Normes d'un Centre d'appel

Généralités

(A) Ces conditions doivent être lues conjointement avec la Matrice de mise en œuvre présentée à l'Annexe 1 de ce document, qui apporte des détails sur les comportements et les résultats que BT considère généralement acceptables en matière de conformité du Fournisseur avec les exigences.

(B) BT peut réaliser des évaluations du risque pour le centre de contact comme l'indique la section 3.10 des Exigences de sécurité des fournisseurs de BT (les « Exigences de sécurité ») à tout moment, avant ou durant la fourniture des services. Sans préjudice de tous les autres recours éventuellement à la disposition de BT, BT peut stipuler des actions correctives, des contrôles compensatoires et des contremesures pour traiter tous les risques identifiés et/ou insatisfaisants ou non conformes à ces Exigences, qui seront mis en place par le Fournisseur et documentés dans une annexe à cette norme ; tous les coûts associés à la mise en place de nouvelles exigences de sécurité devant être convenues entre les deux parties.

(C) Sur demande, BT sera autorisée à revoir les politiques et les procédures du Fournisseur qui exécute les exigences de cette norme comme une partie de la réalisation d'évaluations pour le centre de contact. Ces politiques peuvent inclure mais sans s'y limiter : la politique sur l'utilisation des ordinateurs, l'élimination informatique, l'authentification du client, les contrôles pré-recrutement, l'évaluation des risques et le processus de gestion, etc.

1. Sécurité physique

1.1 Le fournisseur doit assurer que les zones du centre de contact (voir glossaire) utilisées pour le fonctionnement du compte BT/EE sont physiquement séparées de tous les autres secteurs d'activité par des contrôles d'accès physiques.

1.2 Le fournisseur doit disposer d'un processus vérifiable pour accéder sur place aux requêtes et approuver un nouvel accès physique ou la suppression d'un accès physique au domaine du centre de contact. [1]

1.3 En vue d'évaluer les droits d'accès physiques aux zones du centre (y compris les mouvements et les changements internes) et ceci faisant partie du « processus des sortants » du fournisseur, celui-ci doit garantir que le processus vérifiable d'accès est revu tous les trois (3) mois et que la date de chaque révision est enregistrée.

1.4 Le fournisseur doit assurer la protection du travail isolé dans le centre de contact. Cette exigence concerne les agents d'entretien et les employés des tiers.

1.5 Le fournisseur doit disposer d'un processus vérifiable qui assure que le talonnage à l'accès aux portes et aux barrières contrôlées est évité. Le processus doit être applicable et son non respect répété fera l'objet d'une mesure disciplinaire.

2. Laissez-passer et visiteurs

2.1 Le fournisseur doit assurer que les employés autorisés (en raison de leur fonction) à détenir et à utiliser des téléphones portables, des ordinateurs portables, des iPads et/ou des tablettes

[1] Voir la Matrice de mise en œuvre pour des exemples de processus d'accès vérifiable.

dans les zones du centre de contact sont facilement identifiables par les autres employés et les superviseurs.[2]

2.2 Le fournisseur doit disposer sur place d'un processus vérifiable pour l'émission et la gestion des Laissez-passer, et, le cas échéant, des Laissez-passer temporaires pour les employés du centre de contact, qui inclut l'annulation automatique des droits d'accès quand le laissez-passer est arrivé à échéance.

2.3 Le fournisseur doit assurer que les laissez-passer et les cordons n'identifient pas le lieu de travail d'un employé.

2.4 Le fournisseur doit assurer qu'un processus vérifiable des visiteurs est en place et qu'il est divulgué à tous les employés. Un registre des visiteurs doit être conservé comme preuve.[3]

2.5 Les laissez-passer émis pour les visiteurs doivent distinguer ceux-ci des collaborateurs et doivent être restitués lorsque le visiteur quitte le centre de contact, chaque laissez-passer qui n'est pas immédiatement restitué devant être immédiatement désactivé le jour ouvré suivant.

2.6 Le fournisseur doit assurer que les visiteurs du centre de contact sont escortés en permanence et portent des badges/laissez-passer visibles.

3. Collaborateurs

3.1 Le fournisseur doit assurer que les articles personnels (y compris les dispositifs portables) sont rangés dans des casiers désignés, à l'écart de la zone du centre de contact.

3.2 Le fournisseur doit autoriser les médicaments personnels/équipement médical de base nécessaires, tels qu'inhalateurs, insuline ou médicaments contre la toux dans le centre de contact.

3.3 À moins qu'une évaluation du risque le permette, le personnel qui travaille dans le centre de contact n'est pas autorisé à avoir de téléphones ni de dispositifs portables. Le fournisseur doit mettre en place des contrôles ponctuels réguliers d'observation du personnel pour s'assurer qu'il n'y a pas de téléphones et de dispositifs portables dans le centre de contact et signaliser l'interdiction de leur usage. En outre, des programmes de formation destinés à la sensibilisation en matière de sécurité doivent insister clairement sur cette exigence et il faudra mettre des processus disciplinaires en place pour sanctionner les non respects.

