Annexe [XX] – Exigences de sécurité des fournisseurs de BT

Sommaire

PARTIE 1 : INTRODUCTION

1 INTRODUCTION

1.1 Le présent document définit les exigences de sécurité de BT.

1.2 Dans les présentes Exigences de sécurité, les définitions données aux termes cités dans la Partie 5 intitulée « **Définitions** » s'appliqueront ; par ailleurs, ces Exigences de sécurité seront régies par les conditions du Contrat et tous les termes et expressions utilisés dans ces Exigences de sécurité auront la même signification que celle qui leur est donnée dans le Contrat.

1.3 Les présentes Exigences de sécurité viennent s'ajouter aux, et s'appliquent sans préjudice des, autres obligations incombant au Fournisseur aux termes du Contrat (y compris, notamment, les obligations citées dans les Conditions intitulées « **Confidentialité** », « **Protection des données personnelles** » et « **Conformité** »).

PARTIE 2 : EXIGENCES D'ACCÈS LIMITÉ

2 EXIGENCES D'ACCES LIMITE

Cette section sera considérée comme applicable lorsque le Fournisseur fournira des Fournitures impliquant un accès limité aux Informations de BT ou des Clients de BT, ou dispose d'un accès de niveau utilisateur aux Systèmes administratifs de BT. Les Fournisseurs relevant de cette catégorie ne seront tenus de se conformer à aucune autre partie du présent document.

2.1 Sans préjudice d'autres obligations de confidentialité auxquelles il pourrait être tenu, lorsque le Fournisseur ou le Personnel sous contrat ont accès aux Informations de BT, le Fournisseur doit :

2.2 Garantir que les Informations de BT ne sont pas divulguées au Personnel sous contrat, et que ce dernier n'y a pas accès, sauf dans les limites strictement nécessaires pour fournir les Fournitures ; et

2.3 Mettre en place tous les systèmes et processus (d'ordre technique et organisationnel) nécessaires, conformément aux Bonnes pratiques du secteur en matière de sécurité, en vue de protéger la sécurité et la confidentialité des Informations de BT et des Systèmes de BT.

PARTIE 3 : EXIGENCES GÉNÉRALES DE SÉCURITÉ

Le Fournisseur doit satisfaire à cette section lorsqu'il est considéré que la Partie 2 : « Exigences d'accès limité » ne s'applique pas.

3 CONSIDERATIONS GENERALES EN MATIERE DE SECURITE DES INFORMATIONS

Considérations générales en matière de sécurité des informations

3.1 Le Fournisseur doit mettre en œuvre tous les systèmes et processus (d'ordre technique et organisationnel) afin de :

3.1.1 protéger la sécurité et la confidentialité des Informations de BT et des Systèmes de BT comme le prévoient les présentes Exigences de Sécurité ;

3.1.2 garantir la disponibilité, la qualité, l'intégrité et la capacité adaptée pour fournir les Fournitures, sans interruption, tel que l'exigent les Bonnes pratiques du secteur en matière de sécurité.

3.2 Le Fournisseur doit mettre en œuvre un processus informatique documenté de gestion des modifications en vue de garantir que toutes les modifications des processus et des Systèmes du Fournisseur mises en place maintiennent la conformité du Fournisseur vis-à-vis de ces Exigences de sécurité.

3.3 Sur demande écrite de BT, le Fournisseur doit transmettre à BT, des copies de toutes les certifications de sécurité et déclarations de conformité applicables aux Fournitures afin de prouver qu'elles sont conformes aux présentes Exigences de sécurité.

3.4 Le Fournisseur adoptera toutes les mesures raisonnables afin de garantir qu'une(que des) personne(s) compétente(s) sera(ont) nommée(s) et assumera(ont) ses(leurs) responsabilité(s) en tant qu'Interlocuteur pour toutes les questions relatives au Risque en matière de sécurité, à la Gestion des incidents et à la Gestion de la conformité. Le Fournisseur devra communiquer au Contact de Sécurité de BT les coordonnées de cette(ces) personne(s) et toute éventuelle modification de ces coordonnées. Le Fournisseur devra transmettre les informations suivantes :

nom, responsabilité, poste et adresse électronique du groupe et/ou numéro de téléphone.

3.5 Le Fournisseur reconnaît et accepte que, de temps en temps, BT pourra apporter des modifications raisonnables aux Exigences de sécurité de BT, si :

3.5.1 le Fournisseur fait l'objet d'une fusion, d'une acquisition ou d'un changement notable de son actionnariat ou contrôle ;

3.5.2 un changement survient au niveau des normes de sécurité technologiques ou industrielles ; ou

3.5.3 un changement matériel quel qu'il soit survient au niveau des Fournitures ou de la manière dont elles sont fournies

(chacune de ces circonstances constituant une « **Modification des Exigences de sécurité** »).

Sur réception d'une notification écrite de BT exprimant la nécessité d'une Modification des Exigences de sécurité, le Fournisseur devra appliquer ladite Modification des Exigences de sécurité dans les meilleurs délais, et dans tous les cas dans un délai raisonnable (ce délai raisonnable devant être considéré en fonction de la nature de la modification et du risque pour BT).

3.6 Le Fournisseur doit, au moins une fois par an ou dès que des modifications matérielles, quelles qu'elles soient, se produisent sur les Fournitures ou la manière dont elles sont fournies, réexaminer les Exigences de sécurité afin de s'assurer qu'il continue à les respecter intégralement.

3.7 Si le Fournisseur sous-traite certaines de ses obligations aux termes du Contrat, le Fournisseur doit s'assurer que tous les contrats passés avec les sous-traitants concernés comportent des conditions écrites requérant au sous-traitant de respecter les Exigences de sécurité des fournisseurs de BT dans la mesure où elles sont applicables. Ces conditions doivent être mises en place entre le Fournisseur et son sous-traitant avant que le sous-traitant ou son personnel n'accède aux Systèmes de BT et aux Informations de BT.

Utilisation des Informations de BT

3.8 Le Fournisseur ne pourra utiliser les Informations de BT à d'autres fins que celles pour lesquelles elles ont été transmises au Fournisseur et uniquement dans la mesure nécessaire pour permettre au Fournisseur d'exécuter le Contrat. Si le Fournisseur traite des Données personnelles, il ne devra en aucun cas utiliser des Données personnelles faisant partie des Informations de BT à d'autres fins que celles qui ont été indiquées dans l'Annexe relative au traitement.

3.9 Le Fournisseur pourra conserver les Informations de BT pendant toute la durée nécessaire à l'exécution du Contrat, après quoi il ne pourra les conserver plus de deux ans, sauf si une autre période de conservation a été convenue entre BT et le Fournisseur, ou est requise en vertu des lois applicables. Pour éviter toute ambiguïté, quand le Fournisseur traite des Données personnelles, il ne devra pas conserver les Données personnelles qui font partie des Informations de BT au-delà des délais indiqués dans l'Annexe relative au traitement ou dans les Conditions intitulées **« Protection des Données personnelles** ».

3.10 Le Fournisseur doit respecter toutes les politiques et normes applicables disponibles à l'adresse :

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

3.11 Si les Fournitures sont fournies dans le cadre d'un contrat avec le gouvernement du Royaume-Uni, le Fournisseur doit respecter la dernière version de la certification « Cyber Essentials Plus ».

Traitement de l'information

3.12 Le Fournisseur doit posséder et suivre des processus de traitement de l'information correspondant fidèlement au document « 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement) et garantissant au moins que le Fournisseur :

3.12.1 applique les processus appropriés afin de prévenir la distribution non autorisée des Informations de BT sous quelque forme que ce soit, y compris par e-mail, fax, via les réseaux sociaux, sous format papier ou par courrier (par exemple en s'assurant qu'une politique « du bureau propre et de l'écran vide » est en vigueur et que des Informations strictement confidentielles ne sont en aucun cas transmises par fax ou par e-mail) ;

3.12.2 ne mentionne pas les Informations de BT lors des réunions, à moins que tous les participants : (i) aient été autorisés à assister à la réunion ; (ii) aient besoin d'avoir connaissance des informations abordées ; et (iii) aient conscience et tiennent compte de leurs obligations de confidentialité ;

3.12.3 n'enregistre pas les Informations de BT :

3.12.3.1 dans le nuage ou avec des services Internet y compris, notamment, Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin ou Facebook, sauf s'il en a été convenu autrement par écrit avec BT ;

3.12.3.2 sur un ordinateur portable ou un autre dispositif, sauf s'il est protégé par une fonctionnalité complète de cryptage de disque (comme BitLocker) conforme aux normes citées au paragraphe 3.15 ; ou

3.12.3.3 supprime ou place des Informations de BT au-delà de la pratique commerciale habituelle en toute sécurité.

