e alle informazioni di BT, oppure che non gli sia consentito di lavorare nell'ambito dell'erogazione delle forniture.

4.4 Nei limiti consentiti dalla legge, il fornitore dovrà predisporre una linea telefonica riservata, a disposizione di tutto il proprio personale, che il personale temporaneo dovrà usare nel caso in cui qualcuno li inviti ad agire in modo non coerente o in violazione dei presenti requisiti di sicurezza. I relativi verbali dovranno essere segnalati al referente per la sicurezza di BT.

4.5 Laddove le forniture cessino di essere assegnate al personale temporaneo, il fornitore provvederà affinché:

4.5.1 sia revocato l'accesso alle informazioni di BT; e

4.5.2 a discrezione di BT, ogni bene o informazione di BT in possesso del personale temporaneo:

4.5.2.1 venga restituito al team operativo BT competente; oppure

4.5.2.2 venga distrutto ai sensi della versione più aggiornata delle specifiche per la classificazione e il trattamento delle informazioni di terze parti.

4.6 Salvo diverso accordo scritto con il referente per la sicurezza di BT, il fornitore dovrà implementare per il personale temporaneo una procedura di uscita controllata che includa una richiesta scritta al referente per la sicurezza di BT per la rimozione dell'accesso ai sistemi e alle informazioni di BT, nonché di ogni altro accesso. Il personale temporaneo dovrà essere informato che l'accordo di riservatezza sottoscritto resterà in vigore e che le informazioni di BT acquisite tramite il lavoro sulle forniture non dovranno essere divulgate.

4.7 Nell'ambito della concessione dell'accesso, il fornitore dovrà conservare ed esibire i registri di tutto il personale temporaneo che necessita di accesso o coinvolto nell'erogazione di forniture di BT, indicando nominativo, ubicazione dei lavori, indirizzo email 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 ha lasciato il progetto BT e una dichiarazione di controllo pre-assunzione. Il referente per la sicurezza del fornitore dovrà accertarsi in permanenza che l'autorizzazione venga rilasciata unicamente al personale temporaneo interessato.

4.8 Il fornitore dovrà predisporre politiche e procedure tali da garantire che il personale temporaneo non utilizzi i social media per postare o pubblicare online dichiarazioni, commenti, contenuti o immagini che:

4.8.1 potrebbero essere ragionevolmente attribuibili a BT;

4.8.2 diffondano informazioni di BT che siano riservate o contrassegnate come 'riservate' o 'strettamente riservate'; e

4.8.3 siano diffamatori nei confronti di BT, e ne possano danneggiare il marchio e la reputazione.

5 VERIFICA E REVISIONE DELLA SICUREZZA

5.1 Fatto salvo ogni altro diritto alla verifica in capo a BT, al fine di valutare la conformità del fornitore ai presenti requisiti di sicurezza e nei casi in cui sia applicabile la clausola "**Protezione delle informazioni personali**", BT o i propri rappresentanti designati si riservano il diritto di effettuare, di tanto in tanto, una verifica di conformità alla sicurezza riguardante qualunque aspetto delle politiche, delle procedure e dei sistemi del fornitore (purché il fornitore protegga la riservatezza di qualunque informazione non legata all'erogazione delle forniture a BT), tramite una revisione della sicurezza basata sulla documentazione oppure da effettuare nella sede del fornitore o di ogni subappaltatore pertinente che sia coinvolto nell'erogazione delle forniture o nell'esecuzione del contratto.

5.2 Il fornitore dovrà fornire a BT o ai suoi rappresentanti l'accesso e l'assistenza necessari e appropriati per consentire l'effettuazione delle revisioni di sicurezza usando la documentazione oppure in loco. Al fornitore verrà dato un preavviso minimo di 30 giorni lavorativi prima di una revisione di routine in loco. Tuttavia, per fugare ogni dubbio, in caso di una violazione dei dati personali o della sicurezza (effettiva o presunta), BT non sarà tenuta a dare tale preavviso.

5.3 Il fornitore collaborerà con BT al fine di implementare le raccomandazioni concordate e attuare le azioni correttive che BT riterrà necessarie in seguito alla revisione di sicurezza basata sulla documentazione o a una verifica in loco entro 30 giorni dalla notifica di tali raccomandazioni o azioni correttive da parte di BT oppure entro un periodo concordato tra le parti, a spese del fornitore.

5.4 Nel caso in cui BT debba svolgere una verifica indipendente del fornitore e risulti che lo stesso non rispetta i principi e le prassi previste da ISO/IEC 27001:2013, il fornitore dovrà provvedere, a proprie spese, a intraprendere le azioni richieste per ottenere la conformità necessaria e rimborserà integralmente ogni spesa sostenuta da BT nell'ottenimento di tale verifica.

6 ACCERTAMENTI

6.1 Qualora BT abbia motivo di sospettare che si sia verificata:

6.1.1 una violazione dei dati personali;

6.1.2 una violazione di sicurezza;

6.1.3 oppure una violazione dei presenti requisiti di sicurezza,

BT informerà il referente per la sicurezza del fornitore e il fornitore accetta, a proprie spese, di fare quanto segue:

6.1.4 attivarsi immediatamente per accertare la presunta violazione e individuare, evitare e fare ogni sforzo ragionevole per attenuare gli effetti di tale violazione; e

6.1.5 effettuare le attività di recupero o qualunque altra attività necessaria al fine di porre rimedio alla violazione;

6.1.6 fornire i verbali ragionevolmente richiesti da BT relativi ai risultati dell'accertamento e le azioni intraprese per correggere o attenuare la violazione.

In caso di violazione grave, il fornitore dovrà collaborare senza riserve con BT in ogni accertamento o verifica che ne consegua effettuata da BT, da un'autorità di vigilanza e/o dalle autorità preposte all'applicazione della legge. Tale accertamento o verifica includerà l'accesso alle informazioni di BT presenti presso le strutture o sui sistemi del fornitore, previo ragionevole preavviso da parte di BT al fornitore.

Nel corso degli accertamenti, il fornitore avrà l'obbligo di collaborare con BT, fornendo l'opportuna assistenza e l'accesso necessari 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 e il fornitore non potrà in tal caso opporsi alla richiesta o prorogarne i tempi di risposta senza un ragionevole motivo.