3.4 Le fournisseur doit assurer la mise en place d'un processus pour permettre aux parties extérieures de contacter les collaborateurs en cas d'urgence personnelle.[4]

3.5 Il doit y avoir un processus vérifiable pour l'autorisation et l'utilisation de stylos, de crayons et de papier dans le centre de contact. Les stylos, les crayons et le papier ne sont pas permis, sauf si les collaborateurs sont autorisés par leur responsable à les utiliser en raison de la fonction qu'ils remplissent.

3.6 Si cela fait partie de la fonction remplie par l'employé, le fournisseur doit s'assurer que toutes les notes écrites ne sont pas laissées à l'abandon et qu'elles sont rangées en toute sécurité

[2] Voir la Matrice de mise en œuvre pour des exemples de ce qui est considéré comme facilement identifiable.
[3] Voir la Matrice de mise en œuvre pour les informations qui doivent être consignées dans le registre des visiteurs.
[4] Voir la Matrice de mise en œuvre pour des exemples de processus en cas d'urgence personnelle.

(selon la procédure de classification et de manipulation des informations) ou éliminées[5] à la fin de la journée de travail, afin de suivre une « Politique de bureau propre »[6].

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

3.7 Le fournisseur doit disposer de tableaux blancs et de blocs-notes effaçables (y compris stylos et chiffons à sec), qu'il proposera en alternative aux stylos, crayons et papiers, afin de permettre la prise de notes durant les appels. Le fournisseur doit veiller à ce que ces notes soient effacées dès que la demande du client est traitée et toutes les notes doivent être effacées des tableaux blancs à la fin de chaque période de travail du téléopérateur. Les responsables et les superviseurs doivent circuler dans le local et effectuer des contrôles ponctuels pour veiller au respect de cette exigence.

3.8 Le fournisseur doit vérifier que toutes les notes temporaires enregistrées en ligne ou dans des outils électroniques (afin de soutenir les appels des clients) sont automatiquement effacées à la fin de la période de travail de chaque téléopérateur ou à la fin de la journée de travail. Ceci doit se faire automatiquement ou bien il faudra conserver un enregistrement quotidien pour assurer le respect de cette exigence.

3.9 Le fournisseur doit veiller à ce qu'un processus vérifiable de l'usage des tableaux blancs/papier soit établi et mis en place pour assurer :

- que les papiers sont conservés en toute sécurité ou supprimés et éliminés à la fin de chaque journée de travail, et
- que les tableaux blancs sont nettoyés à la fin de chaque période de travail et à la fin de la journée de travail.[7]

3.10 Le fournisseur doit s'organiser pour que toutes les interactions avec les clients soient enregistrées sur le compte (mémo ou bloc-notes en fonction du système utilisé).

3.11 Le fournisseur doit assurer que toutes les interactions avec les clients ne sont pas enregistrées dans des Applications Microsoft Office, sauf si les collaborateurs sont autorisés à le faire par une évaluation des risques comme faisant partie de leur travail.

3.12 Le fournisseur doit assurer que toute fonction autorisée à accomplir l'une des activités suivantes dans le centre de contact est soumise à une évaluation des risques, conformément aux exigences établies dans la section 11. Ces activités peuvent inclure mais sans s'y limiter :

- l'utilisation d'applications Microsoft Office
- l'utilisation de dispositifs portables
- l'utilisation des ordinateurs portables de la société
- l'utilisation d'articles personnels (comme définie dans le glossaire)
- la permission d'imprimer ou de copier les informations du client
- la permission de télécharger des enregistrements d'appels à partir du (des) serveur(s) d'enregistrement d'appels
- l'accès à l'e-mail interne, externe ou à d'autres outils de communication, par ex. messagerie instantanée

[5] Voir la Matrice de mise en œuvre pour des exemples de rangement sécurisé ou d'élimination.
[6] Voir la Matrice de mise en œuvre pour un exemple de ce que doit inclure une Politique de bureau propre.
[7] Voir la Matrice de mise en œuvre pour des exemples de ce que doit comprendre un contrôle des tableaux blancs/papier.

- l'utilisation de stylos/crayons et papier pour la prise de notes
- l'envoi de messages de texte multiples aux clients
- l'accès à distance à l'équipement du client

3.13 Le fournisseur doit s'assurer que la possibilité d'envoyer des messages de texte multiples (un message de texte à plusieurs clients) n'est pas permise, sauf si les collaborateurs sont autorisés à le faire si cela fait partie de leur fonction. Si de tels textes sont transmis, des enregistrements doivent être conservés pour indiquer quand ils ont eu lieu, le(s) destinataire(s) et les raisons de leur envoi.