Contrôle des accès

3.13 Le Fournisseur doit maintenir des contrôles des accès aux Systèmes du Fournisseur adaptés à l'environnement et à la nature des Fournitures fournies à BT, y compris en garantissant, s'il y a lieu, que :

3.13.1 tous les utilisateurs, y compris les utilisateurs du niveau administrateur, ont une ID unique ;

3.13.2 les mots de passe sont modifiés régulièrement (au moins tous les 90 jours) ;

3.13.3 des protections adaptées sont mises en place après des tentatives d'accès infructueuses, en vue de prévenir les attaques par force brute ;

3.13.4 les comptes non utilisés sont automatiquement désactivés ;

3.13.5 les mots de passe ont une force appropriée (avec au moins 8 caractères requis, dont trois caractères appartenant aux catégories suivantes : (i) majuscule ; (ii) minuscule ; (iii) numérique ; et (iv) non alphanumérique) et qu'un historique des mots de passe est enregistré afin d'empêcher l'utilisation de mots de passe précédents pendant 12 mois ;

3.13.6 un accès aux Systèmes du Fournisseur basé sur le profil de l'utilisateur est mis en place, avec au moins des contrôles des accès plus rigoureux pour les administrateurs ; et

3.13.7 que des révisions et audits réguliers des accès des utilisateurs sont effectués.

Accès à distance

3.14 Le Fournisseur ne peut en aucun cas autoriser le Personnel sous contrat à accéder à distance aux informations classées comme strictement confidentielles, sauf s'il en a été convenu autrement par écrit avec BT. Lorsqu'un accès à distance est autorisé, le Fournisseur doit garantir que cet accès à distance fait l'objet des contrôles de sécurité appropriés au sein de l'organisation du Fournisseur, et notamment en veillant à ce que les utilisateurs n'accèdent à distance que via une authentification rigoureuse à deux facteurs. Si, à des fins d'assistance, un accès à distance via des réseaux publics est utilisé, les connexions seront cryptées conformément aux normes citées dans le paragraphe 3.15.

Transmission de données

3.15 La transmission régulière de Registres en bloc des Informations de BT devra avoir lieu via PGP ou une plateforme de transmission approuvée dans le secteur.

Cryptage

3.16 Le Fournisseur doit garantir que les Informations de BT classées comme Confidentielles et Strictement confidentielles sont cryptées, lorsqu'elles sont stockées et lorsqu'elles sont en transit, conformément aux Bonnes pratiques du secteur en matière de sécurité, en veillant à ce que les normes déclarées obsolètes par le secteur ne sont pas utilisées. Les actuelles normes de cryptage approuvées par BT à la Date de début et satisfaisant aux exigences du paragraphe 3.15 sont énumérées dans le document « 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement).

Correctifs

3.17 Le Fournisseur devra posséder et suivre un processus documenté de gestion des correctifs qui devra au moins garantir que le Fournisseur :

3.17.1 déploie des correctifs dans les délais suivants :

Type de correctif	Description	Délai
Correctifs critiques	Correctifs nécessaires pour lutter contre les vulnérabilités immédiates de type « zero-day ».	Dès que possible et dans tous les cas 14 jours après la date de mise sur le marché du correctif.

Correctifs importants	Vulnérabilités classées comme Élevées 7.0 - 8.9 sur l'échelle de classement d'importance qualitative du système d'évaluation standardisé de la criticité des vulnérabilités (Common Vulnerability Scoring System - CVSS)	Dans les 30 jours après la date de mise sur le marché du correctif.
Autres correctifs	Tous les correctifs qui ne sont pas classés comme importants ou critiques.	Dans les 8 jours après la date de mise sur le marché du correctif.

3.17.2 est attentif aux versions de correctifs mises sur le marché par les fournisseurs ;

3.17.3 utilise des correctifs qu'il obtient auprès de : fournisseurs directement pour les systèmes et les correctifs propriétaires qui sont soit (i) signés numériquement ou (ii) vérifiés via l'utilisation d'un cryptage de fournisseur (les cryptages MD5 ne doivent pas être utilisés) pour les paquets de mise à jour afin que le correctif puisse être identifié comme provenant d'une communauté d'assistance réputée pour un logiciel libre ;

3.17.4 teste tous les correctifs sur des systèmes qui représentent précisément la configuration des systèmes de production cible avant le déploiement du correctif sur les systèmes de production et vérifie le fonctionnement correct du service corrigé après toute mise en place d'un correctif ; et

3.17.5 assure la maintenance et la mise à jour des Systèmes du fournisseur afin de garantir que les derniers correctifs des fournisseurs peuvent s'appliquer.

3.18 Si un système ne peut être corrigé par le Fournisseur, ce dernier devra le communiquer à BT par écrit. Sur réception de cette notification, BT examinera le risque pour BT et pour les Informations de BT associé à l'utilisation continue par le Fournisseur du système ; BT pourra ensuite demander au Fournisseur d'entreprendre les mesures nécessaires (aux frais du Fournisseur) pour faire face à ces risques.

Gestion des vulnérabilités

3.19 Le Fournisseur devra posséder et suivre un processus de gestion des vulnérabilités qui devra au moins garantir que le Fournisseur :

3.19.1 adopte les mesures pertinentes (par exemple des analyses) pour identifier les vulnérabilités ;

3.19.2 effectue ses propres simulations d'intrusion régulièrement et en conserve les rapports ; et

3.19.3 réagit à toute notification de vulnérabilité et adopte des plans d'action pour atténuer les vulnérabilités conformément aux paragraphes 3.22 et 3.27.

Simulation d'intrusion

3.20 Le Fournisseur doit :

3.20.1 autoriser BT (ou les sous-traitants de BT autorisés à cet effet) à effectuer des simulations d'intrusion raisonnables, sur préavis raisonnable ; et

3.20.2 fournir à BT un accès aux rapports de simulation d'intrusion du Fournisseur existants concernant les Fournitures fournies.

Audit et enregistrements

3.21 Le Fournisseur devra posséder et suivre un processus d'audit et de connexion qui devra au moins garantir que le Fournisseur enregistre (le cas échéant) les événements suivants :

3.21.1 le début et la fin du processus enregistré ;

3.21.2 les modifications du type d'événements enregistrés selon les besoins de la piste d'audit (par exemple les paramètres de démarrage et toute modification de ces derniers) ;

3.21.3 Le démarrage et l'arrêt des Systèmes du fournisseur ;

3.21.4 Les connexions fructueuses ;

3.21.5 Les tentatives de connexion infructueuses (par exemple erreurs d'ID ou de mot de passe) ;

3.21.6 toutes les opérations effectuées par des utilisateurs privilégiés (par exemple ceux qui disposent d'un accès supérieur aux utilitaires ou applications du système) ;

3.21.7 les augmentations des droits fructueuses et infructueuses ;

3.21.8 tous les accès du Fournisseur ou du Personnel sous contrat du Fournisseur aux Informations strictement confidentielles ou toutes les opérations sur ces dernières ; et

3.21.9 la création, la modification et la suppression de comptes d'utilisateurs ;

3.22 Pour chaque événement vérifiable, le Fournisseur doit conserver une piste d'audit inviolable permettant la reconstruction de ces événements.

3.23 En fonction du niveau de risque du composant/des données, le Fournisseur doit régulièrement inspecter et analyser les journaux d'audit afin de détecter des comportements suspects ou anormaux et de prendre les mesures appropriées et/ou de déclencher une alarme.

3.24 Toutes les alarmes doivent être documentées et gérées rapidement en fonction du niveau de risque de l'alarme.

3.25 Le Fournisseur doit conserver les fichiers journaux pendant 3 mois (sauf mention contraire conformément à la Condition intitulée « **Protection des données personnelles** ») et doit fournir des copies ou autoriser BT à accéder aux fichiers journaux, sur demande de BT, sous un format convenu entre les Parties.

Gestion des menaces et des incidents

3.26 Le Fournisseur doit posséder et suivre un processus formel de gestion des incidents de sécurité définissant clairement les responsabilités pour gérer un Incident de sécurité majeur. Toutes les informations relatives aux Incidents de sécurité majeurs devront être traitées « **confidentiellement** ».

3.27 Le Fournisseur doit informer le Contact de sécurité de BT et le Contact commercial de BT, dans un délai raisonnable à partir du moment où il a connaissance d'un Incident de sécurité majeur, et dans tous les cas, pas au-delà de douze (12) heures à compter de l'heure à laquelle le Fournisseur a connaissance de l'Incident de sécurité majeur.

3.28 Sans retard déraisonnable, le Fournisseur adoptera rapidement l'action corrective appropriée pour atténuer tous les risques et toutes les conséquences liés à l'Incident de sécurité majeur afin de réduire la gravité et la durée de l'incident.

3.29 Le Fournisseur s'engage à fournir toutes les informations raisonnablement requises par BT concernant un Incident de sécurité majeur, y compris notamment :

3.29.1 la date et l'heure ;

3.29.2 le lieu ;

3.29.3 le type d'incident ;

3.29.4 l'impact ;

3.29.5 la classification des informations touchées ;

3.29.6 l'état ; et

3.29.7 le résultat (y compris les recommandations de résolution ou mesures adoptées).

