Standard per i Call Centre

Condizioni generali

(A) I presenti Requisiti dovrebbero essere letti insieme alla Matrice di Implementazione (Appendice 1) del presente documento, che fornisce ulteriori dettagli sui comportamenti e i risultati che BT riterrà generalmente accettabili nel considerare la conformità del Fornitore con i Requisiti.

(B) BT può effettuare valutazioni del rischio per il Contact Centre come stabilito nella sezione 3.10 dei Requisiti di sicurezza per i fornitori di BT (i "Requisiti di sicurezza") in qualsiasi momento, sia prima che durante la fornitura dei servizi. Fatto salvo qualsiasi altro rimedio a disposizione di BT, BT può stipulare azioni correttive, controlli compensativi e contromisure per far fronte a eventuali rischi individuati e/o in caso di insoddisfazione o non conformità con tali Requisiti, che dovranno essere implementati dal Fornitore e documentati sotto forma di appendice al presente Standard; eventuali costi associati all'implementazione dei nuovi requisiti di sicurezza devono essere concordati da entrambe le parti.

(C) BT avrà il diritto di revisionare su richiesta le politiche e le procedure del Fornitore che soddisfano i Requisiti del presente Standard nell'ambito della valutazione dei rischi per il Contact Centre. Tali politiche includono, a titolo esemplificativo ma non esaustivo: Utilizzo dei computer, Smaltimento dei supporti informatici, Autenticazione del cliente, Controlli preliminari all'assunzione, Valutazione dei rischi e Procedimento di gestione, ecc.

1. Sicurezza fisica

1.1 Il Fornitore deve garantire che le aree del Contact Centre (vedi Glossario) utilizzate per la gestione dell'Account di BT/EE siano Fisicamente separate da tutte le altre aree mediante Controlli degli accessi fisici specifici.

1.2 Il Fornitore deve implementare un procedimento verificabile mediante audit per gli accessi in modo da poter richiedere, approvare oppure eliminare un accesso fisico all'area del Contact Centre. [1]

1.3 Per controllare il diritto di accesso fisico alle aree del Contact Center (inclusi cambiamenti e spostamenti interni) e nell'ambito del "procedimento di cessazione di servizio", il Fornitore deve garantire la revisione del procedimento verificabile mediante audit ogni (3) mesi e la registrazione della data di ogni revisione.

1.4 Il Fornitore deve garantire che non venga svolto alcun Lavoro isolato nell'area del Contact Centre. Questo requisito include gli addetti alle pulizie e i dipendenti di terzi.

1.5 Il Fornitore deve predisporre un procedimento verificabile tramite audit che impedisca episodi di tailgating attraverso le porte e/o barriere di accesso controllate. Tale procedimento dovrebbe essere adottato e casi ripetuti di infrazione saranno soggetti ad azioni disciplinari.

2. Pass di sicurezza e visitatori

2.1 Il Fornitore deve fare in modo che i dipendenti cui è permesso (nell'ambito del loro ruolo lavorativo) portare con sé e utilizzare telefoni cellulari, laptop, iPad e/o tablet all'interno dell'area del Contact Centre siano facilmente riconoscibili dagli altri dipendenti e supervisori.[2]

[1] Consultare la Matrice di implementazione per esempi di procedimenti di accesso verificabili mediante audit.
[2] Consultare la Matrice di implementazione per esempi di cosa si intende con "facilmente riconoscibili".

2.2 Il Fornitore deve implementare un procedimento verificabile tramite audit per il rilascio e la gestione di Pass di sicurezza e Pass di sicurezza temporanei in modo da poter contattare i dipendenti del Contact Centre quando necessario; deve essere prevista anche la cancellazione automatica del diritto di accesso allo scadere del periodo di tempo per cui il pass viene richiesto.

2.3 Il Fornitore deve garantire che i pass di sicurezza e i cordini non indichino il posto di lavoro dei dipendenti.

2.4 Il Fornitore deve garantire l'implementazione di un procedimento per i visitatori verificabile tramite audit, che sia accessibile da tutti i dipendenti. Come prova, si deve tenere un registro dei visitatori.[3]

2.5 I pass di sicurezza rilasciati ai visitatori devono differenziarli dai dipendenti e devono essere ritirati quando il visitatore lascia il Contact Centre; i pass di sicurezza che non vengono restituiti immediatamente non saranno più validi dal giorno lavorativo seguente.

2.6 Il Fornitore deve garantire che i visitatori al Contact Centre siano costantemente accompagnati e indossino appositi pass/badge visibili.

3. Dipendenti

3.1 Il Fornitore deve garantire che tutti gli Oggetti personali (inclusi i dispositivi mobili) siano custoditi in Appositi armadietti lontani dall'area del Contact Centre.

3.2 Il Fornitore deve consentire l'introduzione all'interno dell'area del Contact Centre di medicinali/attrezzature mediche di base personali indispensabili come inalatori, insulina o prodotti antitosse.