3.14 Le fournisseur doit assurer que le téléchargement des enregistrements d'appels à partir du (des) serveur(s) d'enregistrement d'appels vers les ordinateurs de bureau ou portables est interdit, celui-ci n'étant possible que si la personne est autorisée à le faire si cela fait partie de sa fonction. S'il est autorisé, un enregistrement doit être conservé indiquant la personne autorisée à remplir cette fonction et si les enregistrements d'appels sont téléchargés, des enregistrements doivent être conservés pour indiquer la raison, l'appel téléchargé actuel et les raisons du téléchargement. La validité de l'autorisation des téléopérateurs et tous les non-respects doivent être revus régulièrement.

4. Équipement

4.1 Le fournisseur doit assurer que tous les téléopérateurs disposent d'écrans d'ordinateur protégés, qui ne sont pas visibles à partir de l'extérieur de la zone du centre de contact isolée.[8]

4.2 Le fournisseur doit assurer que les imprimantes et les télécopieurs sont situés dans des zones sécurisées, réservées aux personnes autorisées et uniquement utilisées à des fins strictement nécessaires. La liste des utilisateurs autorisés et l'utilisation des machines doivent être revues régulièrement pour assurer une validité continue. Toutes les copies imprimées doivent être conservées en toute sécurité conformément à la classification des informations et aux normes de manipulation et ne doivent pas être soustraites du centre de contact jusqu'à ce que BT l'autorise.

4.3 Le fournisseur doit assurer que toute impression et copie requiert un numéro d'utilisateur (User ID) et un code de sécurité afin que toutes les impressions puissent être suivies et consignées à des fins de contrôle.

4.4 Le fournisseur doit assurer que les déchiqueteuses et les conteneurs à déchets confidentiels sont fournis à proximité des imprimantes et des télécopieurs. Les déchiqueteuses et les conteneurs à déchets doivent être vidés régulièrement et le contenu éliminé de façon sûre.

4.5 Le fournisseur doit assurer que toutes les informations en format papier sont éliminées de façon sûre, par déchiquetage ou en les plaçant dans des conteneurs à déchets confidentiels conformément à la section 4.4.

4.6 Le fournisseur doit assurer que tous les biens physiques assignés aux collaborateurs au début de leur entrée en service sont récupérés/supprimés avant la fin de leurs fonctions au centre de contact ou lorsqu'ils cessent leur contrat avec BT/EE et un inventaire des biens physiques doit être effectué.[9]

[8] Voir la Matrice de mise en œuvre pour des exemples de ce que l'on entend par « écrans d'ordinateur protégés ».
[9] Voir la Matrice de mise en œuvre pour des exemples de ce que doit inclure l'Inventaire des biens physiques.

4.7 Le fournisseur doit assurer que les biens physiques qui ont été récupérés ou supprimés sont éliminés de façon sûre et en ligne avec les exigences d'une élimination sécurisée.[10]

5. Accès aux systèmes

5.1 Pour protéger les données du client, tous les téléopérateurs doivent indiquer leur Identifiant d'utilisateur (User ID) lorsqu'ils accèdent au compte/enregistrement d'un client, ainsi que la raison de cet accès. L'accès ne doit être accordé qu'après l'approbation du Propriétaire du système ou d'un gestionnaire de ligne. En outre, l'accès aux comptes des clients ne doit être permis que si cela est requis par la fonction du téléopérateur et doit être réglé au niveau minimum nécessaire pour qu'un téléopérateur puisse effectuer son travail. L'accès des personnes qui n'ont pas besoin d'accéder à un système BT et/ou EE pour voir les enregistrements des clients doit être interdit pour quelque raison que ce soit.

5.2 L'accès « Voir seulement » doit être évité, sauf s'il est requis pour des raisons opérationnelles. L'accès « Voir seulement » autorisé doit être consigné et contrôlé pour éviter toute utilisation indue.

5.3 Le fournisseur doit assurer que les collaborateurs n'ont pas le droit d'accéder à Internet, à leur e-mail personnel ou aux e-mails extérieurs, aux réseaux sociaux (comme Facebook) ou à d'autres outils de communication tels que Messenger ou Communicator, sauf s'ils y sont autorisés par BT et si cela est requis pour l'accomplissement de leur fonction.

5.4 Le fournisseur doit assurer que tous les messages de texte envoyés depuis les systèmes des fournisseurs sont consignés et contrôlés. Si des textes sont transmis, des enregistrements doivent être conservés pour indiquer quand ils ont eu lieu, le(s) destinataire(s) et les raisons de leur envoi.

5.5 Le fournisseur doit assurer que seuls des outils d'accès à distance pré-agréés, utilisés pour accéder aux dispositifs du client à des fins de support technique sont permis et que ceux-ci sont strictement limités au personnel qui doit les réaliser pour remplir sa fonction. L'accès doit être revu tous les 3 mois et est annulé s'il n'est plus nécessaire à l'accomplissement de la fonction. Il faut mettre des solutions en place pour identifier les outils d'accès à distance non agréés.[11]

5.6 Le fournisseur ne doit pas permettre l'accès à distance pour contacter les employés du centre à travers leur e-mail de travail ni aucun système permettant d'accéder aux enregistrements du client.