3.30 Le Fournisseur doit s'assurer que les risques identifiés concernant la confidentialité, l'intégrité ou la disponibilité des Informations de BT dans les processus du Fournisseur ou les Systèmes du fournisseur sont rapidement maîtrisés.

3.31 Si un Incident de sécurité majeur est aussi une Violation des données personnelles, le Fournisseur doit également respecter les clauses de la Condition intitulée « **Protection des données personnelles** » en plus des clauses des présentes Exigences de sécurité. Pour éviter toute ambiguïté, le Fournisseur doit également respecter les clauses de la Condition intitulée « **Protection des données personnelles** » si une Violation des données personnelles se produit, que cette violation soit ou non un Incident de sécurité majeur.

4 SECURITE DU PERSONNEL SOUS CONTRAT

4.1 L'Accès ne devra pas être accordé au Personnel sous contrat avant que ce dernier n'ait suivi la Formation sur la sécurité des informations de BT, laquelle est disponible à l'adresse https://workingwithbt.extra.bt.com ou dans le système de formations de BT si un numéro d'identification BT a été octroyé au Personnel sous contrat. La Formation sur la sécurité des informations de BT doit être remise à jour régulièrement, comme le prévoit https://workingwithbt.extra.bt.com. Le Fournisseur doit conserver les registres des formations et permettre à BT d'y accéder à des fins d'audit.

4.2 Le Fournisseur doit s'assurer que tout le Personnel sous contrat signe un accord de confidentialité prévoyant des obligations raisonnablement similaires à celles qui sont imposées au Fournisseur dans la Partie 2 ci-dessus, avant que le Personnel sous contrat ne commence à travailler dans les bâtiments de BT ou sur les Systèmes de BT ou n'accède aux Informations de BT. Le Fournisseur doit conserver ces accords de confidentialité signés et permettre à BT d'y accéder à des fins d'audit.

4.3 Le Fournisseur doit gérer les manquements aux politiques et procédures de sécurité du Fournisseur et de BT, via des processus formels incluant des actions disciplinaires susceptibles de décréter l'interdiction pour la personne commettant le manquement :

4.3.1 d'accéder aux Systèmes de BT ou aux Informations de BT ; ou

4.3.2 d'effectuer des tâches liées à la fourniture des Fournitures.

De plus, le Fournisseur doit s'assurer que des processus pertinents sont en place pour garantir que tout Personnel sous contrat ayant été expulsé ne puisse en aucun cas être autorisé ultérieurement à accéder aux Systèmes de BT, aux Informations de BT ou à travailler en lien avec la fourniture des Fournitures.

4.4 Le Fournisseur doit, dans la mesure permise par la loi, posséder une ligne d'assistance confidentielle, ouverte à tout son personnel, que le Personnel sous contrat pourra joindre s'ils reçoivent des instructions contraires ou allant à l'encontre de ces Exigences de sécurité. Les rapports pertinents doivent être communiqués au Contact de sécurité de BT.

4.5 Lorsque le Personnel sous contrat n'est plus assigné aux Fournitures, le Fournisseur doit s'assurer que :

4.5.1 ses accès aux Informations de BT sont révoqués ; et

4.5.2 à discrétion de BT, les Actifs physiques de BT ou les Informations de BT que possède le Personnel sous contrat sont :

4.5.2.1 rendus à l'équipe opérationnelle de BT concernée ; ou

4.5.2.2 détruits conformément à la dernière version du document « 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement).

4.6 Sauf s'il en a été convenu autrement par écrit avec le Contact de sécurité de BT, le Fournisseur doit mettre en place une procédure de sortie contrôlée pour le Personnel sous contrat incluant la demande écrite au Contact de sécurité de BT du retrait des droits d'accès aux Systèmes de BT, aux Informations de BT et tout autre Accès. Le Personnel sous contrat doit être averti que son accord de confidentialité reste en vigueur et que les Informations de BT acquises au cours de son travail concernant les Fournitures ne doivent en aucun cas être divulguées.

4.7 Dans le cadre de l'octroi des droits d'Accès, le Fournisseur doit conserver et fournir les registres de tout le Personnel sous contrat nécessitant un accès ou impliqué dans la fourniture des Fournitures à BT, et notamment nom, lieu de travail, adresse électronique professionnelle, numéro de téléphone professionnel direct et extension (le cas échéant) et/ou numéro de téléphone portable, date à laquelle le numéro d'utilisateur (UIN) a été demandé (si la personne en possède un), date à laquelle la personne a été assignée à la fourniture des Fournitures pour BT, date à laquelle elle a suivi la formation obligatoire, date à laquelle elle a cessé de fournir les Fournitures et une déclaration de vérification préalable à l'embauche. Il revient au Contact de sécurité du Fournisseur de s'assurer à tout moment que seul le Personnel sous contrat est Autorisé.

4.8 Le Fournisseur disposer de politiques et de processus en vigueur pour garantir que le Personnel sous contrat n'utilise pas les réseaux sociaux pour publier ou poster en ligne des déclarations, commentaires, contenus ou images qui :

4.8.1 pourraient raisonnablement être considérés comme étant l'opinion de BT ;

4.8.2 divulguent des Informations de BT considérées comme Informations confidentielles ou classées comme Confidentielles ou Strictement confidentielles ; et

4.8.3 sont diffamatoires envers BT, et pourraient être préjudiciables pour la marque et la réputation de BT.

5 AUDITS ET ANALYSES DE SECURITE

5.1 Sans préjudice de tout autre droit d'audit dont dispose BT, afin de vérifier que le Fournisseur respecte bien les Exigences de sécurité, et lorsque la Condition intitulée « **Protection des informations personnelles** » s'applique, BT, ou les représentants qu'il désignera, se réserve le droit d'effectuer un audit de vérification de la conformité en matière de sécurité, de temps en temps, concernant un aspect ou tous les aspects des politiques, processus et système(s) du Fournisseur (étant entendu que le Fournisseur veillera à la confidentialité des informations n'étant pas liées à la fourniture des Fournitures à BT), sous la forme d'une analyse de sécurité documentaire ou sur le(s) site(s) du Fournisseur ou de ses éventuels sous-traitants matériellement impliqués dans la fourniture des Fournitures ou dans l'exécution du Contrat.

5.2 Le Fournisseur permettra à BT, ou à ses représentants, d'accéder et lui fournira l'assistance nécessaire et appropriée, afin de réaliser les analyses de sécurité de type documentaire ou les audits sur site prévus. Un préavis d'au moins 30 jours ouvrables sera donné au Fournisseur avant un audit sur site de routine ; cependant, pour éviter toute ambiguïté, si une

Violation des données personnelles ou une Violation majeure de sécurité survient, qu'elle soit réelle ou suspectée, BT ne donnera pas de préavis.

5.3 Le Fournisseur travaillera avec BT pour mettre en place les recommandations convenues et appliquer toute éventuelle action corrective que BT estimera nécessaire, à la suite d'une analyse de sécurité de type documentaire ou d'un audit sur site, dans les 30 jours suivant la notification de ces recommandations ou actions correctives par BT, ou le délai convenu entre les Parties, aux frais du Fournisseur.

5.4 Si BT doit effectuer un audit indépendant du Fournisseur et qu'il ressort de cet audit que le Fournisseur ne respecte pas les principes et les pratiques de la norme ISO/IEC 27001:2013, le Fournisseur devra, à ses frais, entreprendre les actions requises afin d'être conforme à ladite norme et devra rembourser entièrement tous les frais engagés par BT pour réaliser ledit audit.

6 ENQUETE

6.1 Si BT a des raisons de soupçonner que les événements suivants se sont produits :

6.1.1 une Violation des données personnelles ;

6.1.2 une Violation majeure de sécurité ; ou

6.1.3 une Violation des présentes Exigences de sécurité,

BT en informera le Contact de sécurité du Fournisseur et le Fournisseur s'engage, à ses propres frais :

6.1.4 à adopter immédiatement les mesures nécessaires pour enquêter sur cette violation et identifier, prévenir et adopter les mesures raisonnablement nécessaires afin d'atténuer les effets de ladite violation ; et

6.1.5 à effectuer une récupération ou toute autre action nécessaire pour remédier à la violation ;

6.1.6 à fournir à BT les rapports que BT pourra raisonnablement demander à propos des résultats de l'enquête et des mesures adoptées pour remédier ou atténuer la violation.

En cas de violation grave, le Fournisseur devra collaborer pleinement avec BT dans le cadre de toute enquête ou audit qui s'ensuivra, mené par BT, une autorité réglementaire et/ou une agence d'application de la loi. L'enquête ou l'audit inclura (sur préavis raisonnable envoyé par BT au Fournisseur) l'accès aux Informations de BT détenues dans les locaux du Fournisseur ou stockées dans les Systèmes du Fournisseur.

Pendant toute enquête, le Fournisseur devra coopérer avec BT en donnant accès et en apportant son aide selon les besoins et la situation, en vue d'enquêter sur la violation. BT pourra demander une quarantaine au Fournisseur afin d'évaluer les actifs corporels ou incorporels appartenant au Fournisseur, en vue de contribuer à l'enquête et le Fournisseur ne devra pas refuser ou retarder déraisonnablement cette demande.