SEZIONE 4: REQUISITI DI SICUREZZA SPECIFICI

7 POLITICA E REQUISITI GENERICI DI SICUREZZA

7.1 Il fornitore dichiara e garantisce che i propri sistemi, le forniture e i relativi servizi, le procedure e i luoghi fisici sono e saranno conformi senza interruzioni alla certificazione ISO/IEC 27001:2013 e ad eventuali versioni modificate o future di tale certificazione. Tale conformità dovrà essere garantita, a esclusiva discrezione di BT, mediante:

7.1.1 una certificazione dell'ISMS (sistema di gestione della sicurezza delle informazioni) del fornitore da parte di un ente di certificazione approvato UKAS o di un equivalente internazionale, previa convalida da parte di BT dell'ambito di applicazione e della dichiarazione di applicabilità; oppure

7.1.2 una procedura bilaterale di verifica e prova specificata da BT.

7.2 All'inizio del contratto e in occasione di future nuove certificazioni, il fornitore dovrà presentare una certificazione ISO/IEC 27001 valida.

7.3 In caso di variazioni all'ambito di applicazione o alla dichiarazione di applicabilità, il fornitore dovrà presentare tali variazioni per la nuova convalida utilizzando la procedura di controllo delle modifiche, oppure, in mancanza di una procedura di controllo delle modifiche, tramite la procedura di variazione. Il fornitore dovrà informare BT entro 2 giorni lavorativi di ogni non conformità significativa individuata dall'ente di certificazione o dal fornitore stesso.

8 SICUREZZA FISICA - STRUTTURE DI BT

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante se il fornitore effettua forniture presso le strutture di BT.

8.1 Tutti i membri del personale temporaneo impegnati presso le strutture di BT dovranno essere in possesso ed esibire una tessera di identificazione fornita dal fornitore o da BT che ne dimostri l'autorizzazione ("**tessera per l'accesso autorizzato**"). Le tessere per l'accesso autorizzato dovranno includere una immagine fotografica chiaramente visibile e fedelmente rappresentativa del personale temporaneo. 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 Laddove il personale temporaneo abbia ricevuto una tessera per l'accesso autorizzato da BT, il fornitore dovrà informare BT tempestivamente e, in ogni caso, entro 5 giorni lavorativi, quando tale personale temporaneo non ha più bisogno di accedere alle strutture di BT.

8.3 Solo server conformi agli standard BT, PC Web top 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 apparecchiature non approvate da BT a un qualsiasi dominio BT senza previa autorizzazione del referente per la sicurezza di BT. Il referente per la sicurezza di BT fornirà l'autorizzazione scritta solo contestualmente all'avvio del processo di concessione della politica di sicurezza interna di BT. In ogni caso, il fornitore dovrà assicurarsi che nessuna apparecchiatura di proprietà personale del personale temporaneo o di ogni altro dipendente, (compresi i subappaltatori, i dipendenti temporanei e i lavoratori interinali) sia utilizzato per l'archiviazione, l'accesso o l'elaborazione di dati di BT.

8.4 Nessuna informazione di BT potrà essere rimossa dalle strutture di BT e nessuna apparecchiatura o software potranno essere rimossi o installati presso le strutture di BT senza previa autorizzazione di BT.

8.5 Le linee guida in materia di protezione fisica e di lavori all'interno delle strutture di BT dovranno essere rispettate e dovranno comprendere, senza intento limitativo, l'accompagnamento del personale temporaneo e l'adozione di pratiche lavorative adeguate all'interno delle zone protette.

8.6 Laddove il fornitore sia autorizzato a concedere al proprio personale temporaneo l'accesso non accompagnato alle aree interne alla proprietà di BT, il firmatario autorizzato di BT e il personale temporaneo dovranno aderire alle linee guida del documento "**Accesso dei fornitori alle strutture e agli edifici di BT**" https://groupextranet.bt.com/selling2bt/working/third_party_access/default.htm. Inoltre, il firmatario autorizzato non di BT e i membri del personale temporaneo dovranno essere sottoposti a controlli pre-impiego di livello minimo L2 https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

9 SICUREZZA FISICA - STRUTTURE DEL FORNITORE

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante se il fornitore effettua forniture presso le strutture non di BT. (Ad esempio, fornitori e terze pari dei fornitori)

9.1 L'accesso alle strutture non di BT (siti, edifici o aree interne) in cui vengono erogate le forniture o in cui vengono archiviate o trattate le informazioni di BT dovrà avvenire mediante una tessera di identificazione proveniente da un fornitore autorizzato. Questa tessera dovrà essere utilizzata sempre 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 per accedere alle strutture di interesse o, in alternativa, di un accesso di sicurezza tramite tastiera. Il fornitore dovrà predisporre procedure regolari (almeno mensili) e ad hoc per l'autorizzazione e la diffusione delle modifiche ai codici.

9.2 Il fornitore provvederà affinché l'accesso alle strutture non di BT in cui vengono eseguite le forniture, o in cui vengono archiviate o trattate le informazioni di BT, avvenga tramite autorizzazione. Il fornitore dovrà aderire ai processi e alle procedure di sicurezza per il controllo e il monitoraggio del personale temporaneo, dei visitatori e di ogni altro individuo esterno, comprese le terze parti con accesso fisico a queste aree (ad esempio, gli addetti al controllo ambientale, alla vigilanza e alla pulizia).

9.3 Su richiesta di BT, il fornitore disporrà affinché il personale temporaneo venga isolato in maniera sicura dal resto del personale del fornitore. Inoltre, il fornitore dovrà disporre affinché i sistemi e l'infrastruttura utilizzati per erogare le forniture siano contenuti in una rete logica dedicata. Tale rete dovrà includere solo i sistemi dedicati alla fornitura di una struttura sicura per il trattamento dei dati.

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

Laddove vengano richieste, il fornitore dovrà dare a BT le prove della valutazione dei rischi. Se, dopo essere state richieste, tali prove non verranno messe a disposizione, BT potrà richiedere una valutazione dei rischi relativa all'ambiente utilizzato per l'erogazione del servizio (centri dati, aree per il trattamento dei dati, sale computer) effettuata da BT o dal suo rappresentante, prima dell'avvio dell'erogazione delle forniture. Inoltre, BT dovrà essere informata prima di ogni lavoro significativo sulle strutture che potrebbe compromettere la sicurezza delle informazioni di BT.

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 video sorveglianza), come deterrente, o 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:

9.5.1 laddove le prove video CCTV debbano essere conservate per accertamenti su incidenti o indagini penali; oppure

9.5.2 se previsto come requisito necessario di ottemperanza normativa.