3.3 Salvo in caso di autorizzazione a seguito di una valutazione dei rischi, il personale che lavora all'interno dell'area del Contact Centre non può portare con sé cellulari o dispositivi mobili senza autorizzazione. Il Fornitore deve implementare controlli a campione periodici di osservazione del personale per garantire che cellulari o dispositivi mobili non siano introdotti nell'area del Contact Centre e deve predisporre appositi cartelli che proibiscono l'uso di tali dispositivi. Inoltre, nei programmi di formazione per la sensibilizzazione alla sicurezza si dovrebbe indicare chiaramente questo requisito; in caso di inadempienza è previsto un procedimento disciplinare.

3.4 Il Fornitore deve garantire l'implementazione di una procedura per consentire agli esterni di contattare i dipendenti in caso di un'emergenza personale.[4]

3.5 Deve essere previsto un procedimento verificabile tramite audit per l'autorizzazione e l'utilizzo di penne, matite e carta all'interno dell'area del Contact Centre. Penne, matite e carta non sono consentiti a meno che i dipendenti non siano espressamente autorizzati dal loro Responsabile, nell'ambito del loro ruolo lavorativo.

3.6 Il Fornitore deve garantire che, se prodotto nell'ambito del ruolo lavorativo di un dipendente, qualsiasi appunto scritto non sia lasciato incustodito e sia archiviato (così come per la gestione

[3] Consultare la Matrice di implementazione per le informazioni che devono essere contenute nel Registro dei visitatori.
[4] Consultare la Matrice di implementazione per esempi di procedure di emergenza personale.

e classificazione delle informazioni) o smaltito [5] in modo sicuro alla fine della giornata lavorativa per attuare una politica della scrivania pulita[6].

http://www.selling2bt.bt.com/working/ThirdPartySecuritystandards/index.htm

3.7 Per prendere appunti durante le chiamate, il Fornitore deve predisporre lavagne bianche e blocchi cancellabili (inclusi penne lavabili e panni) come alternativa a penne, matite e carta. Il Fornitore deve garantire che questi appunti vengano cancellati alla conclusione della richiesta del cliente ed eliminati dalle lavagne bianche alla fine del turno di ogni consulente. I Responsabili e i supervisori devono supervisionare l'area ed effettuare controlli a campione per garantire la conformità con questo requisito.

3.8 Il Fornitore deve garantire che tutti gli appunti temporanei registrati online o in strumenti elettronici (per supportare le chiamate dei clienti) sia cancellato automaticamente alla fine del turno di ogni consulente o alla fine della giornata lavorativa. Ciò deve avvenire in modo automatico oppure è necessario conservare un report giornaliero per garantire la conformità con questo requisito.

3.9 Il Fornitore deve predisporre un procedimento verificabile tramite audit per l'utilizzo di lavagne bianche/documenti cartacei al fine di garantire che:

- qualsiasi documento cartaceo sia archiviato o eliminato e smaltito in modo sicuro alla fine di ogni giornata lavorativa; e
- le lavagne bianche siano pulite alla fine di ogni turno e alla fine della giornata lavorativa.[7]

3.10 Il Fornitore deve fare in modo che tutte le interazioni con i clienti siano registrate nell'Account (memo o blocco-note a seconda del sistema usato).

3.11 Il Fornitore deve garantire che le interazioni con i clienti non vengano registrate in alcuna applicazione Microsoft Office a meno che i dipendenti non siano espressamente autorizzati tramite una valutazione dei rischi, nell'ambito del loro ruolo lavorativo.

3.12 Il Fornitore deve garantire che qualsiasi ruolo autorizzato ad eseguire una delle seguenti attività all'interno dell'area del Contact Centre sia sottoposto a una valutazione dei rischi secondo i requisiti di cui alla sezione 11. Le attività includono, a titolo esemplificativo ma non esaustivo:

- Utilizzo di applicazioni di Microsoft Office
- Utilizzo di dispositivi mobili aziendali
- Utilizzo di laptop aziendali
- Utilizzo di oggetti personali (vedi Glossario)
- Possibilità di stampare o copiare le informazioni relative al clienti
- Possibilità di scaricare le registrazioni delle chiamate da uno o più server che registrano le chiamate

[5] Consultare la Matrice di implementazione per esempi di archiviazione e smaltimento sicuri.
[6] Consultare la Matrice di implementazione per esempi di cosa dovrebbe includere la politica della scrivania pulita.
[7] Consultare la Matrice di implementazione per esempi di cosa dovrebbe comprendere un audit delle lavagne bianche/dei documenti cartacei.

- Accesso a e-mail interne ed esterne o ad altri strumenti di comunicazione come ad es. strumenti di messaggistica istantanea
- Utilizzo di penne/matite e carta per prendere appunti
- Invio di messaggi di testo multipli ai clienti
- Accesso remoto all'attrezzatura del cliente

3.13 Il Fornitore deve garantire che non sia permesso inviare messaggi di testo multipli (un messaggio di testo a più clienti), a meno che i dipendenti non siano espressamente autorizzati nell'ambito del loro ruolo lavorativo. Nel caso in cui ciò avvenga, è necessario conservare i report che attestino quando ciò si è verificato, il/i destinatario/i e i motivi dell'invio.