5.7 Le fournisseur doit assurer que l'accès « Voir seulement » est permis aux collaborateurs uniquement pour les lecteurs partagés fournis et contrôlés par BT et/ou EE. Aucuns autres lecteurs partagés ne devront être utilisés dans le centre de contact. Le téléchargement, la copie, la suppression ou la modification des informations du client d'un système, application ou base de données de BT et/ou EE est interdit.

[10] Voir la Matrice de mise en œuvre pour un exemple de ce en quoi doivent consister les exigences d'élimination.
[11] Voir la Matrice de mise en œuvre pour des exemples de comportements à identifier et d'outils d'accès à distance.

6. Enregistrements des appels

6.1 Le fournisseur doit assurer que tous les appels des clients sont enregistrés. Le fournisseur doit assurer que les enregistrements d'appels (voix et écran) sont protégés durant leur transmission du Bureau du PC vers le(s) serveur(s) d'enregistrement d'appels.[12]

6.2 Le fournisseur doit assurer que les enregistrements d'appels sont conservés en sécurité, en particulier s'ils incluent des Informations sur la carte de paiement (PCI) afin d'éviter la perte ou l'utilisation indue des données du client. Les données PCI doivent être encodées et une solution de gestion de clé doit être mise en place pour protéger cette meilleure pratique d'utilisation du secteur. BT et/ou EE peut revoir l'encodage et les solutions de protection du stockage de temps à autre pour assurer qu'ils sont adéquats et appropriés.

7. Authentification du client

7.1 Le fournisseur doit assurer qu'un processus d'authentification approuvé est défini et mis en place pour les appels « entrants » et « sortants ».[13]

7.2 Le fournisseur doit assurer que les pins ou les mots de passe utilisés par le client pour authentifier leur identité ne sont pas visibles par d'autres collaborateurs du centre de contact, par exemple grâce à l'utilisation d'écrans d'ordinateur protégés ou à une séparation physique.

7.3 Le fournisseur doit assurer que l'authentification du client est automatisée de telle façon qu'elle ne requière pas que le client révèle son pin complet ou son mot de passe au téléopérateur, par exemple à travers la sollicitation, générée par un système, de certains chiffres/lettres aléatoires du mot de passe, par exemple, le 1er, le 3e et le 5e. BT et/ou EE peut revoir le processus d'authentification du client de temps à autre pour assurer la conformité avec les exigences.

7.4 Le fournisseur doit assurer que lorsque le client a oublié son pin ou son mot de passe et qu'il a besoin de le réinitialiser, aucune réinitialisation ne se produit jusqu'à ce que le client ait satisfait aux contrôles d'authentification supplémentaires.[14]

7.5 Le fournisseur doit assurer que les systèmes de saisie du pin du compte du client ou du mot de passe sont automatisés et ne requièrent aucune intervention du collaborateur du centre de contact.

7.6 Le fournisseur doit assurer que la création de nouveaux pins ou mots de passe est générée par un système automatisé et que les nouveaux pins ou mots de passe sont envoyés directement au client soit par message texte ou par e-mail sans intervention du téléopérateur.

7.7 Le fournisseur doit assurer que le nouveau mot de passe ou pin du compte peut être réinitialisé par le client en ligne ou à travers un système de Réponse vocale interactive (IVR).

7.8 Le fournisseur doit assurer qu'il existe une possibilité d'« aide à la réinitialisation par les collaborateurs », permettant au client de réinitialiser leur pin ou mot de passe avec l'aide d'un

[12] Voir la Matrice de mise en œuvre pour des exemples de la façon dont les transmissions des enregistrements d'appels doivent être protégées.
[13] Voir la Matrice de mise en œuvre pour des exemples de ce que doit impliquer le processus d'authentification du client.
[14] Voir la Matrice de mise en œuvre pour des exemples de ce en quoi doivent consister les contrôles d'authentification supplémentaires.

collaborateur du centre de contact. La possibilité de réinitialiser un pin ou un mot de passe doit être limitée à un nombre restreint de collaborateurs.[15]

7.9 Sur demande, le fournisseur doit être capable de générer une piste d'audit montrant les réinitialisations du pin ou du mot de passe du client, ainsi que le système utilisé pour réaliser la réinitialisation (en ligne, IVR ou aide de l'employé) et quel collaborateur a été impliqué dans la démarche.