PARTIE 4 : EXIGENCES DE SÉCURITÉ SPÉCIFIQUES

7 EXIGENCES DE SECURITE GENERIQUES ET POLITIQUE

7.1 Le Fournisseur déclare et affirme que les Systèmes du fournisseur, les Fournitures, les services, processus et sites physiques associés sont conformes, et resteront conformes, à la norme ISO/IEC 27001:2013 et à toute autre version modifiée ou future de ladite norme. Cette conformité doit être garantie, à l'entière discrétion de BT, par :

7.1.1 la certification des ISMS (systèmes de gestion des informations) du Fournisseur par un service d'accréditation du Royaume-Uni (UKAS) ou toute entité de certification équivalente dans un autre pays approuvée lorsque la portée et la déclaration d'applicabilité a été validée par BT ; ou

7.1.2 un audit bilatéral et des processus d'essai spécifiés par BT.

7.2 Le Fournisseur doit envoyer un certificat ISO/IEC 27001 valide au début du Contrat et lors des renouvellements successifs de la certification.

7.3 Si la portée du certificat ou de la déclaration d'application change, à tout moment, le Fournisseur doit envoyer ces modifications à des fins de re-validation en suivant la procédure de contrôle des modifications (ou, à défaut, une procédure de contrôle des modifications via le processus de variation). Le Fournisseur doit communiquer à BT, sous 2 jours ouvrables, toute non-conformité majeure identifiée par l'entité de certification ou par le Fournisseur.

8 SECURITE PHYSIQUE - LOCAUX DE BT

Le Fournisseur doit satisfaire à cette section s'il fournit les Fournitures dans les locaux de BT.

8.1 Tout Personnel sous contrat travaillant dans les locaux de BT doit être en possession, et porter de manière visible, une carte d'identification fournie par le Fournisseur ou par BT prouvant que le Personnel sous contrat a été autorisé (la « **Carte d'accès autorisé** »). Les Cartes d'accès autorisé doivent comporter une photo affichée sur la carte représentant fidèlement l'aspect du Personnel sous contrat. Le Personnel sous contrat pourra également disposer d'une carte d'accès électronique et/ou une carte visiteurs à durée limitée, lesquelles devront être utilisées conformément aux instructions données localement.

8.2 Si une Carte d'accès autorisé a été remise au Personnel sous contrat par BT, le Fournisseur doit communiquer à BT rapidement et, dans tous les cas, dans les 5 jours ouvrables lorsqu'il n'est plus nécessaire pour ce Personnel sous contrat d'accéder aux locaux de BT.

8.3 Seuls les serveurs fabriqués par BT, les PC Webtop de BT et les terminaux de confiance sont autorisés à se connecter directement (branchés dans un port LAN ou par une connexion sans fil) aux domaines de BT. Le Fournisseur ne doit pas (et, le cas échéant, doit s'assurer que le Personnel sous contrat respecte cette interdiction), sans l'autorisation préalable par écrit du Contact de sécurité de BT, connecter un équipement qui n'a pas été approuvé par BT à un domaine de BT quel qu'il soit. Le Contact de sécurité de BT ne donnera l'autorisation écrite qu'après avoir initié le processus de concession de la politique de sécurité au sein de BT. Le Fournisseur doit à tout moment s'assurer qu'aucun équipement personnel appartenant à un Personnel sous contrat ou à tout autre employé (y compris les sous-traitants ou intérimaires) n'est utilisé pour enregistrer, accéder ou traiter des données de BT.

8.4 Aucune Information de BT ne doit être extraite des locaux de BT et aucun équipement ou logiciel ne doit être extrait ou installé dans les locaux de BT, sans l'autorisation préalable de BT.

8.5 Les mesures de protection physique ainsi que les directives de travail dans les locaux de BT doivent être respectées et comprennent notamment l'accompagnement du Personnel sous contrat et l'adoption de pratiques de travail appropriées dans des zones sécurisées.

8.6 Lorsque le Fournisseur est autorisé à fournir à son Personnel sous contrat un accès non-hébergé à des zones situées dans les bâtiments de BT, le signataire autorisé de BT et le Personnel sous contrat doivent respecter le document guide intitulé « **Accès du Fournisseur aux Sites et Bâtiments de BT** » disponible à l'adresse https://groupextranet.bt.com/selling2bt/working/third_party_access/default.htm. De plus, le signataire autorisé de BT et le Personnel sous contrat non-autorisés devront posséder au moins des vérifications préalables au recrutement L2 https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

9 SECURITE PHYSIQUE - LOCAUX DU FOURNISSEUR

Le Fournisseur doit satisfaire à cette section s'il fournit les Fournitures à partir de locaux n'appartenant pas à BT (par ex., le site du Fournisseur ou le site d'un tiers du Fournisseur)

9.1 L'accès aux locaux n'appartenant pas à BT (sites, bâtiments ou zones internes) dans lesquelles les Fournitures sont fournies, ou dans lesquelles les Informations de BT sont stockées ou traitées, ne doit être autorisé qu'au moyen d'une carte d'identification d'un Fournisseur autorisé. Cette carte doit être utilisée à des fins de vérification d'identité dans les locaux applicables, à tout moment, et à ce titre, la photo affichée sur la carte doit représenter fidèlement l'aspect de la personne. Une Carte d'accès électronique autorisé pourra également être remise aux personnes afin d'accéder aux locaux concernés, ou un accès de sécurité par clavier. Le Fournisseur doit posséder des processus pour : l'autorisation, la dissémination des modifications de codes (lesquelles doivent se produire au moins une fois par mois) et des modifications de codes ponctuelles.

9.2 Le Fournisseur doit garantir que cet accès aux locaux n'appartenant pas à BT dans lesquels les Fournitures sont fournies, ou dans lesquels les Informations de BT sont stockées ou traitées, est autorisé et le Fournisseur doit respecter des processus et procédures de sécurité pour contrôler et surveiller le Personnel sous contrat, les visiteurs et d'autres personnes externes, y compris des tiers ayant un accès physique à ces zones (par ex., contrôle environnemental, entretien, compagnies d'alarme, nettoyage).

9.3 Si BT en fait la demande, le Fournisseur doit s'assurer que le Personnel sous contrat se trouve dans une zone séparée et sécurisée par rapport au Personnel du Fournisseur. De plus, le Fournisseur doit garantir que les systèmes et les infrastructures utilisés pour fournir les Fournitures sont intégrés dans un réseau logique dédié. Ce réseau ne doit comporter que les systèmes consacrés à la livraison d'une installation de traitement des données sécurisée.

9.4 Les zones sécurisées dans les locaux du Fournisseur (par ex., les salles de communication réseau), doivent être séparées et protégées par des contrôles d'accès appropriés afin de garantir que seul de Personnel sous contrat autorisé peut accéder à ces zones sécurisées. L'accès à ces zones par le Personnel sous contrat doit être vérifié au moins une fois par mois et une évaluation de l'octroi des droits d'accès à ces zones doit être effectuée au moins une fois par an.

Sur demande de BT, le Fournisseur devra remettre à BT les justificatifs de l'évaluation des risques effectuée. Si ces preuves ne sont pas remise à BT sur demande de cette dernière, alors, à discrétion de BT, une évaluation des risques de l'environnement utilisé pour fournir le Service (comme des centres de données, des zones de traitement des données, des salles informatiques) sera effectuée par BT ou ses représentants, avant que le Fournisseur ne commence à fournir les Fournitures. De plus, si des travaux susceptibles de compromettre la sécurité des informations de BT ont lieu dans les locaux du Fournisseur, ce dernier devra le communiquer à BT.

9.5 Des systèmes de sécurité CCTV, ainsi que leurs supports d'enregistrement, devront être utilisés par le Fournisseur en réponse à des incidents de sécurité, en tant qu'outil de surveillance, en tant que mesure dissuasive ou en tant que moyen de détection d'individus commettant un délit. Si les images de CCTV sont enregistrées (sur une cassette ou numériquement), elles doivent être conservées pendant au moins 20 jours. Toutefois, cette période pourra être prolongée dans les cas suivants :

9.5.1 si les preuves vidéo de CCTV doivent être conservées pour l'enquête d'un incident ou d'un délit ; ou

9.5.2 si la loi le prévoit autrement.

9.5.3 Tous les enregistrements de CCTV doivent être stockés dans une armoire verrouillée et la clé doit être détenue et contrôlée en toute sécurité. L'accès à l'armoire doit être limité au personnel autorisé uniquement.

9.6 Tous les enregistreurs de CCTV doivent être situés dans des conditions sûres afin de prévenir la modification ou la suppression et la possibilité de visualisation par mégarde de tout écran de CCTV, et conformément aux instructions portant sur l'utilisation des systèmes de CCTV, disponible à l'adresse

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

9.7 Toutes les zones des locaux du Fournisseur utilisées pour fournir les Services et les Fournitures doivent être inspectées afin de détecter les éventuels risques et menaces, au moins une fois par mois, par le Fournisseur. Le Fournisseur doit tenir compte et mettre en place toutes les mesures appropriées afin de garantir la sécurité physique concernant les aspects suivants :

9.7.1 connaissance des menaces locales, y compris notamment, les menaces potentielles de l'industrie locale et la proximité de matières dangereuses stockées ; et

9.7.2 les catastrophes naturelles, y compris les risques de menaces telles que les inondations, les glissements de terrain ou les conditions climatiques extrêmes.