3.14 Il Fornitore deve garantire che non sia permesso né sia possibile scaricare le registrazioni delle chiamate da uno o più server che registrano le chiamate a meno che il soggetto non sia espressamente autorizzato nell'ambito del suo ruolo lavorativo. In caso di autorizzazione, è necessario conservare un report che attesti chi è autorizzato ad eseguire questa funzione; se si scaricano tutte le registrazioni, è necessario conservare i report che attestano perché ciò si è verificato, quali chiamate sono state effettivamente scaricate e i motivi. È necessario riesaminare periodicamente la validità dei consulenti autorizzati e dei casi di non conformità.

4. Attrezzatura

4.1 Il Fornitore deve garantire che gli schermi dei computer di tutti i consulenti siano protetti e non siano visibili dall'esterno dell'area separata del Contact Centre.[8]

4.2 Il Fornitore deve garantire che le stampanti e i fax siano posizionati in aree sicure con accesso limitato solo al personale autorizzato e che siano utilizzati solo per scopi strettamente necessari. Al fine di garantirne continuamente la validità, è necessario riesaminare periodicamente l'elenco degli utenti autorizzati e l'utilizzo delle attrezzature. Eventuali copie cartacee dovrebbero essere archiviate in modo sicuro in base allo Standard sulla classificazione e il trattamento delle informazioni e non devono essere eliminate dal Contact Centre fatta salva autorizzazione da parte di BT.

4.3 Il Fornitore deve garantire che per effettuare operazioni di stampa e copia sia necessario inserire un ID utente e un codice di sicurezza in modo che tutte le stampe siano monitorate e registrate ai fini dell'audit.

4.4 Il Fornitore deve garantire che nelle aree in cui sono posizionati fax e stampanti, siano presenti distruggidocumenti di tipo cross-cut e cestini per rifiuti di tipo riservato. I distruggidocumenti e i cestini devono essere svuotati periodicamente e il contenuto deve essere smaltito in modo sicuro.

4.5 Il Fornitore deve garantire che tutti i documenti cartacei siano smaltiti in modo sicuro, distruggendoli per mezzo del distruggidocumenti o gettandoli negli appositi cestini per rifiuti di tipo riservato ai sensi della sezione 4.4.

4.6 Il Fornitore deve garantire che tutte le Risorse fisiche assegnate a ciascun individuo all'inizio del lavoro siano recuperate/eliminate prima del termine del lavoro all'interno dell'area del Contact Centre oppure quando termina il contratto di BT/EE; è necessario conservare un inventario delle Risorse fisiche.[9]

[8] Consultare la Matrice di implementazione per esempi di cosa si intende con 'schermi dei computer protetti'.
[9] Consultare la Matrice di implementazione per esempi di cosa includere nell'inventario delle Risorse fisiche.

4.7 Il Fornitore deve garantire che tutte le Risorse fisiche che vengono recuperate o eliminate siano smaltite in modo sicuro e in conformità con i requisiti relativi allo smaltimento sicuro.[10]

5. Accesso ai sistemi

5.1 Al fine di proteggere i dati relativi ai clienti, tutti i consulenti devono registrare i propri ID utente quando accedono a un account/report del cliente insieme al motivo di tale accesso. L'accesso viene concesso solo previa approvazione da parte del Proprietario del sistema o del responsabile di linea. Inoltre, l'accesso agli account dei clienti deve essere concesso solo se è richiesto per il ruolo del consulente e deve essere impostato al livello minimo necessario affinché egli possa svolgere la propria funzione. L'accesso non deve essere consentito, per nessun motivo, a chiunque non necessiti di accedere al sistema di BT e/o EE per visualizzare i report relativi ai clienti.

5.2 Salvo quando necessario per motivi operativi, evitare l'accesso in modalità 'solo visualizzazione'. È necessario registrare e monitorare ogni accesso autorizzato in modalità 'solo visualizzazione' al fine di prevenire usi impropri.

5.3 Il Fornitore deve garantire che ai dipendenti non sia concesso accedere a Internet, alle e-mail personali o esterne, a social media (come Facebook) o ad altri strumenti di comunicazione come Messenger o Communicator a meno che non siano autorizzati da BT oppure sia necessario nell'ambito del loro ruolo lavorativo.

5.4 Il Fornitore deve garantire che tutti i messaggi di testo inviati dai sistemi del fornitore siano registrati e monitorati. Nel caso in cui vengano inviati messaggi di testo, è necessario conservare un report che attesti quando ciò si è verificato, il/i destinatario/i e i motivi dell'invio.