8. Confidentialité des données

En plus de la formation obligatoire de BT en Sécurité et en Protection des données (voir Annexe 2) que tous les collaborateurs du fournisseur doivent suivre et s'assurer d'avoir compris, les conditions requises suivantes doivent également être remplies :

8.1 Le fournisseur doit assurer que les collaborateurs du centre de contact ont facilement accès aux informations pertinentes concernant la sécurité et la protection des données sur la première page de leur page d'accueil Intranet (ou, s'ils ne disposent pas d'Intranet, au moyen d'actualisations régulières par e-mail et de formation).

8.2 Le fournisseur doit organiser des recyclages réguliers, au moins deux fois par an pour tous les collaborateurs du centre de contact, afin de renforcer les comportements positifs et d'adopter les meilleures pratiques de sécurité.

9. Surveillance

9.1 Le fournisseur doit mettre en place une vérification de la qualité des appels par des superviseurs/responsables, en sélectionnant aléatoirement des appels téléphoniques de clients (entrants et sortants), qui devra être réalisée toute les semaines pour assurer, entre autres exigences, que le processus correct d'authentification du client a été utilisé.[16]

9.2 Le fournisseur doit assurer que tous les appels sont considérés comme « appels manqués » si le processus correct d'authentification du client n'a pas été suivi. Suite à tout appel manqué, le fournisseur doit mettre en place un processus de rétroaction pour rappeler aux téléopérateurs du centre de contact leurs responsabilités en matière d'authentification correcte des clients et de conservation sécurisée des mots de passe (le cas échéant).

9.3 Le fournisseur doit disposer d'un processus de contrôle au cas où un collaborateur du centre de contact ait des appels manqués répétés et ne parvienne pas à effectuer le processus correct d'authentification du client. Ce processus doit comporter les conséquences encourues par un téléopérateur qui ne parvient pas, de façon répétée, à réaliser correctement l'authentification du client ou à conserver correctement l'enregistrement et peut être utilisé comme preuve pour la gestion de performance ou les procédures disciplinaires à l'encontre de l'individu en question.

10. Conformité

10.1 Le fournisseur doit assurer qu'un processus de contrôle documenté est en place pour réaliser et gérer des vérifications régulières des conduites de sécurité et/ou des contrôles ponctuels

[15] Voir la Matrice de mise en œuvre pour des exemples de ce en quoi doit consister la possibilité de réinitialisation avec l'aide du collaborateur.
[16] Voir la Matrice de mise en œuvre pour des exemples de ce que doit inclure au minimum le contrôle qualité.

de la conformité avec cette norme et les exigences de sécurité de BT, par exemple circuler dans le local, nettoyer les bureaux, etc.[17]

10.2 Le fournisseur doit mettre en place un processus qui assure la réalisation de révisions basées sur des résultats trimestriels (à partir de 10 % des entrées), auxquelles sont soumis les collaborateurs du centre ou toutes les autres personnes qui travaillent sous un contrat BT et/ou EE pour assurer qu'un processus de sélection pré-recrutement et une formation en sécurité (faisant partie du processus de recrutement) ont été suivis et qu'ils opèrent de façon satisfaisante. Ceci est destiné à assurer que la formation de base des collaborateurs qui travaillent au centre de contact a été suivie de façon adéquate (en ligne avec la politique de contrôles pré-recrutement de BT) et qu'ils ont été formés en sécurité, afin d'être sûr que les informations sensibles du client sont correctement protégées.

10.3 Le fournisseur doit mettre en place un processus qui assure la réalisation de révisions basées sur des résultats trimestriels (à partir de 100 % des entrées), auxquelles sont soumis les collaborateurs du centre ou toutes les autres personnes qui travaillent sous un contrat BT et/ou EE pour assurer que la formation obligatoire en Sécurité et en Protection des données a été suivie.

10.4 Le fournisseur doit assurer l'organisation de séances de recyclage concernant les obligations des collaborateurs en matière de Sécurité et de Protection des données et des documents devront attester de leur participation et de leur compréhension.

10.5 Le fournisseur doit assurer que les politiques, les normes, les directives et les processus pertinents sont à la disposition des collaborateurs du centre pour assurer la conformité avec cette norme et les exigences de BT en matière de Sécurité.

11. Évaluation des risques

Le fournisseur doit assurer que toutes les non conformités, autorisations ou exceptions spécifiques à ces exigences font l'objet d'une évaluation de risque par le fournisseur et sont documentées selon le processus d'évaluation du risque. L'évaluation du risque doit comporter :

- la raison pour laquelle l'activité est requise et pourquoi une non conformité à ces exigences est justifiable ;
- l'état de toute non conformité, permanente ou temporaire, par exemple ;
- si elle est temporaire, la date à laquelle les contrôles vont être mis en place et la date à laquelle l'activité sera terminée ;
- la fonction/poste de la personne et pourquoi l'activité est appropriée à cette fonction (et pourquoi ils sont exclus de la conformité avec les contrôles) ;
- des contrôles d'atténuation sur place pour minimiser les risques provenant de l'activité ;
- la justification de la mise en place de certains contrôles et/ou de la non mise en place des contrôles nécessaires ;
- la preuve de l'approbation du gestionnaire senior.