9.8 Le câblage d'alimentation et de télécommunication dans les locaux du Fournisseur transportant des données ou alimentant les services d'information ou les services radio/satellite utilisés pour fournir les Fournitures doit être évalué par le Fournisseur afin de déterminer son niveau de protection en vue de prévenir l'interruption des opérations commerciales. Des mesures physiques de protection de sécurité proportionnelles au niveau de risque de l'activité des opérations pour lesquelles elles sont employées doivent être mises en place, comme suit :

9.8.1 la chaussée essentielle à l'activité, le blindage des câbles, les regards ou boîtiers dans lesquels passent des câbles essentiels à l'activité doivent être protégés ;

9.8.2 l'accès aux chambres de raccordement ou armoires à câbles dans les bâtiments opérationnels doit être limité par l'utilisation de lecteurs de contrôle d'accès électronique ou un processus de gestion des clefs efficace ;

9.8.3 les liens de communications informatiques et les équipements de communication dans les installations informatiques doivent être protégés physiquement et contre l'environnement ; et

9.8.4 les liens de communication par radio ou satellite et les équipements de communication doivent être correctement protégés.

9.9 BT pourra demander, sauf s'il en a été convenu autrement entre le Fournisseur et le Contact de sécurité de BT, que des services de gardiennage soient assurés par le Fournisseur afin de compléter les mesures de sécurité électroniques et physiques dans les locaux du Fournisseur, lorsque :

9.9.1 le site a une grande importance opérationnelle (par ex., les centres de contact, les centres de données, les centres de réseaux stratégiques, etc.) ;

9.9.2 Les Informations de BT traitées peuvent avoir un impact ou nuire à la marque et à la réputation de BT ;

9.9.3 un grand volume d'Informations de BT est traité (par ex., en cas d'externalisation des processus de gestion) ;

9.9.4 le client impose des exigences contractuelles ;

9.9.5 il existe un risque/une menace spécifique au site ;

9.9.6 le Fournisseur est en possession d'Informations de BT qui sont particulièrement sensibles.

9.10 Afin de protéger les équipements de BT (comme des serveurs ou des interrupteurs de BT) dans les locaux du Fournisseur contre des menaces ou dangers environnementaux, et contre les éventuels accès non autorisés, les Équipements de BT doivent être situés dans une zone protégée et séparée des équipements utilisés pour des systèmes d'organisations extérieures à BT. Le niveau de séparation doit garantir que la sécurité des équipements de BT ne pourra en aucun cas être compromise, délibérément ou accidentellement, en raison d'un accès accordé à des organisations externes à BT. Ces séparations peuvent par exemple prendre la forme d'une paroi de sécurité, d'armoires verrouillées ou d'un grillage métallique.

9.11 Le Fournisseur doit avoir mis en place toutes les mesures appropriées afin de garantir la sécurité physique concernant les aspects suivants :

9.11.1 mesures de prévention de l'incendie y compris, notamment, des alarmes, des capteurs et des dispositifs de lutte contre l'incendie ;

9.11.2 les conditions climatiques, en tenant compte de la température, de l'humidité et de l'électricité statique et la gestion de ces conditions, leur surveillance et la réponse à des conditions extrêmes (par ex., arrêt automatique, alarmes).

9.11.3 des équipements de contrôle tels que des appareils de climatisation et des détecteurs d'eau ;

9.11.4 la présence de réservoirs d'eau, tuyauteries, etc., dans les locaux ;

9.11.5 des accès contrôlés (le cas échéant, l'accès du personnel aux systèmes doit faire l'objet d'audits) ; et

9.11.6 la supervision du Personnel sous contrat n'étant pas normalement associé à la gestion des Systèmes de BT ou à l'accès à ces derniers.

9.12 Des périmètres de sécurité (des barrières comme des parois, des clôtures, des portes d'entrée contrôlées par carte ou des postes de gardiennage) doivent être mis en place pour protéger les zones contenant des Informations sensibles de BT ou des Informations des clients de BT (y compris des Données personnelles) et ainsi que dans les installations de traitement associées.

9.13 Les points d'accès, comme les sites destinés à la livraison ou au chargement des marchandises, et d'autres points où des personnes non-autorisées pourraient entrer dans les locaux doivent être contrôlés et, si possible, isolés des installations de traitement des informations, afin d'éviter tout accès non-autorisé ou les attaques délibérées.

9.14 Le Fournisseur doit garantir que l'accès physique aux zones ayant accès aux Informations de BT ou aux Informations des clients de BT (y compris des Données personnelles) est contrôlé par des cartes à puces ou à détecteurs de proximité (ou des systèmes de sécurité équivalents) et le Fournisseur doit effectuer au moins une fois par mois des audits internes pour garantir le respect de ces clauses.

9.15 Le Fournisseur doit garantir que les photos et/ou captures d'image des Informations de BT ou des Informations des clients de BT (y compris des Données personnelles) sont strictement interdites. Dans des circonstances exceptionnelles, lorsque la capture de ce type d'images peut s'avérer nécessaire pour les besoins de l'activité commerciale, une exemption temporaire à cette clause doit être obtenue par écrit auprès du Contact de sécurité de BT.

9.16 Le Fournisseur doit suivre une politique du « bureau propre et de l'écran vide » afin de protéger les Informations de BT.

10 FOURNITURE D'EQUIPEMENTS D'HEBERGEMENT

Le Fournisseur doit satisfaire à cette section s'il fournit un environnement d'hébergement pour BT ou des équipements de Clients de BT.

10.1 Le Fournisseur doit, lorsqu'il fournit une zone d'accès sécurisé dans ses locaux pour héberger des équipements de BT ou de Clients de BT (le « **Site du Fournisseur** ») :

10.1.1 garantir que le Personnel sous contrat accédant au Site du Fournisseur possède une carte d'identification ou une carte électronique d'accès contrôlé. Cette carte doit être utilisée à des fins de vérification d'identité dans le Site du Fournisseur, à tout moment, et à ce titre, la photo affichée sur la carte doit représenter fidèlement l'aspect du Personnel sous contrat ; et

10.1.2 avoir mis en place des procédures de gestion des menaces de sécurité à l'encontre des équipements de BT ou de Clients de BT ou d'un tiers travaillant pour le compte de BT, afin de protéger les Informations de BT et de Clients de BT dans le Site du Fournisseur ; et

10.1.3 utiliser des systèmes de sécurité CCTV, ainsi que leurs supports d'enregistrement, sur le Site du Fournisseur en réponse à des incidents de sécurité, en tant qu'outil de surveillance, en tant que mesure dissuasive et en tant que moyen de détection d'individus commettant un délit. Le Fournisseur doit garantir que les enregistrements des systèmes de CCTV sont conservés pendant 20 jours afin de constituer un outil d'enquête efficace ; et

10.1.4 fournir à BT un plan de sol de l'espace alloué dans la zone de sécurité du Site du Fournisseur ; et

10.1.5 garantir que les armoires de BT et des Clients de BT dans le Site du Fournisseur sont verrouillées et que seul le personnel autorisé de BT, les représentants de BT approuvés et le Personnel sous contrat concerné y ont accès ; et

10.1.6 mettre en place un processus de gestion des clefs sûr dans le Site du Fournisseur ; et

10.1.7 inspecter régulièrement la zone locale entourant le Site du Fournisseur afin de détecter les éventuels risques et menaces ; et

10.1.8 documenter et maintenir des procédures opérationnelles (dans la langue du pays dans lequel les travaux pour BT sont exécutés) pour se décharger des exigences de sécurité énumérées dans ce paragraphe 10 et, sur demande, donner à BT accès à ces documents.

10.2 BT doit remettre au Fournisseur :

10.2.1 un registre des actifs physiques de BT et/ou des Clients de BT se trouvant dans le Site du Fournisseur ; et

10.2.2 une liste détaillée des employés, sous-traitants et agents de BT requérant un accès au Site du Fournisseur (de façon permanente).

11 DEVELOPPEMENT DE SERVICES

Le Fournisseur doit satisfaire à cette section s'il se charge du développement des Fournitures destinées à être utilisé par BT et/ou les Clients de BT. Cela inclut les « composants standard », la configuration du logiciel et les composants nécessaires à la fabrication des Fournitures.