5.5 Il Fornitore deve garantire che siano concessi solo strumenti di accesso remoto precedentemente approvati, usati per accedere ai dispositivi dei clienti per scopi di assistenza e che tali strumenti siano limitati al personale a cui servono per lo svolgimento del suo lavoro. Gli accessi dovrebbero essere riesaminati ogni 3 mesi e ogni accesso non più necessario per svolgere il lavoro dovrebbero essere revocato. Devono essere previste soluzioni specifiche per identificare gli strumenti di accesso remoto non approvati.[11]

5.6 Il Fornitore non deve consentire l'accesso remoto alle e-mail lavorative dei dipendenti del Contact Centre e non deve permettere ad alcun sistema di accedere ai report relativi ai clienti.

5.7 Il Fornitore deve garantire che ai dipendenti sia concesso l'accesso in modalità 'sola visualizzazione' solo a unità condivise fornite e gestite da BT e/o EE. All'interno del Contact Centre non devono essere utilizzate unità condivise. Non è permesso scaricare, copiare, eliminare o modificare le informazioni relative ai clienti dai sistemi, dalle applicazioni o dai database di BT e/o EE.

[10] Consultare la Matrice di implementazione per un esempio di cosa dovrebbero includere i requisiti relativi allo smaltimento sicuro.

[11] Consultare la Matrice di implementazione per esempi di comportamenti atti a identificare gli strumenti di accesso remoto.

6. Registrazioni delle chiamate

6.1 Il Fornitore deve garantire che tutte le chiamate dei clienti vengano registrate. Il Fornitore deve garantire che le registrazioni (vocali e visive) delle chiamate siano protette durante la trasmissione dal PC desktop all'uno o più server di registrazione delle chiamate.[12]

6.2 Il Fornitore deve garantire che le registrazioni delle chiamate siano archiviate in modo sicuro, in particolare se includono dati di carte di pagamento (PCI) al fine di prevenire la perdita o l'uso improprio di questi dati del cliente. I dati PCI devono essere criptati e deve essere prevista una soluzione di gestione delle chiavi per proteggerli secondo le migliori prassi del settore. BT e/o EE possono occasionalmente revisionare la crittografia e le soluzioni di archiviazione protetta per valutare che siano adeguate e appropriate.

7. Autenticazione del cliente

7.1 Il Fornitore deve garantire un procedimento di autenticazione del cliente approvato per le chiamate in entrata e in uscita. [13]

7.2 Il Fornitore deve garantire che i pin o le password utilizzati dai clienti per autenticarsi non siano visibili ad altri dipendenti del Contact Centre, per esempio tramite l'uso di schermi di computer protetti o separazione fisica.

7.3 Il Fornitore deve garantire che l'autenticazione del cliente sia automatizzata in modo tale che il cliente non debba rivelare il proprio pin o password per intero al consulente, ad esempio tramite una richiesta generata dal sistema di inserire cifre/lettere causali nella password ad es. in prima, terza e quinta posizione. BT e/o EE possono riesaminare occasionalmente il procedimento di autenticazione del cliente per garantire la conformità con i presenti Requisiti.

7.4 Il Fornitore deve garantire che, nel caso in cui un cliente abbia dimenticato il pin o la password e debba resettarli, il reset sia possibile solo dopo che il cliente ha superato correttamente controlli di autenticazione aggiuntivi.[14]

7.5 Il Fornitore deve garantire che i sistemi per impostare il pin o la password dell'account di un cliente siano automatizzati e non richiedano alcuna interazione da parte di un dipendente del Contact Centre.

7.6 Il Fornitore deve garantire che la creazione di nuovi pin o password sia generata da un sistema automatizzato e che ogni nuovo pin o password sia inviato direttamente al cliente tramite messaggio o e-mail, senza l'intervento del consulente.

7.7 Il Fornitore deve garantire che i clienti possano resettare pin o password sia online sia tramite un sistema di risposta vocale interattiva (IVR).

7.8 Il Fornitore deve garantire che esista una struttura per il "reset assistito da un dipendente" che consenta al cliente di resettare pin o password con l'assistenza di un dipendente del

[12] Consultare la Matrice di implementazione per esempi di protezione della trasmissione delle registrazioni delle chiamate.
[13] Consultare la Matrice di implementazione per esempi di cosa dovrebbe includere il procedimento di autenticazione del cliente.
[14] Consultare la Matrice di implementazione per esempi di cosa dovrebbero includere i controlli di autenticazione aggiuntivi.

Contact Centre. La possibilità di resettare pin o password deve essere limitata a un numero ristretto di dipendenti.[15]

7.9 Il Fornitore deve esser in grado di generare, su richiesta, un audit trail che mostri le operazioni di reset di pin e password del cliente, il sistema usato (online, IVR, assistenza di un dipendente) e quale dipendente è stato coinvolto in questa transazione.

8. Data Privacy

Oltre alla formazione obbligatoria di BT sulla Sicurezza e protezione dei dati (vedi Allegato 2) che tutti i dipendenti devono seguire e dichiarare di aver compreso, devono essere rispettati anche i seguenti requisiti:

8.1 Il Fornitore deve garantire che i dipendenti all'interno dell'area del Contact Centre possano accedere facilmente alle informazioni relative alla sicurezza e alla protezione dei dati, pertinenti e applicabili, dalla pagina principale della Homepage della loro rete intranet (oppure, nel caso non abbiano l'intranet, tramite e-mail periodiche di aggiornamento e formazione).