9.5.3 Tutte le registrazioni CCTV dovranno essere conservate in un armadio chiuso, con la chiave conservata e controllata in condizioni di sicurezza. L'accesso all'armadio dovrà essere limitato unicamente al personale autorizzato.

9.6 Tutti i registratori CCTV dovranno essere ubicati in punti sicuri, per evitare modifiche o cancellazioni e la possibilità di visioni "casuali" dei relativi schermi CCTV, seguendo le linee guida sull'utilizzo dei sistemi di CCTV consultabili su

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

9.7 Ogni area delle strutture del fornitore utilizzata per l'erogazione dei servizi e delle forniture dovrà essere ispezionata almeno con cadenza mensile dal fornitore per verificare l'assenza di rischi e minacce. Il fornitore dovrà considerare e attuare tutte le misure adeguate al fine di garantire la sicurezza fisica per quanto riguarda:

9.7.1 la consapevolezza di minacce locali tra cui, in via non limitativa, minacce potenziali provenienti dall'industria locale e la vicinanza a stoccaggi di materiali pericolosi; e

9.7.2 disastri naturali, compresi i rischi derivanti da allagamenti, frane o fenomeni meteorologici estremi.

9.8 Il fornitore dovrà verificare il livello di protezione dei cavi di alimentazione e telecomunicazione presenti nelle proprie strutture che trasmettono i dati o supportano i servizi informativi o i servizi radio/satellitari utilizzati nell'erogazione 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:

9.8.1 le sedi stradali, le schermature dei cavi, i pozzetti o le scatole da incasso a marciapiede attraversati da cavi di importanza critica per l'azienda dovranno essere protetti;

9.8.2 l'accesso ai vani cavi o agli armadi delle risalite cavi all'interno degli edifici operativi dovrà essere limitato mediante l'uso di appositi lettori di controllo elettronici degli accessi o con una efficace gestione delle chiavi;

9.8.3 i collegamenti per le comunicazioni informatiche e le apparecchiature per le comunicazioni poste all'interno degli impianti informatici dovranno essere protetti a livello fisico e ambientale; e

9.8.4 i collegamenti per le comunicazioni radio e satellitari e le relative apparecchiature dovranno essere protetti adeguatamente.

9.9 Salvo previo accordo tra il fornitore e il referente per la sicurezza di BT, BT richiederà che le misure di sicurezza elettronica e fisica presso le sedi dei fornitori siano integrate con l'implementazione di servizi di vigilanza nelle seguenti circostanze:

9.9.1 il luogo ha importanza operativa (ad esempio, centri di contatto, centri dati, infrastrutture di rete importanti, ecc.)

9.9.2 le informazioni di BT trattate possono avere conseguenze sul marchio e sulla reputazione di BT o danneggiarli

9.9.3 elevato volume di informazioni di BT trattate (ad esempio, vernalizzazione di processi aziendali)

9.9.4 requisiti contrattuali dei clienti

9.9.5 presenza di rischi/minacce specifici relativi al sito

9.9.6 il fornitore è in possesso di informazioni di BT altamente sensibili.

9.10 Per tutelare le apparecchiature di BT (ad esempio, server o switch) installate presso le strutture dei fornitori da minacce o pericoli di tipo ambientale, nonché dal rischio di accessi non autorizzati, tali apparecchiature dovranno essere collocate in un'area protetta e segregate dalle apparecchiature utilizzate per i sistemi delle organizzazioni non BT. Il livello di segregazione dovrà garantire che la sicurezza delle apparecchiature di BT non possa essere compromessa né deliberatamente, né accidentalmente, per effetto di un accesso accordato a organizzazioni non BT. Potrebbe, ad esempio, consistere in pareti divisorie sicure, armadi con chiusura a chiave o ingabbiature metalliche.

9.11 Il fornitore dovrà attuare misure adeguate al fine di garantire la sicurezza fisica per quanto riguarda:

9.11.1 le misure di prevenzione degli incendi, inclusi, senza intento limitativo, gli allarmi e le apparecchiature di rilevamento e spegnimento;

9.11.2 le condizioni climatiche, tenendo in considerazione la temperatura, l'umidità e l'elettricità statica, nonché la gestione, il monitoraggio e la risposta alle condizioni estreme (come, ad esempio, lo spegnimento automatico, allarmi);

9.11.3 le apparecchiature di controllo, inclusi, senza intento limitativo, i sistemi di climatizzazione e rilevamento idrico;

9.11.4 l'ubicazione delle cisterne e dei tubi idraulici all'interno delle strutture;

9.11.5 l'accesso verificabile. Laddove sia appropriato, l'accesso del personale ai sistemi dovrà essere verificabile; e

9.11.6 la supervisione del personale temporaneo non normalmente associato alla gestione o all'accesso ai sistemi di BT.

9.12 A protezione delle zone contenenti informazioni sensibili di BT o informazioni sui clienti di BT (compresi i dati personali) e delle strutture di elaborazione delle informazioni dovranno essere eretti perimetri di sicurezza (barriere quali pareti, recinzioni, cancelli ad apertura mediante tessera o reception presidiate).

9.13 Per evitare l'accesso non autorizzato o aggressioni deliberate, dovranno essere controllati, e se possibile isolati dalle installazioni di trattamento delle informazioni, i punti d'accesso quali le zone di consegna e di carico e altri punti da cui potrebbero entrare nelle strutture persone non autorizzate.

9.14 Il fornitore dovrà assicurarsi che l'accesso fisico alle aree da cui si accede alle informazioni di BT o alle informazioni sui clienti di BT (compresi i dati personali) avvenga mediante carte di prossimità o a microprocessore (o con sistemi di sicurezza equivalenti) e dovrà effettuare verifiche interne mensili per accertare il rispetto di tali disposizioni.

9.15 Il fornitore disporrà il divieto di scattare fotografie o acquisire in altro modo immagini delle informazioni di BT o delle informazioni dei clienti di BT (compresi i dati personali). In circostanze eccezionali per cui possa presentarsi la necessità per motivi aziendali di acquisire tali immagini, sarà necessario ottenere dal referente per la sicurezza di BT l'esenzione temporanea da questa clausola in forma scritta.

9.16 A tutela delle informazioni di BT, il fornitore dovrà mettere in atto una politica aziendale di blocco dei computer e pulizia dello spazio di lavoro.