11.1 Le Fournisseur doit mettre en place les mesures de sécurité convenues sur tous les composants fournis qui constituent les Fournitures et/ou les Services, de sorte à ce qu'elles protègent la confidentialité, la disponibilité et l'intégrité des Fournitures, et notamment en :

11.1.1 conservant la documentation appropriée (dans la langue du pays dans lequel les travaux pour BT sont exécutés) concernant la mise en place des mesures de sécurité et en garantissant que la documentation et les mesures de sécurité sont conformes aux bonnes pratiques du secteur ;

11.1.2 limitant les possibilités pour des personnes non autorisées (par ex., des hackers) d'accéder aux Systèmes de BT et aux Informations de BT, aux Réseaux de BT ou aux Fournitures de BT ; et

11.1.3 en réduisant le risque de détournement des Systèmes de BT et des Informations de BT, des Réseaux de BT ou des Fournitures de BT, susceptibles d'entraîner un manque à gagner ou une perte de service.

11.2 Le Fournisseur, sur demande de BT, doit démontrer que tout logiciel ou matériel construit (exclusifs et du commerce) livré à BT est le même que celui qui a été convenu avec BT. Le Fournisseur doit veiller à l'intégrité des constructions y compris les mises à jour, les systèmes d'exploitation et l'application de l'usine au bureau.

11.3 Le Fournisseur doit garantir que le développement de systèmes destinés à être utilisés par BT ou la construction et l'entretien du matériel détenu par BT est renforcé conformément aux Exigences en matière de sécurité des systèmes informatiques de BT fournies par l'équipe opérationnelle de BT ou créés selon les bonnes pratiques du secteur.

11.4 Le Fournisseur doit garantir que les systèmes et les processus utilisés pour les activités d'essai et de développement sont séparés des systèmes de production. Un processus de contrôle des modifications doit être utilisé pour la promotion de tout code vis-à-vis de l'environnement de production. Les données d'essai fournies par BT doivent être supprimées après un délai fixé par le propriétaire des données de BT et les données réelles ou de production ne peuvent en aucun cas être utilisées dans des environnements de développement ou d'essai.

11.5 Toutes les vulnérabilités critiques en matière de sécurité mises à jour lors des analyses de sécurité et classées comme présentant un risque moyen ou supérieur doivent être résolues avant le lancement. Toute violation de sécurité dans les Services identifiée par BT ou par le Fournisseur devra être résolue aux frais du Fournisseur, dans les délais raisonnablement fixés par BT.

11.6 Les Fournitures doivent être soumises à une simulation d'intrusion commandée par le Fournisseur avant d'être lancées, au moins une fois par an et après des modifications ou incidents majeurs, aux frais du Fournisseur.

11.7 Les Fournitures développées pour être utilisées par BT ou ses clients doivent être développées en utilisant un Cycle de développement sécurisé (SDLC) reconnu par les normes du secteur afin de limiter les risques d'introduction de vulnérabilités de sécurité dans l'environnement de production et/ou celui des clients. Le SDLC doit inclure les barrières suivantes, avec des artéfacts tangibles résultants de chaque révision et susceptibles d'être inspectés par BT dans le cadre de l'audit prévu au paragraphe 5 de la Partie 3 des présentes Exigences de sécurité :

11.7.1 Évaluation de la sécurité des exigences commerciales ;

11.7.2 Évaluation de la sécurité de la conception ;

11.7.3 Évaluation de la sécurité du code source (automatique et/ou manuel) et ;

11.7.4 audit de sécurité de la solution avant son déploiement (incluant des simulations d'attaques de sécurité) conformément à un plan d'audit spécifique au projet et documenté fondé sur les rapports issus des évaluations de la sécurité des exigences commerciales, de la conception et du code.

Des orientations supplémentaires sont données dans les Normes sur les directives du secteur destinées aux tiers, sur le « Codage sécurisé », disponible à l'adresse

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

12 DEPOT DE SECURITE

Cette question est désormais traitée dans le contrat principal.

13 ACCES AUX SYSTEMES DE BT

Le Fournisseur doit satisfaire à cette section si le Personnel sous contrat du Fournisseur doit accéder aux Systèmes de BT pour fournir les Fournitures.

13.1 BT peut autoriser, à son entière discrétion, un Accès limité lorsque cela est strictement nécessaire pour fournir les Fournitures.

13.2 Concernant l'Accès, le Fournisseur doit respecter toutes les politiques, normes et instructions de BT pertinentes données au Fournisseur et doit (et, veillera à ce que tout le Personnel sous contrat respecte ces obligations) :

13.2.1 s'assurer que l'identification de l'utilisateur, les mots de passe, les PIN, les jetons et les accès de conférence sont attribués à un Personnel sous contrat et ne sont pas partagés. Les données doivent être stockées en toute sécurité et à distance des dispositifs auxquels ils donnent accès. Si une autre personne a connaissance d'un mot de passe, ce dernier doit être modifié immédiatement ;

13.2.2 sur demande raisonnable, donner à BT les rapports que BT pourra raisonnablement demander concernant le Personnel sous contrat autorisé à accéder aux Systèmes de BT ;

13.2.3 les connexions entre domaines vers des Systèmes de BT ne sont pas autorisées, sauf si cela a été spécifiquement approuvé et autorisé par le Contact de sécurité de BT ;

13.2.4 mettre en œuvre tous les efforts raisonnables pour garantir qu'aucun virus ou code malveillant (tel que ces expressions sont généralement comprises dans le secteur informatique) ne puisse s'introduire afin de limiter le risque de corruption des Systèmes de BT ou des Informations de BT par quelque moyen que ce soit ; et

13.2.5 mettre en œuvre tous les efforts raisonnables pour garantir que les fichiers contenant des informations, des données ou des supports n'ayant aucun lien avec les Fournitures ne soient pas enregistrés sur les Équipements de BT, les Serveurs de BT, les ordinateurs portables et de bureau fournis par BT, les installations de stockage centralisé de BT ou les Systèmes de BT.

13.2.6 lorsque BT a fourni au Fournisseur un accès à Internet ou à l'intranet de BT, garantir que le Personnel sous contrat accède à Internet ou à l'intranet de BT convenablement et qu'ils n'utilisent cet accès que pour fournir les Fournitures pertinentes et que des sites inacceptables ou dangereux soient bloqués des utilisateurs. Il relève de la responsabilité du Fournisseur de garantir que les instructions relatives aux abus sur Internet ou par e-mail soient communiquées au Personnel sous contrat au moins une fois par an. Ces instructions doivent expliquer clairement que :

13.2.6.1 les utilisateurs ne doivent pas :

(i) Accéder à des contenus offensants, sexuels, sexistes, racistes ou politiquement offensants ;
(ii) Exécuter des actions susceptibles de porter atteinte à la réputation de BT ou d'autres individus ;
(iii) Diriger une entreprise privée ;
(iv) (d) enfreindre des droits d'auteur ; ou
(v) contourner ou traverser des pare-feu ou d'autres mécanismes de sécurité mis en place par BT ;

13.2.6.2 Le Personnel sous contrat ne doit pas contribuer à des sites ni publier des déclarations en ligne susceptibles d'être raisonnablement considérées comme étant le point de vue de BT.

13.3 Le Fournisseur doit effectuer régulièrement des révisions afin de s'assurer que tout le Personnel sous contrat auquel un Accès a été octroyé en a réellement besoin pour exécuter ses tâches. Des copies de la documentation des révisions doivent être mises à disposition de BT, à des fins d'inspection, dans le cadre de l'audit décrit dans le paragraphe 5.1 :

13.4 Lorsqu'un employé, y compris les sous-traitants et les intérimaires, n'ont plus besoin d'accéder aux Systèmes de BT, par exemple lorsqu'ils quittent l'entreprise ou changent de fonction, le Fournisseur doit le communiquer à BT rapidement et dans tous les cas sous 5 jours ouvrables.

14 ACCES AUX INFORMATIONS DE BT A PARTIR DES SYSTEMES DU FOURNISSEUR

La conformité à cette section est requise si des Informations de BT sont stockées ou traitées sur les Systèmes du Fournisseur.

14.1 Si un Accès aux Systèmes du Fournisseur est octroyé à du Personnel sous contrat afin de fournir les Fournitures et/ou les Services, le Fournisseur doit démontrer qu'il assume sa responsabilité à l'égard de cet Accès (y compris notamment en utilisant des comptes d'utilisateurs uniques, une gestion des mots de passe et une piste/journal d'audit clair pour toutes les actions du Personnel sous contrat).

14.2 Le Fournisseur doit maintenir des systèmes qui détectent et enregistrent toute tentative de dommages, modification ou accès non-autorisé aux Informations de BT à partir des Systèmes du Fournisseur. Par exemple, la connexion au système et des processus d'audit, IDS et PIS, etc.

14.3 Le Fournisseur doit maintenir des contrôles pour détecter et protéger les systèmes contre des logiciels malveillants, des virus et des codes malveillants sur les Systèmes du Fournisseur et garantir que des procédures de sensibilisation de l'utilisateur appropriées sont mises en place.

14.4 Le Fournisseur doit garantir que tout logiciel non-autorisé est identifié et supprimé des Systèmes du Fournisseur en retenant, traitant ou accédant aux Informations de BT au moins une fois par mois.