[17] Voir la Matrice de mise en œuvre pour des exemples de ce que doivent comprendre les contrôles ponctuels de conformité.

12. Glossaire

Terme	Explication
Centre de contact client	Un centre de contact (également dénommé centre d'interaction avec le client ou centre e-contact) est un point central de l'entreprise, à partir duquel tous les contacts des clients sont traités. Le centre de contact comprend normalement un ou plusieurs centre(s) d'appels mais peut aussi comporter d'autres types de contact avec le client, tels que des bulletins via e-mail, des catalogues par courrier postal, des enquêtes de site Web et des causeries et le recueil d'informations des clients durant l'achat en magasin. Un centre de contact fait généralement partie de la gestion globale de la relation client (CRM).
Casiers désignés	Le personnel qui travaille dans le centre de contact n'est pas autorisé à conserver des articles personnels capables d'enregistrer les informations du client, tels que téléphones portables, à son poste de travail. Ces articles doivent être gardés dans des casiers personnels (marqués comme tels) éloignés du centre de contact.
Collaborateur/trice	Collaborateur désigne toute personne qui travaille dans le centre de contact, y compris les collaborateurs permanents et temporaires du fournisseur, le personnel d'agence, les entrepreneurs et les travailleurs.
Escorte	Un processus formel de visite doit être mis en place, assurant au minimum que les visiteurs du centre de contact sont escortés en permanence afin d'éviter que les personnes ne se perdent ou pénètrent dans des zones où l'accès est interdit.
Matrice de mise en œuvre	La matrice présentée en annexe, qui établit les résultats et les standards minima que le fournisseur doit atteindre lorsqu'il met en place certains processus, politiques ou procédures mentionnés dans les exigences.
Travail isolé	Un processus doit être mis en place pour assurer que la pratique d'un travail individuel dans le centre de contact en dehors des heures ouvrées normales n'est pas permis sans l'autorisation de la direction. Ceci inclut les équipes de nettoyage et d'autres personnes ne faisant pas partie du personnel de la société, comme le personnel d'entretien.
Applications Microsoft Office	Les Applications Microsoft Office incluent sans s'y limiter, Word, PowerPoint, Excel, Outlook et OneNote. Pour empêcher toute exfiltration de données, les interactions avec le client qui impliquent des systèmes en ligne ne doivent pas être enregistrées sur ces applications (sauf autorisation préalable) car les informations peuvent facilement être copiées et en être extraites.
Articles personnels	Tout article personnel pouvant être utilisé pour capturer/enregistrer des informations client - ceci comprenant sans s'y limiter : les téléphones portables, les montres intelligentes, les iPods, les iPads, les caméras, les clés USB, les stylos et le papier.
Contrôles d'accès physiques	Les contrôles d'accès physiques utilisés vont dépendre de la zone où est situé le centre de contact. Les contrôles d'accès physiques peuvent être techniques (par ex. carte magnétique, clavier, biométrique) ou procéduraux (par ex. clés avec un processus de déconnexion vérifiable ou un processus de connexion où la

	personne qui contrôle l'accès vérifie l'ID), mais les contrôles d'accès physiques utilisés doivent être appropriés à la zone.
Biens physiques	Aux fins de ce document – les biens physiques se réfèrent à tout bien qui est capable de traiter ou de stocker les données ou les informations du client.
Séparation physique	Aux fins de ce document, la séparation physique signifie que les conversations ne peuvent pas être écoutées et que les informations ne peuvent pas être vues à partir d'autres secteurs d'activité. Une barrière physique (murs, immeubles séparés, etc.) avec des contrôles physiques qui régissent l'entrée de la zone doit être mise en place.
Incident de sécurité	Un incident de sécurité est un changement dans l'opération normale des affaires, qui a un impact sur la confidentialité, l'intégrité ou la disponibilité ou les éléments d'information, indiquant qu'une défaillance de la politique de sécurité, normes de sécurité/exigences peut s'être produite ou qu'une protection de la sécurité peut avoir échoué. Voici quelques exemples : mauvaise utilisation du système, accès non autorisé, équipement perdu/volé et infection par des logiciels malveillants.
Approbation de la haute direction	Lorsqu'il est nécessaire d'accorder une exception à ces exigences, les conditions doivent faire l'objet d'une évaluation du risque et la personne qui approuve doit être quelqu'un qui a la responsabilité de la gestion de la zone fonctionnelle qui a l'autorité requise.
Propriétaire du système	Ceci désigne le responsable de l'ensemble de l'approvisionnement, développement, intégration, modification ou opération et maintenance d'un système d'information.
Talonnage	La pratique du talonnage ou permettre à un individu non autorisé d'accéder à travers une porte/barrière ou un portail d'accès contrôlé ; ne pas utiliser le laissez-passer personnel pour avoir accès à une zone autorisée des installations du fournisseur utilisée pour assumer des contrats BT/EE.
Laissez-passer temporaire	Ceux-ci doivent être émis en tant qu'élément d'un processus vérifiable (tel qu'un livre, un registre ou un tableur), qui doit enregistrer toute émission de laissez-passer temporaires, en mentionnant la date de leur émission, le nom, le département, le numéro de contact et la raison de l'émission, ainsi que le nom de l'hôte et la date de la restitution du laissez-passer temporaire. Un processus doit être mis en place pour traiter les cartes qui ne sont pas restituées.
Identifiant d'utilisateur (User ID)	Les imprimantes et les télécopieurs situés dans le centre de contact doivent requérir que l'utilisateur saisisse un seul ID et code de sécurité, de façon à permettre de contrôler leur utilisation individuellement. Les collaborateurs doivent en outre saisir cet ID unique lorsqu'ils accèdent aux comptes/enregistrements du client conformément à la section 5.1.