10 PREDISPOSIZIONE DI UN AMBIENTE DI HOSTING

L'osservanza delle clausole contenute nella presente sezione 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 nelle proprie strutture un'area ad accesso protetto per l'hosting di apparecchiature di BT o dei clienti di BT ("**Sito del fornitore**"), il fornitore dovrà:

10.1.1 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 come strumento di verifica dell'identità presso le strutture del fornitore e dovrà includere una immagine fotografica chiaramente visibile e fedelmente rappresentativa del membro del personale temporaneo; e

10.1.2 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

10.1.3 dovrà fare uso di sistemi di sicurezza CCTV e dei relativi supporti di registrazione presso il proprio sito sia in risposta a incidenti di sicurezza, come strumento di video sorveglianza, come deterrente e come ausilio nella possibile cattura di individui colti nell'atto di commettere un reato. Il fornitore dovrà assicurare 20 giorni di registrazione mediante CCTV per un possibile utilizzo come efficace strumento investigativo; e

10.1.4 fornire a BT una pianta degli spazi assegnati nell'area protetta del sito del fornitore;

10.1.5 assicurarsi che 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; e

10.1.6 introdurre un processo di gestione sicura delle chiavi presso il sito del fornitore; e

10.1.7 ispezionare regolarmente l'area che circonda il sito del fornitore per verificare l'eventuale presenza di rischi e minacce; e

10.1.8 documentare e mantenere le procedure operative (nella lingua del Paese da cui hanno avuto origine i lavori di BT) per ottemperare ai requisiti di sicurezza indicati nel presente paragrafo 10 e, su richiesta, fornire a BT l'accesso a tale documentazione.

10.2 BT dovrà trasmettere al fornitore le seguenti informazioni:

10.2.1 un registro dei beni materiali di BT o del cliente di BT presenti presso il sito del fornitore; e

10.2.2 estremi dei dipendenti, subappaltatori e agenti di BT che abbiano necessità di accedere (continuativamente) al sito del fornitore.

11 SVILUPPO DELLE FORNITURE

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante se il fornitore si occupa dello sviluppo di forniture per uso da parte di BT o dei clienti di BT. Ciò comprende i "componenti standard", le configurazioni del software e i componenti di fabbricazione relativi alle forniture.

11.1 Il fornitore dovrà attuare misure di sicurezza concordate in tutti i componenti forniti che costituiscono le forniture e/o i servizi, al fine di salvaguardare il carattere di riservatezza, disponibilità e integrità delle forniture agendo nel modo seguente:

11.1.1 conservando l'opportuna documentazione (nella lingua del Paese da cui hanno avuto origine i lavori di 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;

11.1.2 riducendo al minimo la possibilità che soggetti non autorizzati (ad esempio, pirati informatici) accedano ai sistemi, alle informazioni, alle reti o ai servizi di BT; e

11.1.3 riducendo al minimo il rischio di uso improprio dei sistemi, delle informazioni, delle reti o dei servizi di 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 (proprietario 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, dalla fase di produzione a quella di utilizzo.

11.3 Il fornitore dovrà fare in modo 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 siano soggetti a protezione avanzata in linea con i requisiti di sicurezza di BT, se forniti dal team operativo di BT, oppure realizzati secondo le migliori prassi del settore.

11.4 Il fornitore dovrà fare in modo che i sistemi e i processi utilizzati per le attività di sviluppo e prova siano segregati rispetto ai sistemi produttivi. Dovrà essere utilizzato un processo di controllo delle variazioni per la promozione di qualunque codice nell'ambiente di produzione. I dati di prova forniti da BT dovranno essere eliminati al termine di un periodo stabilito dal proprietario dei dati BT. Inoltre, negli ambienti di sviluppo o prova non dovranno essere utilizzati i dati in tempo reale o di produzione.

11.5 Ogni vulnerabilità della sicurezza di tipo critico riscontrata durante le prove e classificata di rischio medio o maggiore dovrà essere risolta prima della diffusione. Ogni lacuna nella sicurezza dei servizi individuata da BT o dal fornitore dovrà essere rettificata a spese del fornitore nei tempi ragionevoli stabiliti da BT.

11.6 Prima dell'immissione, le forniture dovranno superare prove di penetrazione indipendenti commissionate dal fornitore; tali prove dovranno essere effettuate con cadenza minima annuale e dopo ogni cambiamento o incidente, a spese del fornitore.

11.7 Le forniture sviluppate per l'utilizzo da parte di BT o dei suoi clienti dovranno essere sviluppate utilizzando un ciclo di vita dello sviluppo sicuro (SDLC, Secure Development LifeCycle) documentato, secondo standard del settore riconosciuti, al fine di ridurre al minimo il rischio di introdurre vulnerabilità della sicurezza nell'ambiente produttivo e/o presso i clienti. L'SDLC deve comprendere i seguenti gate, con manufatti materiali derivanti da ogni revisione e ispezionabili da parte di BT all'interno del quadro di audit di cui al paragrafo 5 della sezione 3 dei presenti requisiti di sicurezza:

11.7.1 revisione della sicurezza relativa ai requisiti aziendali;

11.7.2 revisione della sicurezza relativa alla progettazione;

11.7.3 revisione della sicurezza relativa al codice sorgente (automatico e/o manuale); e

11.7.4 verifica della sicurezza della soluzione prima della sua implementazione (incluso con attacchi simulati) seguendo un piano di verifica documentato e specifico per progetto basato sui verbali derivanti dalle revisioni di sicurezza relative ai requisiti aziendali, alla progettazione e al codice.

Per ulteriori indicazioni, consultare la sezione 'Secure Coding' del documento Third Party-Industry Guidance Standards:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm

12 DEPOSITO IN GARANZIA

Ora contenuto nel contratto principale.

13 ACCESSO AI SISTEMI DI BT

L'osservanza delle clausole contenute in questa sezione 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 dell'erogazione delle forniture.