14.5 Le Fournisseur doit garantir que l'accès aux ports de diagnostic et de gestion, ainsi que des outils de diagnostic, sont bien contrôlés.

14.6 Le Fournisseur doit garantir que l'accès aux outils d'audit du Fournisseur est limité au Personnel sous contrat et que leur utilisation est surveillée.

14.7 Le Fournisseur doit garantir que les révisions des codes et les simulations d'intrusion sur tous les logiciels produits en interne (y compris tout Logiciel) utilisés pour traiter les Informations de BT sont réalisées par une équipe indépendante qui ne doit pas inclure les développeurs du logiciel.

14.8 Dans la mesure où des serveurs sont utilisés pour fournir les Fournitures, ils ne doivent pas être déployés sur des réseaux non-sécurisés (des réseaux hors du périmètre de sécurité, situés au-delà de votre contrôle administratif, par ex., des réseaux connectés à Internet) sans les contrôles de sécurité appropriés.

14.9 Le Fournisseur doit garantir que les modifications aux Systèmes du Fournisseur qui détiennent et traitent des Informations de BT et/ou qui sont utilisés pour fournir les Fournitures, sont contrôlées et sujettes à des procédures formelles de contrôle des modifications.

14.10 Le Fournisseur doit garantir que les horloges et heures du système sont synchronisées en utilisant la dernière version de NTP ou d'une technologie de synchronisation des heures similaire.

14.11 Si le Fournisseur fournit des systèmes qui donnent un accès en ligne aux Clients de BT :

14.11.1 Les identifiants en ligne pour les Clients de BT doivent au moins contenir les éléments suivants :

14.11.1.1 ID d'utilisateur ;

14.11.1.2 mot de passe en ligne ;

14.11.1.3 trois questions et réponses d'authentification pour récupérer l'accès au compte ;

14.11.1.4 une méthode de contact alternative à des fins d'authentification.

14.11.2 Le Client de BT doit être capable de choisir un ID d'utilisateur unique pour ses identifiants en ligne et le mot de passe en ligne ne doit pas contenir son ID d'utilisateur unique.

14.11.3 Le mot de passe en ligne du Client de BT doit avoir une longueur minimum de 8 caractères et contenir au moins 1 caractère des trois ensembles suivants : (i) nombre décimal (0-9) ; (ii) lettre en majuscule (A-Z) ; (iii) lettre en minuscule (a-z) ; (iv) caractère alphanumérique.

14.11.4 Pour modifier un mot de passe en ligne, le Client de BT doit saisir son mot de passe actuel, puis saisir deux fois le nouveau mot de passe.

14.11.5 Lorsqu'un Client de BT oublie son ID d'utilisateur ou son mot de passe, le système fourni par le Fournisseur doit générer un e-mail et l'envoyer à l'adresse électronique enregistrée pour le Client de BT. Cet e-mail contiendra un lien de demande de réinitialisation de l'ID d'utilisateur ou du mot de passe, après avoir renseigné correctement les champs suivants du formulaire en ligne :

14.11.5.1 MSISDN ou numéro de téléphone fixe

14.11.5.2 Mot de passe en ligne

14.11.5.3 ID d'utilisateur de Client de BT

14.11.6 Le lien de demande de réinitialisation de mot de passe doit avoir une durée de validité limitée de 30 minutes au maximum, avant d'expirer, auquel cas une nouvelle demande de réinitialisation de mot de passe devra être envoyée.

14.11.7 Une fois le mot de passe réinitialisé avec succès, le Client de BT doit être contraint de modifier le mot de passe fourni.

14.11.8 La récupération des identifiants d'utilisateur des Clients de BT lorsque l'ID d'utilisateur et le mot de passe ont tous deux été oubliés doit générer un e-mail et l'envoyer à l'adresse électronique. Cet e-mail contiendra un lien de demande de réinitialisation de l'ID d'utilisateur et du mot de passe, après avoir renseigné correctement le prénom et le nom de famille, le numéro de téléphone et l'adresse électronique du Client de BT.

14.11.9 Des niveaux supérieurs d'authentification des clients pourront être requis en fonction de la sensibilité des données et des fonctionnalités auxquelles les utilisateurs ont accès.

15 FOURNISSEUR HEBERGEANT DES INFORMATIONS DE BT

Le Fournisseur doit satisfaire à cette section s'il héberge en externe des Informations de BT classées comme « Confidentielles » ou « Strictement confidentielles » dans un environnement de services dans un nuage ou un environnement de serveurs de Fournisseurs ou Sous-traitants.

15.1 Le Fournisseur doit, à l'égard des Fournitures, garantir que les environnements dans lesquels des Informations de BT sont hébergées satisfont aux Exigences relatives à l'hébergement externe de données par des tiers, disponible à l'adresse :

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

16 SECURITE DES RESEAUX

Le Fournisseur doit satisfaire à cette section s'il construit, développe ou supporte des Réseaux de BT ou des Actifs en réseau.

16.1 Le Fournisseur doit, à l'égard des Fournitures, mettre en place les mesures de sécurité convenues sur tous les composants fournis, de sorte à ce qu'elles préservent la confidentialité, la disponibilité et l'intégrité des Réseaux de BT et/ ou des actifs de 21CN. Le Fournisseur fournira à BT toute la documentation concernant la mise en place du Réseau de sécurité s'appliquant aux Fournitures et devra garantir qu'il :

16.1.1 est conforme, et garantir que le Réseau de sécurité dont le Fournisseur est responsable est conforme, à toutes les exigences légales et réglementaires ;

16.1.2 met en œuvre tous les efforts raisonnables pour empêcher aux individus non-autorisés (comme les hackers) d'accéder aux Éléments de gestion du réseau et à d'autres éléments accessibles via le Réseau de BT et/ou le 21Cn ; et

16.1.3 met en œuvre tous les efforts raisonnables pour réduire le risque de détournement des Réseaux de BT et/ou 21CN par les individus autorisés à y accéder et qui pourrait entraîner un manque à gagner ou une perte de service ; et

16.1.4 met en œuvre tous les efforts raisonnables pour détecter les éventuelles violations de sécurité susceptibles de se produire en garantissant une rectification rapide de toute violation ; il s'engage également à identifier les individus qui ont obtenu un accès et à déterminer comment ils ont obtenu l'autorisation ; et

16.1.5 réduit le risque de configuration inadéquate des Réseaux de BT par exemple en n'octroyant que les permissions minimum requises pour exécuter les tâches propres à une fonction.

16.2 Le Fournisseur doit prendre toutes les mesures raisonnables pour sécuriser toutes les interfaces sur les Fournitures et/ou les Services, et ne doit pas considérer que les composants fournis sont utilisés dans un environnement sécurisé.

16.3 Le Fournisseur doit fournir au Contact de sécurité de BT les noms, adresses (et toutes les autres informations que BT pourra lui demander) de tout le Personnel sous contrat devant de temps en temps être impliqué dans le déploiement, la maintenance et/ou la gestion des Fournitures avant que ces personnes ne soient effectivement impliquées dans ces opérations de déploiement, maintenance et/ou gestion.

16.4 Concernant ses activités d'assistance basées au Royaume-Uni, le Fournisseur doit avoir une équipe de sécurité compétente comprenant au moins un ressortissant du Royaume-Uni qui sera disponible pour assurer la liaison avec le

Contact de Sécurité de BT (ou les personnes qu'il désignera) et l'équipe assistera aux réunions que le Contact de sécurité de BT convoquera raisonnablement de temps en temps.

16.5 Le Fournisseur fournira au Contact de sécurité de BT un planning (mis à jour régulièrement selon les besoins) des composants actifs compris dans les Fournitures et/ou les Services ainsi que leurs sources respectives.

16.6 Le Fournisseur fournira les informations de son personnel qui sera en liaison avec l'équipe de gestion des vulnérabilités de BT (CERT) concernant la discussion sur les vulnérabilités identifiées par BT et par le Fournisseur au niveau des Fournitures et/ou des Services. Le Fournisseur fournira à BT en temps et en heure des informations sur les vulnérabilités, et adoptera les mesures nécessaires pour être conforme (aux frais du Fournisseur) aux exigences raisonnables concernant les vulnérabilités qui lui seront communiquées par le Contact de sécurité de BT de temps en temps. Le Fournisseur communiquera à BT les éventuelles vulnérabilités suffisamment à l'avance afin de pouvoir appliquer ou installer les contrôles nécessaires avant que le Fournisseur ne communique publiquement les vulnérabilités.

16.7 Le Fournisseur accordera au Contact de sécurité de BT et aux personnes que ce dernier désignera, de temps en temps, un accès complet et sans restriction aux locaux dans lesquels les Fournitures sont développées, fabriquées ou créées afin d'exécuter les analyses et/ou évaluations de la conformité en matière de sécurité, et le Fournisseur devra coopérer (et s'assurer que tout le Personnel sous contrat concerné coopère) dans le cadre de ces analyses de la conformité en matière de sécurité.

16.8 Le Fournisseur doit garantir que tous les composants liés à la sécurité compris dans les Fournitures identifiés par BT de temps en temps soient, aux frais du Fournisseur, évalués indépendamment à la satisfaction raisonnable de BT.