8.2 Il Fornitore deve fornire promemoria periodici, al meno due volte all'anno, a tutti i dipendenti all'interno dell'area del Contact Centre al fine di rafforzare i comportamenti positivi e supportare le best practice in materia di sicurezza.

9. Monitoraggio

9.1 Il Fornitore deve fare in modo che i supervisori/responsabili eseguano settimanalmente un "controllo qualità" del monitoraggio delle chiamate su una selezione casuale di chiamate del cliente (in entrata e in uscita) al fine di garantire, tra gli altri requisiti, che venga utilizzato il procedimento di autenticazione del cliente corretto.[16]

9.2 Nel caso non sia stato seguito il corretto procedimento di autenticazione del cliente, il Fornitore deve garantire che le chiamate siano considerate "chiamate fallite". Per ogni chiamata fallita, il Fornitore dovrebbe implementare un procedimento di feedback per ricordare ai consulenti del Contact Centre che sono responsabili della corretta autenticazione dei clienti e della protezione delle password (a seconda dei casi).

9.3 Il Fornitore deve predisporre un procedimento verificabile tramite audit nel caso che un dipendente del Contact Centre produca ripetutamente "chiamate fallite" e non sia stato in grado di eseguire il procedimento di autenticazione del cliente corretto. Questo dovrebbe includere le conseguenze di un ripetuto errore di autenticazione del cliente o di gestione di report da parte di un consulente e può essere usato come prova per procedure disciplinari o di controllo delle prestazioni dei soggetti interessati.

10. Conformità

10.1 Il Fornitore deve garantire che esista un procedimento verificabile tramite audit documentato per effettuare e gestire controlli di conformità locali periodici in materia di sicurezza e/o controlli a campione di conformità per verificare la conformità con il presente Standard e i

[15] Consultare la Matrice di implementazione per esempi di cosa dovrebbe includere una struttura per il "reset assistito da un dipendente".

[16] Consultare la Matrice di implementazione per esempi di cosa deve essere incluso, come minimo, in un controllo qualità.

Requisiti di sicurezza di BT ad esempio supervisione dell'area, politica della scrivania pulita, ecc.[17]

10.2 Il Fornitore deve implementare un procedimento al fine di garantire che, trimestralmente, vengano eseguite revisioni sulla base delle prove (basate sul 10% dei neo-assunti) sui dipendenti del Contact Centre o su qualsiasi soggetto che lavora nell'ambito di contratti BT e/o EE, al fine di garantire che il procedimento di selezione preliminare all'assunzione e la formazione in materia di sicurezza (come parte del procedimento di reclutamento) siano completati e funzionino in modo efficace. Questo al fine di garantire che il background dei dipendenti che lavorano all'interno dell'area del Contact Centre sia stato adeguatamente controllato (in linea con la politica di controlli preliminari all'assunzione) e che essi abbiano preso parte alla formazione in materia di sicurezza per esser certi che le informazioni sensibili dei clienti siano protette in modo adeguato.

10.3 Il Fornitore deve implementare un procedimento al fine di garantire che, trimestralmente, vengano eseguite revisioni sulla base delle prove (basate sul 100% dei neo-assunti) sui dipendenti del Contact Centre o su qualsiasi soggetto che lavora nell'ambito di contratti BT e/o EE, al fine di garantire il completamento della formazione annuale obbligatoria in materia di sicurezza e protezione dei dati.

10.4 Il Fornitore deve garantire che vengano svolti corsi di aggiornamento trimestrali sugli obblighi dei dipendenti in materia di sicurezza e protezione dei dati e che la partecipazione dei dipendenti e la comprensione dei contenuti vengano documentate.

10.5 Il Fornitore deve garantire che i dipendenti del Contact Centre possano accedere alle politiche, agli standard, alle linee guida e ai procedimenti pertinenti al fine di garantire la conformità con il presente Standard e con i Requisiti di sicurezza di BT.

11. Valutazione dei rischi

Il Fornitore deve garantire che eventuali non conformità, autorizzazioni o eccezioni specifiche a questi requisiti siano sottoposte a una valutazione dei rischi da perte del fornitore e documentate secondo il procedimento di gestione dei rischi. La valutazione dei rischi deve includere:

- il motivo per cui l'attività è richiesta, e perché eventuali non conformità rispetto a questi Requisiti sono giustificabili;
- lo stato di eventuali non conformità ad es. permanente o temporanea;
- se temporanea, la data entro cui verranno effettuati i controlli e la data in cui l'attività verrà completata;
- funzione/ruolo dei soggetti e perché l'attività è adeguata a questo ruolo (e perché sono esclusi dal rispettare i controlli);
- svolgimento di controlli per minimizzare i rischi derivanti dall'attività;
- giustificazione per l'implementazione di determinati controlli e/o per la mancata implementazione dei controlli necessari; e
- prova dell'autorizzazione dei massimi dirigenti.