13.2 In relazione all'accesso, il fornitore dovrà rispettare tutte le politiche, gli standard e le istruzioni pertinenti forniti da BT al fornitore stesso e provvederà (e, quando opportuno, disporrà affinché il personale temporaneo provveda) a quanto segue:

13.2.1 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 dovranno 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;

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

13.2.3 vietare il collegamento interdominio ai sistemi di BT se non specificamente approvato e autorizzato dal referente per la sicurezza di BT;

13.2.4 usare tutti i mezzi ragionevoli per garantire 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 di BT e delle informazioni di BT con qualsiasi mezzo; e

13.2.5 usare mezzi ragionevoli per garantire che i file contenenti informazioni, dati o materiali multimediali non attinenti alle forniture non vengano archiviati nelle apparecchiature di BT, nei server di BT, nei computer portatili e desktop forniti da BT, nei sistemi di archiviazione centralizzati di BT o nei sistemi di BT.

13.2.6 Nel caso in cui BT abbia concesso al fornitore l'accesso ad internet o all'intranet di BT, il fornitore dovrà far sì che il personale temporaneo acceda a tali reti solo in modo adeguato e solo ai fini dell'erogazione delle forniture, e che i siti inaccettabili o pericolosi per gli utenti vengano bloccati. Sarà compito del fornitore accertarsi che le linee guida in materia di utilizzo improprio di internet e della posta elettronica vengano trasmesse al personale temporaneo interessato con cadenza almeno annuale. Tali linee guida dovranno impedire

13.2.6.1 agli utenti di fare quanto segue:

(i) accedere a contenuti a sfondo sessuale, sessista, razzista o politicamente offensivo;
(ii) effettuare atti suscettibili di ledere la reputazione di BT o di singole persone;
(iii) gestire un'attività privata;
(iv) (d) violare i diritti d'autore; oppure
(v) superare il firewall o altri meccanismi di sicurezza di BT mediante operazioni di aggiramento o tunneling;

13.2.6.2 contribuire alla pubblicazione di siti o dichiarazioni online che potrebbero essere ragionevolmente interpretate come il punto di vista di BT.

13.3 Il fornitore dovrà effettuare regolari revisioni per assicurarsi che l'accesso sia necessario per svolgere le attività. Dovranno essere messe a disposizione di BT per l'ispezione copie della documentazione delle revisioni nel contesto del quadro di verifica illustrato nel paragrafo 5.1:

13.4 Il fornitore dovrà informare BT tempestivamente e, in ogni caso, entro 5 giorni lavorativi, quando un dipendente, compresi i subappaltatori, i dipendenti temporanei e i lavoratori interinali, non ha più bisogno di accedere ai sistemi di BT, ad esempio se lascia l'azienda o cambia ruolo.

14 ACCESSO ALLE INFORMAZIONI DI BT CONTENUTE NEI SISTEMI DEL FORNITORE

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

14.1 Laddove al personale temporaneo venga consentito l'accesso ai sistemi del fornitore relativamente all'erogazione di forniture e/o servizi, il fornitore dovrà dimostrare la propria responsabilità per tale accesso (incluso, senza intento limitativo, con l'utilizzo di account utente unici, la gestione delle password e una pista chiara di audit/log per tutte le azioni compiute dal personale temporaneo).

14.2 Il fornitore dovrà introdurre sistemi che rilevino e registrino ogni tentativo di danneggiamento, modifica o accesso non autorizzato alle informazioni di BT o ai sistemi del fornitore. Ad esempio, senza intento limitativo, i sistemi di registrazione e verifica dei processi, IDS, IPS ecc.

14.3 Il fornitore dovrà introdurre controlli atti a rilevare e contrastare software, virus e codici maligni e far sì che vengano attuate procedure adeguate di sensibilizzazione degli utenti.

14.4 Il fornitore dovrà assicurarsi che, con cadenza almeno mensile, l'eventuale software non autorizzato venga identificato e rimosso dai sistemi del fornitore utilizzati per contenere, trattare o accedere a informazioni di BT.

14.5 Il fornitore dovrà assicurarsi che l'accesso alle porte di diagnosi e gestione, nonché agli strumenti diagnostici, sia soggetto a controlli di sicurezza.

14.6 Il fornitore dovrà assicurarsi che l'accesso agli strumenti di verifica del fornitore sia limitato al personale temporaneo interessato e che l'utilizzo degli stessi sia monitorato.

14.7 Il fornitore dovrà assicurarsi che un team indipendente dagli sviluppatori conduca riesami dei codici e prove di penetrazione su ogni software di produzione interna (compreso ogni software) utilizzato per trattare le informazioni di BT.

14.8 I server utilizzati per l'erogazione delle forniture non dovranno essere installati su reti non affidabili (poste al di fuori del perimetro di sicurezza o del controllo amministrativo; ad esempio, esposte a internet) senza adeguati controlli di sicurezza.

14.9 Il fornitore dovrà assicurarsi che ogni modifica apportata a singoli sistemi del fornitore che contengono o trattano informazioni di BT e/o che vengono utilizzati per l'erogazione delle forniture sia controllata e sottoposta a procedure formali di controllo delle modifiche.

14.10 Il fornitore dovrà assicurarsi che gli orologi e gli orari interni di tutti i sistemi siano sincronizzati usando l'ultima versione di NTP o di un'equivalente tecnologia di sincronizzazione oraria.

14.11 Laddove il fornitore fornisca sistemi che offrono l'accesso online ai clienti di BT:

14.11.1 le credenziali online per i clienti di BT dovranno contenere come minimo quanto segue:

14.11.1.1 identificativo utente;

14.11.1.2 password online;

14.11.1.3 tre domande e risposte di autenticazione a supporto dell'accesso all'account; e

14.11.1.4 un metodo di contatto alternativo ai fini dell'autenticazione.

14.11.2 Il cliente di BT dovrà poter scegliere un identificativo utente unico per le sue credenziali online; inoltre, la password online non potrà includere l'identificativo utente unico.

14.11.3 La password online del cliente di BT deve avere un minimo di 8 caratteri e contenere almeno 1 carattere delle seguenti 3 categorie; (i) numeri decimali (0-9), (ii) lettere maiuscole (A-Z), (iii) lettere minuscole (a- z); (iv) caratteri non alfanumerici.

14.11.4 Per cambiare una password online, il cliente di BT dovrà fornire l'attuale password e poi inserire due volte la nuova password.

14.11.5 Se il cliente di BT dimentica l'identificativo utente o la password, il sistema fornito dal fornitore dovrà generare una email diretta all'indirizzo email del cliente di BT contenente il link per la reimpostazione dell'identificativo utente o della password previo inserimento nel modulo online dei seguenti dati:

14.11.5.1 MSISDN o numero di telefono fisso

14.11.5.2 password online

14.11.5.3 identificativo del cliente di BT

14.11.6 Il link per la richiesta di reimpostazione della password deve avere una durata massima di 30 minuti prima della scadenza, dopodiché sarà necessaria una nuova richiesta di reimpostazione della password online.