PROJECT KITE : Matrice de mise en œuvre destinée au fournisseur pour remplir les exigences du centre de contact.

Référence du programme	Description générale	Résultats minima susceptibles d'être considérés comme conformes
1.2	Processus d'accès vérifiable	Un tableur ou un registre de noms, comprenant des détails sur la façon dont l'accès est octroyé, la justification de l'octroi de cet accès, la date de l'annulation de l'accès et la raison pour laquelle on le fait.
2.1	Reconnaissance facile	Le personnel autorisé à utiliser téléphones portables, ordinateurs portables, iPads, tablettes en raison de sa fonction doit être facilement identifiable par des moyens tels que cordon d'une couleur différente ou d'autres moyens d'identification distincts.
2.4	Registres des visiteurs	Les informations suivantes doivent être consignées : i) le nom de la personne ; ii) l'organisation à laquelle elle appartient ; iii) la date et l'heure de son entrée et de son départ ; iv) le but de sa visite ; v) le nom de la personne qu'elle vient rencontrer ; vi) le numéro d'enregistrement de tout véhicule amené sur le site ; vii) le numéro de téléphone portable ; viii) le numéro d'identification du laissez-passer visiteur.
3.5	Urgence personnelle	Un système doit être mis en place pour que la famille et les amis puissent continuer à contacter le collaborateur en cas d'urgence personnelle. Ce système de contact peut se faire à travers l'usage d'un numéro de standard téléphonique ou du numéro d'un superviseur qui peut être utilisé comme point de contact central.
3.7	Stockage ou élimination sécurisée	Lorsque des notes ont été produites au cours de l'activité du collaborateur, des exemples de stockage ou d'élimination sécurisée incluent, mais sans s'y limiter, l'utilisation de déchiqueteuses, de conteneurs à déchets confidentiels (et

		potentiellement fermés) et/ou un stockage dans des installations permises qui peuvent être fermées par les collaborateurs.
3.7	Politique du bureau propre	Tout le matériel doit être stocké ou éliminé en toute sécurité immédiatement après son usage et aucun matériel ne doit être laissé sur le bureau à la fin de la journée de travail. Des contrôles ponctuels réguliers d'observation du personnel doivent être mis en place et il faut disposer d'un processus disciplinaire pour traiter les cas de non respect.
3.10	Audit de tableaux blancs/papier	En ce qui concerne les processus de la section 3, un enregistrement (sous forme de tableur) doit être fait pour prouver que les contrôles ponctuels sont effectués et que la conformité avec les exigences est assurée.
4.1	Écrans d'ordinateur protégés	Il ne doit pas être possible de voir les écrans des téléopérateurs dans l'environnement du centre de contact et les informations ne doivent pas pouvoir être lues par les personnes du centre de contact non autorisées à le faire (telles que le personnel de nettoyage et d'entretien). Les données du client présentes sur les écrans d'ordinateur doivent être occultées en positionnant les écrans de façon adéquate ou en utilisant des écrans d'intimité.
4.6	Inventaire des biens physiques	Un inventaire de tous les biens physiques et des autres éléments assignés aux personnes, tels que les laissez-passer, les clés de casier, les ordinateurs portables, les ordinateurs de bureau ou les jetons d'accès à distance doivent être conservés à des fins de contrôle. Lorsqu'un téléopérateur quitte son emploi ou est transféré du centre de contact, des processus doivent être mis en place pour assurer que les étapes suivantes sont suivies pour annuler tout accès logique et physique et récupérer tous les biens physiques, clés, laissez-passer, etc. Ceci doit être effectué comme faisant partie de la liste de contrôle des « Sortants » lorsqu'ils quittent la fonction.
4.7	Exigences d'élimination sécurisée	Lorsque des biens physiques sont éliminés à la fin de leur vie utile, un logiciel propriétaire tel que « Tabernus » ou « Blanco » doit être utilisé pour assurer que toutes les informations confidentielles du client ont été effacées de l'équipement de façon permanente (le cas échéant) et selon la norme approuvée par BT et/ou EE. Si l'élimination sécurisée des données ne peut être effectuée en utilisant ce logiciel, l'équipement doit faire l'objet d'une destruction sécurisée en utilisant un processus approuvé par BT et/ou par EE. Le responsable de la sécurité BT et/ou EE peut vous aider dans ce domaine. Lorsque les informations confidentielles ou les informations du client ont