[17] Consultare la Matrice di implementazione per esempi di cosa dovrebbero includere i controlli a campione di conformità.

12. Glossario

Termine	Spiegazione
Customer Contact Centre	Un Contact Centre (chiamato anche Customer Interaction Centre o E-Contact Centre) rappresenta un punto centrale di un'azienda dal quale vengono gestiti tutti i contatti con i clienti. Il Contact Centre include solitamente uno o più call centre online ma può includere anche altre metodologie di contatto clienti, tra cui newsletter via e-mail, cataloghi tramite posta, richieste e chat tramite sito web e raccolta di informazioni dai clienti in caso di acquisto in negozio. In un'azienda, il Contact Centre rientra generalmente nella gestione della relazione con la clientela (Customer Relationship Management, CRM).
Appositi armadietti	Il personale che lavora nell'area del Contact Centre non può portare con sé alla propria postazione lavorativa oggetti personali in grado di registrare informazioni sui clienti, come i telefoni cellulari, che devono essere chiusi con lucchetto in appositi armadietti personali (indicati come tali) lontani dall'area del Contact Centre.
Dipendente(i)	Il termine "dipendente" indica ogni soggetto che lavora all'interno dell'area del Contact Centre inclusi i dipendenti a tempo indeterminato e determinato del Fornitore, i lavoratori interinali, i lavoratori autonomi e gli operai.
Accompagnato/i	In caso di visite, deve essere previsto un procedimento formale che garantisca, come minimo, che i visitatori al Contact Centre siano sempre accompagnati al fine di evitare che si perdano o che accedano ad aree in cui non sono ammessi.
Matrice di implementazione	La matrice allegata che stabilisce, come minimo, i risultati e gli standard che il Fornitore deve ottenere nell'implementazione di determinati procedimenti, politiche o procedure cui si fa riferimento nei Requisiti.
Lavoro isolato	Deve essere previsto un procedimento che impedisca l'esecuzione di lavori isolati individuali all'interno dell'area del Contact Centre al di fuori dell'orario lavorativo normale, senza autorizzazione della direzione. Ciò vale per il personale addetto alle pulizie e per tutti coloro che non appartengono all'azienda come i manutentori.
Applicazioni Microsoft Office	Le Applicazioni Microsoft Office includono, a titolo esemplificativo ma non esaustivo: Word, PowerPoint, Excel, Outlook e OneNote. Al fine di prevenire la perdita di dati, le interazioni con i clienti che includono sistemi online non devono essere registrate su tali applicazioni (salvo autorizzazione) poiché le informazioni contenute in tali applicazioni possono essere facilmente copiate ed estrapolate.
Oggetti personali	Qualsiasi oggetto che può essere usato per fotografare/registrare le informazioni dei clienti inclusi, a titolo esemplificativo ma non esaustivo: iPod, iPad, macchine fotografiche, flash drive USB, penne e carta.
Controlli degli accessi fisici	I metodi di controllo degli accessi fisici utilizzati dipenderanno dall'area in cui si trova il Contact Centre. I metodi di controllo degli accessi fisici possono essere tecnici (ad es. tesserini, tastiere, biometrica) o procedurali (ad es. chiavi con un procedimento di uscita verificabile mediante audit o un procedimento di entrata

	in cui il personale addetto verifica l'ID). Tuttavia, i controlli degli accessi fisici utilizzati devono essere adeguati all'area interessata.
Risorse fisiche	Ai fini del presente documento, con risorsa fisica si intende qualsiasi risorsa che elabora o archivia informazioni o dati relativi ai clienti.
Fisicamente separate	Ai fini del presente documento, con fisicamente separate si intende che da altre aree lavorative non deve essere possibile sentire alcuna conversazione né vedere alcuna informazione. A tal fine deve essere prevista una barriera fisica (muri, edifici separati, ecc.) con controlli fisici all'entrata.
Problema di sicurezza	Un problema di sicurezza è un cambiamento nelle attività aziendali di routine che ha un impatto sulla riservatezza, l'integrità o la disponibilità delle risorse informatiche e che indica una violazione della politica di sicurezza o dei requisiti/norme di sicurezza oppure che una delle misure di sicurezza adottate non ha funzionato. Ecco alcuni esempi: Uso improprio del sistema, Accesso non autorizzato, Furto/perdita di attrezzature e Infezione causate da malware.
Autorizzazione dei massimi dirigenti	Laddove è necessaria un'eccezione a tali requisiti, occorre fare una valutazione dei rischi e l'approvazione può essere fornita solo da chi è responsabile della gestione dell'area funzionale e ha l'autorità richiesta.
Proprietario del sistema	Indica il responsabile ufficiale per l'acquisto, lo sviluppo, l'integrazione, le modifiche, o il funzionamento e la manutenzione di un sistema informatico.
Tailgating	Consiste nel seguire un utente o nel consentire l'accesso a personale non autorizzato attraverso un porta/barriera o gate di accesso controllati per accedere a un'area; non usare il proprio pass di sicurezza per accedere a un'area autorizzata nella sede del Fornitore in cui vengono eseguiti i contratti BT/EE.
Pass di sicurezza temporanei	Questi devono essere rilasciati nell'ambito di un procedimento verificabile tramite audit (come un libro, un registro o un foglio elettronico); si deve registrare ogni rilascio di pass di sicurezza temporaneo, così come la data di emissione, il nome, il dipartimento, il numero di contatto, il motivo del rilascio, il nome dell'ospitante e la data in cui il pass temporaneo viene restituito. Deve essere previsto un procedimento specifico per le tessere che non vengono restituite.
ID utente	Per utilizzare le stampanti e i fax che si trovano all'interno dell'area del Contact Centre, ogni utente deve inserire un codice ID e un codice di sicurezza unici al fine di monitorarne l'utilizzo su base individuale. Inoltre, i dipendenti devono inserire questo ID unico quando devono accedere agli account/report dei clienti, secondo quanto stabilito nella sezione 5.1.