14.11.7 Dopo aver completato la reimpostazione della password, il cliente di BT dovrà essere obbligato a scegliere una nuova password.

14.11.8 Nel caso in cui il cliente di BT abbia dimenticato sia l'identificativo utente sia la password online, il recupero delle credenziali utente dovrà generare una email diretta all'indirizzo email registrato contenente il link per la reimpostazione dell'identificativo utente o della password che richiederà l'inserimento di nome e cognome, numero telefonico e indirizzo email del cliente di BT.

14.11.9 Potranno essere richiesti altri gradi di autenticazione del cliente a seconda del carattere sensibile dei dati e della funzionalità a cui viene richiesto l'accesso.

15 HOSTING DELLE INFORMAZIONI DI BT DA PARTE DEL FORNITORE

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante se il fornitore si affida a servizi esterni di hosting per le informazioni di BT classificate come riservate o strettamente riservate in un ambiente di servizi cloud, oppure in un ambiente con 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 di BT siano conformi ai requisiti per l'hosting di dati esterno di terze parti disponibili su:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

16 SICUREZZA DI RETE

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

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 di 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 farà in modo che essa:

16.1.1 insieme a tutta la sicurezza di rete di cui è responsabile il fornitore, soddisfi ogni requisito legale e normativo; e

16.1.2 si adoperi per impedire che soggetti non autorizzati (ad esempio, pirati informatici) accedano a elementi di gestione della rete e ad altri elementi accessibili tramite le reti di BT e/o 21CN; e

16.1.3 si adoperi per ridurre il rischio di uso improprio delle reti di BT e/o 21CN tale da causare perdite potenziali di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi; e

16.1.4 si adoperi per rilevare le potenziali violazioni della sicurezza, 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 ottenerlo; e

16.1.5 riduca al minimo il rischio di errata configurazione delle reti di BT, ad esempio concedendo il numero minimo di autorizzazioni necessarie per adempiere al ruolo oggetto di contratto.

16.2 Il fornitore dovrà adottare tutte le misure ragionevoli allo scopo di mettere in sicurezza tutte le interfacce presenti nelle forniture e/o nei servizi, senza presupporre che i componenti forniti vengano fatti funzionare in un ambiente sicuro.

16.3 Il fornitore dovrà comunicare al referente per la sicurezza di 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 saranno direttamente coinvolti nell'installazione, manutenzione e/o gestione delle forniture prima che intraprendano tali operazioni di installazione, manutenzione e/o gestione.

16.4 Relativamente alle attività di supporto svolte nel Regno Unito, il fornitore si affiderà a un team specializzato in sicurezza composto da almeno un cittadino del Regno Unito che fungerà da collegamento con il referente per la sicurezza di BT (o con i suoi addetti) e il team parteciperà alle riunioni che il referente per la sicurezza di BT potrà richiedere periodicamente.

16.5 Il fornitore dovrà trasmettere al referente per la sicurezza di BT un prospetto (opportunamente aggiornato) di tutti i componenti attivi contenuti nelle forniture e/o nei servizi con indicazione delle rispettive fonti.

16.6 Il fornitore dovrà comunicare gli estremi dei membri del suo personale che fungeranno da collegamento con il team per la gestione delle vulnerabilità (CERT) di BT in relazione alla discussione delle vulnerabilità individuate da BT e dal fornitore nelle forniture e/o nei servizi. Il fornitore dovrà fornire puntualmente a BT informazioni sulle vulnerabilità, e adempierà, a proprie spese, ai ragionevoli obblighi relativi alle vulnerabilità di cui venga informato di volta in volta dal referente per la sicurezza di BT. Il fornitore dovrà informare BT di eventuali vulnerabilità con sufficiente anticipo, in modo da consentire l'applicazione o l'installazione di sistemi di mitigazione prima che il fornitore stesso divulghi pubblicamente le vulnerabilità.

16.7 Il fornitore dovrà concedere di volta in volta al referente per la sicurezza di BT e a chi da esso designato l'accesso completo e illimitato alle strutture in cui le forniture vengono sviluppate, prodotte o create al fine di condurre prove e/o valutazioni di conformità alla sicurezza. Il fornitore sarà inoltre tenuto a collaborare a tali prove di conformità alla sicurezza (e disporrà affinché l'intero personale temporaneo interessato faccia altrettanto).

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

16.9 In relazione alle informazioni fornite o ottenute da BT e accompagnate dalla dicitura "**STRETTAMENTE RISERVATE**" o la cui natura riservata sia facilmente riconoscibile, il fornitore dovrà provvedere affinché:

16.9.1 l'accesso a tali informazioni sia consentito unicamente al personale temporaneo appositamente autorizzato da BT per la visione e il trattamento e venga conservato un registro di tali accessi;

16.9.2 tali informazioni siano 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 password forte) e che rendano rilevabili con grande probabilità eventuali azioni o tentativi di compromissione;

16.9.3 una volta trasmesse, tali informazioni vengano sottoposte a misure di sicurezza adeguate mediante crittografia con Secure Email, PGP o WinZip 9; e

16.9.4 non vengano, salvo autorizzazione scritta di BT, esportate al di fuori dello spazio economico europeo.

16.10 Il fornitore dovrà comunicare tempestivamente, e in ogni caso entro il termine di 7 giorni lavorativi, al referente per la sicurezza di BT i dettagli completi delle caratteristiche e funzionalità delle forniture (quelle esistenti o quelle pianificate e contenute nella roadmap delle forniture) che di volta in volta:

16.10.1 il fornitore conosce; o che

16.10.2 il referente per la sicurezza di BT ritiene ragionevolmente (e ne dà pertanto comunicazione al fornitore) che siano progettate, o potrebbero essere utilizzate, per l'intercettazione legale o altre forme di intercettazione del traffico delle telecomunicazioni. Tali dettagli dovranno includere tutte le informazioni ritenute ragionevolmente necessarie per consentire al referente per la sicurezza di 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 di BT, il fornitore dovrà comunicare immediatamente a BT ogni eventuale modifica apportata al proprio metodo di accesso attraverso i firewall, fornendo ad esempio la traduzione degli indirizzi di rete.