		été supprimées, les biens physiques peuvent être réutilisés ailleurs ou être éliminés, le cas échéant.
5.5	Outils d'accès à distance	Afin d'éviter l'accès non autorisé aux données du client, il faut mettre en place des processus formels pour assurer que seuls les outils d'accès à distance approuvés au préalable par BT et/ou EE peuvent accéder aux dispositifs des clients. Des solutions doivent être mises en place pour identifier les outils d'accès à distance non approuvés et ces solutions doivent être revues régulièrement pour assurer que les outils non approuvés ne peuvent pas être et/ou n'ont pas été utilisés. L'utilisation des outils d'accès à distance approuvés doit en outre être limitée aux personnes autorisées, celles-ci n'obtenant l'autorisation qu'à travers un processus formel, comportant une évaluation du risque qu'implique la nécessité d'accéder à distance.
6.1	Transmission des enregistrements d'appels	Il est essentiel d'encoder les enregistrements des appels des clients du PC vers des serveurs d'enregistrement d'appel et cet encodage doit inclure les enregistrements vocaux et les détails de l'écran.
7.1	Authentification du client	Tous les téléopérateurs doivent suivre le processus d'authentification du client tel qu'il est approuvé par BT et/ou EE pour s'assurer que la personne est bien celle qu'elle prétend être. Ce processus sera précisé aux fournisseurs et aux téléopérateurs et peut différer selon la (les) fonctionnalité(s) que fournit le centre de contact.
7.4	Contrôles d'authentification supplémentaires	Avant de procéder au changement du PIN ou du mot de passe du client, les téléopérateurs doivent s'assurer en outre qu'ils obtiennent les informations suffisantes de la part du client, que la personne est bien celle qu'elle prétend être en lui posant certaines questions de sécurité sur son identité en plus de son nom et adresse, telles que l'activité récente de son compte, le montant de la dernière facture ou depuis combien de temps il est client de BT ou d'EE. Cependant, il ne s'agit que d'exemples et cette liste n'est pas exhaustive.

7.8	Réinitialisations avec l'aide du téléopérateur	Pour aider les clients qui ne sont pas capables de réinitialiser leur PIN ou mot de passe en ligne ou via IVR, il doit être possible de faciliter ces réinitialisations avec l'aide du téléopérateur du centre de contact. Cependant, un processus formel doit être mis en place pour assurer que la possibilité de réinitialiser avec le collaborateur est restreinte à un nombre limité de collaborateurs et que les sauvegardes sont en place pour garantir que tout collaborateur ayant la possibilité de réinitialiser le PIN du client ou les mots de passe est physiquement séparé des autres téléopérateurs du centre de contact et que les contrôles appropriés sont en place. La liste des approbateurs doit être revue régulièrement pour assurer que cette approbation est encore requise et qu'elle est utilisée à bon escient.
9.1	Contrôle de qualité des appels	Les directeurs doivent réaliser des contrôles de qualité, y compris la surveillance hebdomadaire d'une sélection aléatoire d'appels téléphoniques de clients (entrants et sortants) traités par les téléopérateurs et la révision mensuelle de tous les enregistrements et des processus implémentés par le fournisseur. Ceci a pour but d'assurer que le fournisseur respecte ces exigences et, en particulier, que les téléopérateurs utilisent le processus correct d'authentification des clients et conservent les enregistrements appropriés.
10.1	Contrôles ponctuels de conformité	Un processus vérifiable doit être mis en place pour mener et gérer les contrôles de conformité de la sécurité du site et des contrôles ponctuels de conformité avec toutes les exigences. De même que le fournisseur est obligé à réaliser ces contrôles, BT et/ou EE peuvent aussi réaliser des contrôles ponctuels à tout moment. Les contrôles ponctuels incluent sans se limiter : • ID de sécurité/laissez-passer • Bureau propre/écran propre • Utilisation de casiers personnels • Dispositifs portables personnels • Utilisation de tableurs • Suppression et élimination des informations confidentielles imprimées ou télécopiées • Authentification du client • Contrôles de surveillance de la qualité des appels • Traçage de la réinitialisation de mot de passe • Utilisation de messages texte • Respect de la formation en protection des données et sécurité

		Tout audit des contrôles ponctuels inclut les mesures détaillées à prendre là où les écarts et les non respects sont mis en évidence. Tous les plans de redressement requis par BT et/ou EE doivent être suivis jusqu'à leur achèvement.