PROJECT KITE: Matrice di implementazione per i requisiti dei Contact Centre per i fornitori.

Riferimento	Descrizione generale	Risultati minimi probabilmente considerati conformi.
1.2	Procedimento per gli accessi verificabile tramite audit	Un foglio di calcolo o un data log con i nomi, inclusi i dettagli su quando l'accesso è stato concesso, il motivo per cui tale accesso è stato concesso, la data di eliminazione dell'accesso e il motivo di tale annullamento.
2.1	Facilmente riconoscibile/i	Il personale cui è concesso utilizzare cellulari, laptop, iPad, tablet nell'ambito del loro ruolo lavorativo deve essere facilmente riconoscibile ad esempio per mezzo di cordini di colori differenti o altri mezzi di identificazione distinguibili.
2.4	Registro dei visitatori	Dovrebbero essere registrate le seguenti informazioni: i) nome del soggetto, ii) organizzazione di appartenenza, iii) data e ora di ingresso e di uscita, iv) scopo della visita, v) nome della persona che riceve la visita, vi) numero di registrazione di ogni veicolo portato sul luogo, vii) numero di cellulare, viii) numero di identificazione del pass visitatore.
3.5	Emergenza personale	In caso di emergenza personale, deve essere previsto un sistema che consenta a familiari e amici di contattare il dipendente. Questo sistema di contatto potrebbe prevedere un numero di centralino dedicato o il numero di un supervisore da usare come punto di contatto centrale.
3.7	Archiviato o smaltito in modo sicuro	Laddove nell'ambito del ruolo lavorativo di un dipendente vengano prodotti appunti, esempi di archiviazione o smaltimento sicuri includono, a titolo esemplificativo ma non esaustivo, l'uso di distruggidocumenti, cestini per rifiuti di tipo riservato (possibilmente chiusi con lucchetto) e /o archiviazione all'interno di apposite strutture che possono essere chiuse con lucchetto dai dipendenti.
3.7	Politica della scrivania pulita	Tutti i materiali dovrebbero essere archiviati o smaltiti in modo sicuro immediatamente dopo l'uso e nessun materiale dovrebbe essere lasciato sulla scrivania alla fine della giornata lavorativa. Occorre implementare Controlli a campione periodici di osservazione del personale e deve essere previsto un procedimento disciplinare per gestire le non conformità.

3.10	Audit per lavagne bianche/carta	In relazione ai procedimenti di cui alla sezione 3, occorre tenere un report (ad esempio sotto forma di foglio di calcolo) per dimostrare l'esecuzione di controlli a campione e garantire la conformità con i requisiti.
4.1	Schermi di computer protetti	Gli schermi dei consulenti non devono essere visibili all'interno dell'ambiente del Contact Centre e le informazioni non devono poter essere lette da personale non autorizzato all'interno del Contact Centre (come personale addetto alle pulizie o alla manutenzione). I dati dei clienti sugli schermi dei computer devono essere tenuti nascosti posizionando il monitor in modo adeguato oppure tramite l'uso di appositi schermi di protezione.
4.6	Inventario delle Risorse fisiche	Ai fini dell'audit, occorre tenere un inventario delle Risorse fisiche e degli altri oggetti assegnati ai soggetti come pass di sicurezza, chiavi degli armadietti, laptop, desktop o token di accesso remoto. Quando un consulente cessa il suo servizio oppure viene spostato dal Contact Centre, devono essere previsti dei procedimenti per garantiscono l'adozione immediata di misure atte a eliminare tutti gli accessi logici e fisici e a recuperare eventuali Risorse fisiche, chiavi e pass di sicurezza. Questa deve essere una delle procedure da effettuare da coloro che cessano il servizio.
4.7	Requisiti relativi allo smaltimento sicuro	Quando le Risorse fisiche vengono smaltite alla fine della loro vita utile, occorre usare un software proprietario come 'Tabernus' o 'Blanco' per garantire che tutte le informazioni riservate o dei clienti vengano cancellate dall'attrezzatura in modo permanente (se pertinente) ai sensi dello Standard approvato da BT e/o EE. Se non è possibile effettuare un'eliminazione sicura dei dati utilizzando questo software, allora è necessario distruggere l'attrezzatura in modo sicuro con un procedimento approvato da BT e/o EE. Il contatto di sicurezza di BT e/o EE può fornire ulteriore assistenza. Dopo aver eliminato tutte le informazioni riservate o del cliente, le Risorse fisiche possono essere riutilizzate altrove oppure smaltite, a seconda del caso.
5.5	Strumenti di accesso remoto	Al fine di prevenire accessi non autorizzati ai dati dei clienti, occorre implementare dei procedimenti formali per garantire che solo gli strumenti di accesso remoto che sono stati precedentemente approvati da BT e/o EE possano accedere ai dispositivi del cliente. Occorre implementare soluzioni adeguate per identificare strumenti di accesso remoto non autorizzati; tali soluzioni devono essere riesaminate periodicamente al fine di garantire che strumenti non autorizzati non possano essere e non siano stati utilizzati. Inoltre, l'uso di strumenti di accesso remoto approvati deve essere limitato a personale autorizzato; tale autorizzazione viene ottenuta solo tramite un procedimento formale che include una