16.12 Il fornitore non potrà utilizzare strumenti di monitoraggio di rete in grado di visualizzare informazioni relative alle applicazioni.

16.13 Il fornitore dovrà assicurarsi che, quando non è necessaria, la funzionalità IPv6 inclusa nei sistemi operativi sia disabilitata sugli host (ad esempio, i dispositivi degli utenti finali o i server) collegati alle reti e ai domini di BT.

16.14 Il fornitore dovrà rispettare e disporrà affinché le forniture o i servizi rispettino le politiche eventualmente vigenti e i requisiti di sicurezza di BT. Ogni inadempienza dovrà essere concordata all'atto della firma del contratto o mediante un processo sede di controllo delle modifiche (o equivalente).

16.15 Il fornitore provvederà affinché tutto il personale temporaneo venga sottoposto a controlli pre-impiego adeguati rispetto al livello di accesso, come indicato su https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

I fornitori coinvolti nella realizzazione, sviluppo o supporto delle reti o delle infrastrutture di rete di BT 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 BT sono previsti controlli pre-impiego di livello L3. Laddove il fornitore sia impossibilitato a ottenere direttamente il nulla osta di sicurezza per il personale temporaneo nell'ambito dei controlli L3, potrà richiedere a proprie spese l'assistenza di BT.

16.16 Il fornitore dovrà provvedere alla manutenzione dell'hardware e del software secondo le specifiche del fabbricante.

16.17 Il fornitore non utilizzerà ad altri fini i materiali multimediali rimovibili (dischi, drive USB, ecc.) destinati al supporto e alla manutenzione.

17 SICUREZZA DI RETE DEL FORNITORE

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante laddove la rete del fornitore verrà utilizzata per l'erogazione delle forniture (sono incluse le reti LAN, WAN, Internet, wireless e radio).

17.1 In relazione alle forniture o ai servizi, il fornitore dovrà attuare misure di sicurezza in tutte le reti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle informazioni di BT. Le misure e il fornitore dovranno:

17.1.1 soddisfare ogni requisito legale e normativo; e

17.1.2 adoperarsi per impedire che soggetti non autorizzati (ad esempio, pirati informatici) accedano alla rete o alle reti del fornitore;

17.1.3 adoperarsi per ridurre il rischio di uso improprio della rete o delle reti del fornitore tale da causare perdite potenziali di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi; e

17.1.4 adoperarsi per rilevare le potenziali violazioni della sicurezza, 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 ottenerlo.

17.2 Dovranno essere predisposte misure adeguate che assicurino la sicurezza dei componenti, incluso, non in senso limitativo, quanto segue:

17.2.1 utilizzo di efficaci principi di "**difesa in profondità**";

17.2.2 utilizzo di sistemi di controllo atti a impedire qualsivoglia attacco intenzionale;

17.2.3 utilizzo di firewall, router e switch;

17.2.4 comunicazioni sicure tra i dispositivi e le stazioni di gestione;

17.2.5 comunicazioni sicure tra dispositivi, secondo le necessità; ciò comprende la crittografia di ogni accesso degli amministratori non effettuato da console;

17.2.6 progettazione di un'architettura robusta, graduata e dotata di una gestione dell'identità efficace e robusta, nonché di una configurazione del sistema operativo che dovrà essere soggetta a protezione avanzata e debitamente documentata;

17.2.7 disattivazione, laddove opportuno, dei servizi, delle applicazioni e delle porte non utilizzati;

17.2.8 disattivazione o eliminazione degli account guest;

17.2.9 installazione sulle reti e sui sistemi del fornitore delle patch di sicurezza più aggiornate, non appena possibile dopo le prove. Ogni eccezione dovrà essere comunicata a BT per essere sottoposta a una valutazione dei rischi. BT si riserva il diritto di obbligare il fornitore a installare le patch, dopo la valutazione dei rischi;

17.2.10 l'elusione di relazioni di fiducia tra server;

17.2.11 l'impiego del principio di sicurezza, basato sulle migliori prassi, di "**minore privilegio**" al fine di svolgere una funzione;

17.2.12 assicurarsi che siano predisposte misure adeguate per la gestione degli attacchi di tipo "denial of service";

17.2.13 assicurarsi che siano predisposte misure adeguate per il rilevamento e/o la protezione dalle intrusioni;

17.2.14 monitorare tutti i venditori pertinenti e ogni altra fonte pertinente di informazioni per rilevare gli avvisi di vulnerabilità;

17.2.15 dove opportuno, effettuare il monitoraggio dell'integrità al fine di rilevare eventuali aggiunte, modifiche o cancellazioni di file o dati di sistema critici; e

17.2.16 cambiare tutte le password di default e quelle fornite dal venditore prima che i componenti di rete entrino in funzione.

18 SICUREZZA DEL CLOUD

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante quando il fornitore presta a BT servizi correlati al cloud.

18.1 Il fornitore dovrà conformarsi a quanto segue:

l'ultima versione dei requisiti di controllo CCM (Cloud Controls Matrix) dell'ente Cloud Security Alliance; i requisiti di sicurezza di BT per l'hosting esterno consultabili su: https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm 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.

18.2 Il fornitore dovrà attuare misure di sicurezza concordate in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle forniture e ridurre al minimo il rischio che soggetti non autorizzati (ad esempio, altri clienti del cloud) accedano ad informazioni e forniture di BT.

19 CENTRO DI CONTATTO

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante quando il fornitore fornisce un centro di contatto per BT.

19.1 Il fornitore dovrà, in relazione alle forniture, assicurarsi che gli ambienti in cui sono archiviate, trattate o visualizzate le informazioni di BT rispettino i requisiti indicati nella versione più aggiornata degli standard sui centri di contatto di terze parti disponibile su:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

SEZIONE 5: DEFINIZIONI

In questi requisiti di sicurezza, saranno valide le definizioni che seguono, altrimenti ai presenti requisiti di sicurezza saranno applicabili i termini del contratto, e tutte le parole e le espressioni utilizzate in questi requisiti di sicurezza avranno lo stesso significato a loro attribuito nel contratto:

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

- interconnessione con i sistemi di BT
- in formato cartaceo o non elettronico

- informazioni di BT contenute nei sistemi del fornitore
- supporti mobili

e/o accesso agli edifici di BT per l'erogazione delle forniture (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 con autorizzazione scritta ricevuta dal referente per la sicurezza di BT; il termine "**autorizzazione**" sarà interpretato di conseguenza. Il livello di accesso accordato sarà correlato e limitato a quanto necessario per l'erogazione delle forniture.

"**Sistemi amministrativi di BT**": indicherà la piattaforma di fatturazione di BT (attualmente iSupplier), o altri sistemi puramente amministrativi concordati con BT;

"Cliente di BT": nell'ambito di questi requisiti della sicurezza, questo termine comprenderà le aziende o gli individui a cui BT fornisce beni o servizi.

"**Informazioni di BT**": tutte le informazioni relative a BT o ai clienti di BT fornite al fornitore e tutte le informazioni elaborate o trattate dal fornitore per conto di BT o dei clienti di BT in virtù del contratto.

"**Reti di BT**": la rete controllata o amministrata da BT.

"**Beni materiali di BT**": tutti i beni materiali (tra cui router, switch, server, chiavi degli armadi, token per portatili, tessere di accesso, progetti o documenti) detenuti dal fornitore ma appartenenti a BT.

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

"**Referente per la sicurezza di BT**": l'addetto alla sicurezza delle informazioni di BT Security o il referente commerciale di BT, se ne viene informato il fornitore o la sicurezza centrale [0800 321999, +44 1908 641100] che fungerà da unico punto di contatto per i temi relativi ai presenti requisiti di sicurezza e per gli incidenti di sicurezza.

"**Sistemi di BT**": i servizi e i componenti di servizi, prodotti, reti, server, processi, sistemi cartacei o sistemi informatici (parzialmente o integralmente) posseduti e/o gestiti da BT, oppure altri sistemi che potrebbero essere gestiti in hosting presso le strutture di BT, compreso iSupplier (secondo la definizione contenuta nella clausola "**Pagamento e fatturazione**").

"**Grossi quantitativi di informazioni**": più di 1000 informazioni individuali di BT classificate come riservate, oppure 100 informazioni individuali di BT classificate come strettamente riservate.

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

"**Personale temporaneo**", "**personale temporaneo interessato**": vedi definizione nel contratto.

"**Cyber Essentials Plus**": indica il programma statale britannico di supporto alle organizzazioni contro gli attacchi informatici consultabile su https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

"**Buone prassi di sicurezza del settore**": relativamente a ogni attività e circostanza, l'implementazione delle prassi, delle politiche, degli standard e degli strumenti di sicurezza che ragionevolmente e normalmente ci si aspetterebbe da una persona competente ed esperta impegnata nello stesso tipo di attività in circostanze uguali o simili.

"**Informazioni**": informazioni disponibili in forma tangibile o in altro modo, inclusi, senza intento limitativo, specifiche, relazioni, dati, appunti, documentazione, disegni, software, elaborazioni computerizzate, progetti, schemi circuitali, modelli, schemi, campioni, invenzioni (brevettabili o meno) e know-how, unitamente ai supporti (se del caso) sui quali tali informazioni vengono fornite.

"**Interne**", "**pubbliche**", "**riservate**" e "**strettamente riservate**": questi termini hanno i significati a loro assegnati nelle specifiche per la classificazione e il trattamento delle informazioni di terze parti.

"**ISO 27001**": versione corrente della normativa internazionale sui sistemi di gestione della sicurezza pubblicata dalla Organizzazione internazionale per la standardizzazione (ISO) e dalla Commissione elettrotecnica internazionale (CEI).

"**Infrastruttura di rete**": dispositivo o altro componente della rete di BT che supporta le attività di rete.

"**Sicurezza di rete**": sicurezza dei percorsi e nodi di comunicazione interconnessi che collegano logicamente le tecnologie degli utenti finali le une alle altre e ai relativi sistemi di gestione.

"**Trattare**", "**trattato**" o "**trattamento**", "**allegato sul trattamento**" e "**dati personali**": avranno i significati a loro attribuiti nella clausola "**Protezione dei dati personali**".

"**Incidente di sicurezza rilevante**": una lacuna, effettiva o presunta, nella sicurezza dei sistemi o dei servizi, ed eventi relativi alla sicurezza che incidono sulle forniture o sull'esecuzione del contratto (ad esempio, perdita, danno, sottrazione o uso improprio, effettivo o presunto, delle informazioni o dei sistemi di BT). Ciò include, senza intento limitativo:

- perdite relative al servizio, all'apparecchiatura o alle strutture;
- corruzione, danneggiamento o uso improprio dei beni materiali di BT;
- guasti o sovraccarichi dei sistemi;
- errori umani;
- inadempienze relative ai requisiti di sicurezza illustrati nel presente documento;
- violazioni delle disposizioni relative alla sicurezza fisica;
- modifiche incontrollate ai sistemi;

- guasti del software o hardware;
- violazioni dell'accesso: e
- perdite di dati, effettive o presunte, relative ai sistemi associati a BT e alle connessioni tra BT e il fornitore.

"**Accesso remoto**": l'accesso remoto effettuato da casa o da un altro luogo mediante una rete pubblica (ad esempio, internet) oppure l'accesso remoto della rete del fornitore a un sistema di BT.
"**Requisiti di sicurezza**": si riferisce ai presenti requisiti di sicurezza di BT, come debitamente aggiornati di volta in volta.
"**Forniture**": indicherà tutti i "**servizi**", le "**forniture**", i "**beni**" e i "**lavori**" indicati nel contratto e ogni esecuzione del contratto stesso.
"**Sistemi del fornitore**": qualsiasi computer, applicazione o sistema di rete di proprietà del fornitore utilizzato per accedere a, archiviare o trattare informazioni di BT o utilizzato per l'erogazione delle forniture.
"**Referente per la sicurezza del fornitore**": la persona i cui estremi di contatto verranno comunicati di volta in volta dal fornitore a BT e che sarà il referente unico per ogni questione attinente ai presenti requisiti della sicurezza e a qualsiasi incidente di sicurezza rilevante.
"**Trasferimento**" o "**trasferito**": lo spostamento delle informazioni di 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 la concessione dell'accesso alle informazioni di BT in possesso del personale temporaneo (inclusi, senza intento limitativo, i dati personali) da parte di un luogo o di un individuo a un altro, tramite sistema fisico, vocale o elettronico.
"**Specifiche per la classificazione e il trattamento delle informazioni di terze parti**" indica i requisiti relativi alla gestione delle informazioni da parte del fornitore indicati in https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm compresi gli aggiornamenti.