		valutazione dei rischi della necessità dell'accesso remoto.
6.1	Trasmissione delle registrazioni delle chiamate	È necessario criptare le registrazioni delle chiamate dei clienti dal PC ai server di registrazione delle chiamate e tale crittografia deve includere sia le registrazioni vocali sia i dettagli visivi.
7.1	Autenticazione del cliente	Tutti i consulenti devono seguire il procedimento di autenticazione del cliente così come approvato da BT/EE per garantire che il cliente sia la persona che sostiene di essere. Questo procedimento verrà comunicato ai Fornitori e ai consulenti e può differire a seconda della/e funzione/ fornita/e dal Contact Centre.
7.4	Controlli di autenticazione aggiuntivi	I consulenti devono garantire, prima di procedere alla modifica del PIN o della password del cliente, di accertarsi inoltre di ricavare dal cliente informazioni sufficienti al fine di verificare loro stessi che la persona è chi dice di essere ponendo alcune domande di sicurezza sulla sua identità, sul nome e sull'indirizzo, come ad esempio quale attività recente è stata svolta nel suo account, l'importo dell'ultima fatturazione o da quanto tempo è cliente di BT o EE. Tuttavia, questi sono solo alcuni degli esempi e l'elenco non è esaustivo.
7.8	Reset assistito da un dipendente	Al fine di facilitare i clienti che non sono in grado d resettare il proprio PIN o password online oppure tramite IVR, deve essere possibile semplificare queste operazioni di reset grazie all'assistenza di un dipendente del call centre. Tuttavia, deve esistere un procedimento formale atto a garantire che la struttura per il "reset assistito da un dipendente" sia limitata a un numero ristretto di dipendenti, e che vengano implementate le dovute misure di protezione per garantire che ogni dipendente con la facoltà di resettare PIN e password del cliente sia fisicamente separato dagli altri all'interno del Contact Centre e che siano effettuati i dovuti controlli. È necessario riesaminare periodicamente l'elenco di coloro che possono fornire l'approvazione al fine di garantire che l'approvazione sia ancora necessaria e che sia usata con discrezione.
9.1	Controllo qualità del monitoraggio delle chiamate	I responsabili devono eseguire controlli di qualità, inclusi controlli settimanali su una selezione casuale di chiamate del cliente (in entrata e in uscita) gestite dai consulenti e un controllo mensile di tutti i report e procedimenti implementati dal Fornitore. Questo dovrebbe fare in modo che il Fornitore sia in conformità con questi Requisiti e, in particolare, che i dipendenti stiano usando il corretto procedimento di

		autenticazione del cliente e stiano tenendo dei report corretti.
10.1	Controlli a campione di conformità	Occorre implementare un procedimento verificabile tramite audit per condurre e gestire controlli di conformità locali periodici in materia di sicurezza e controlli a campione di conformità per tutti i Requisiti. Così come il Fornitore ha l'obbligo di eseguire tali controlli, anche BT e/o EE possono eseguire in qualsiasi momento controlli a campione sulla conformità. I controlli a campione includono, a titolo esemplificativo ma non esaustivo: • ID di sicurezza/ Pass di sicurezza • Scrivania pulita/schermo pulito • Utilizzo di armadietti personali • Dispositivi mobili personali • Utilizzo di lavagne bianche • Eliminazione e smaltimento di informazioni riservate stampate o inviate a mezzo fax • Autenticazione del cliente • Controlli qualità del monitoraggio delle chiamate • Audit trail per il reset delle password • Utilizzo di messaggi di testo • Conformità con la formazione in materia di sicurezza e protezione dei dati Tutti i controlli a campione devono includere i dettagli delle azioni da intraprendere laddove vengano evidenziate discrepanze o non conformità. È necessario tenere traccia di eventuali misure correttive richieste da BT e/o EE fino al completamento.