16.9 À l'égard de toute Information fournie par ou obtenue auprès de BT et classée comme « **STRICTEMENT CONFIDENTIELLE** » ou facilement interprétée comme étant confidentielle, le Fournisseur doit garantir que :

16.9.1 l'accès à ces Informations ne soit donné qu'au Personnel sous contrat spécifiquement autorisé par BT pour voir et traiter ces Informations, et garder une trace écrite de ces accès ;

16.9.2 ces Informations soient traitées, utilisées et enregistrées avec grand soin et cryptées avant d'être enregistrées au moyen de PGP ou WinZip 9, et dans des conditions garantissant un niveau élevé de résistance aux compromissions délibérées (c.-à-d., en utilisant l'algorithme de cryptage le plus fort disponible / en utilisant un mot de passe robuste) et rendant les tentatives de compromission ou les compromissions réelles très facilement détectables ;

16.9.3 une fois ces Informations transmises, que des mesures de sécurité adaptées sont appliquées à ces Informations en les cryptant via Secure Email, PGP ou WinZip 9 ; et

16.9.4 que ces Informations ne sont pas, sans l'autorisation écrite de BT, exportées hors de l'Espace Économique Européen.

16.10 Le Fournisseur doit rapidement, et dans tous les cas sous 7 jours ouvrables, fournir au Contact de sécurité de BT toutes les informations concernant des options et/ou fonctionnalités des Fournitures (ou devant être dans la Feuille de route des Fournitures), de temps en temps :

16.10.1 dont le Fournisseur a connaissance ; ou

16.10.2 qui sont raisonnablement considérées par le Contact de sécurité de BT, et ainsi présentées explicitement au Fournisseur, comme conçues pour, ou susceptibles d'être utilisées pour, l'interception légale ou toute autre interception des télécommunications. Ces informations incluront toutes les Informations raisonnablement nécessaires pour permettre au Contact de sécurité de BT de comprendre pleinement la nature, la composition et la portée de ces options et/ou fonctionnalités.

16.11 Afin de maintenir l'accès aux Réseaux et/ou systèmes de BT, le Fournisseur devra communiquer à BT immédiatement toute modification de sa méthode d'Accès via les pare-feu, y compris la fourniture d'une traduction d'adresses de réseau.

16.12 Le Fournisseur ne doit en aucun cas utiliser des outils de surveillance du réseau capables de voir les informations des applications.

16.13 Le Fournisseur doit garantir que la fonctionnalité IPv6 incluse dans les systèmes d'exploitation est désactivée sur les hébergeurs (par exemple les dispositifs ou serveurs de l'utilisateur final) qui se connectent au Réseau et domaines de BT lorsqu'elle n'est pas nécessaire.

16.14 Le Fournisseur doit satisfaire, et garantir que les Fournitures et les Services satisfont, aux politiques de BT quand elles sont transmises et aux Exigences de sécurité. Toute non-conformité doit être convenue entre les Parties au moment de la signature du Contrat ou via une procédure de contrôle des modifications (ou équivalent).

16.15 Le Fournisseur doit garantir que tout le Personnel sous contrat possède des vérifications préalables au recrutement appropriées au niveau d'Accès, tel que cela est défini dans https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

Les Fournisseurs qui construisent, développent ou assurent l'assistance des Réseaux de BT ou des Actifs en réseau doivent garantir que tout le Personnel sous contrat possède au moins des vérifications préalables au recrutement L2. Les vérifications préalables au recrutement L3 seront requises pour les postes identifiés par le Contact de sécurité de BT. Si le Fournisseur n'est pas en mesure d'attester directement la sécurité du Personnel sous contrat, dans le cadre des vérifications L3, BT l'aidera en obtenant l'attestation aux frais du Fournisseur.

16.16 Le Fournisseur doit veiller à ce que le matériel et le logiciel restent conformes aux spécifications du fabricant.

16.17 Le Fournisseur ne doit en aucun cas utiliser des supports amovibles (disques, clefs USB, etc.) destinés à l'assistance et à la maintenance à d'autres fins.

17 SECURITE DU RESEAU DU FOURNISSEUR

Le Fournisseur doit satisfaire aux clauses de cette section si le réseau du Fournisseur est destiné à être utilisé pour fournir les Fournitures (y compris les réseaux LAN, WAN, Internet, sans fil et radio).

17.1 Le Fournisseur doit, concernant les Fournitures ou les Services, mettre en place des mesures de sécurité sur ses réseaux, de sorte à ce qu'elles préservent la confidentialité, la disponibilité et l'intégrité des Informations de BT. Ces mesures doivent et le Fournisseur doit :

17.1.1 satisfaire à toutes les exigences légales et réglementaires ; et

17.1.2 mettre en œuvre tous les efforts raisonnables pour empêcher que des individus non-autorisés (par ex., des hackers) n'accèdent au(x) Réseau(x) du Fournisseur ;

17.1.3 mettre en œuvre tous les efforts raisonnables pour réduire le risque de détournement du(des) Réseau(x) du Fournisseur par les individuels autorisés à y accéder qui pourraient entraîner un manque à gagner ou une perte de service ; et

17.1.4 mettre en œuvre tous les efforts raisonnables pour détecter les éventuelles violations de sécurité et garantir une rectification rapide de toute violation, tout en identifiant les individus qui ont obtenu un accès et en déterminant comment ils ont obtenu l'autorisation ; et

17.2 Les mesures appropriées doivent être mises en place pour garantir la sécurité des composants, y compris notamment :

17.2.1 l'utilisation de principes de **défense en profondeur** » efficaces ;

17.2.2 l'utilisation de contrôles en place empêchant toute attaque délibérée ;

17.2.3 l'utilisation de pare-feu, routeurs, interrupteurs ;

17.2.4 communications sécurisées entre les dispositifs et les postes de gestion ;

17.2.5 communications sécurisées entre les dispositifs, selon les besoins (y compris le cryptage de tous les accès administrateur hors console) ;

17.2.6 une conception de l'architecture robuste, avec différents niveaux et différentes zones, une gestion des identités robuste efficace et utilisant une configuration de système devant être correctement renforcée et documentée ;

17.2.7 désactivation (lorsque cela est possible) des services, applications et ports qui ne sont pas utilisés ;

17.2.8 désactivation ou suppression des comptes invités ;

17.2.9 installation des correctifs de sécurité les plus récents sur le(s) Réseau(x) et Système(s) du Fournisseur dès que cela est possible après les essais. Toute exception doit être communiquée à BT quand ces exceptions auront été soumises à une évaluation des risques. BT se réserve le droit d'obliger le Fournisseur à installer des correctifs à l'issue de l'évaluation des risques ;

17.2.10 éviter les relations de confiance entre les serveurs ;

17.2.11 utilisation du principe de sécurité du « **privilège minimum** » pour exécuter une fonction ;

17.2.12 garantir que des mesures appropriées sont mises en place pour traiter les attaques par déni de service ;

17.2.13 garantir que des mesures appropriées sont mises en place pour assurer la détection et/ou la protection contre les intrusions ;

17.2.14 surveiller tous les fournisseurs et autres sources d'information concernées pour des alertes de vulnérabilité ;

17.2.15 le cas échéant, effectuer des vérifications d'intégrité pour détecter des ajouts, des modifications ou des suppressions de fichiers systèmes ou données essentielles ; et

17.2.16 modifier tous les mots de passe fournis par défaut ou par les fournisseurs avant de mettre en service les composants du réseau.

18 SECURITE DU NUAGE

Le Fournisseur doit satisfaire aux clauses de cette section s'il fournit à BT des services sur le nuage.

18.1 Le Fournisseur doit satisfaire :

à la dernière version de la matrice CCM (Cloud Controls Matrix) de Cloud Security Alliance ; aux exigences de sécurité d'hébergement externe de BT disponible à l'adresse : https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm ; Les accords de niveau de service de réseau et d'infrastructure (interne ou sous-traités) doivent documenter clairement les contrôles de sécurité, la capacité et les niveaux de service, ainsi que les exigences commerciales ou du client.

18.2 Le Fournisseur doit mettre en place les mesures de sécurité convenues sur tous les composants fournis, de sorte à ce que ces mesures préservent la confidentialité, la disponibilité, la qualité et l'intégrité des Fournitures en limitant la possibilité pour des individus non-autorisés (par ex. d'autres clients du nuage) d'accéder aux Informations de BT et aux Fournitures de BT.

19 CENTRE DE CONTACT

Le Fournisseur doit satisfaire aux clauses de cette section lorsqu'il fournit un centre de contact pour BT.

19.1 Le Fournisseur doit, à l'égard des Fournitures, garantir que les environnements dans lesquels les Informations de BT sont stockées, traitées ou visualisées sont conformes à la dernière version de la Norme destinée aux tiers en matière de Centre de contact, disponible à l'adresse :

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

PARTIE 5 : DÉFINITIONS

Dans les présentes Exigences de sécurité, les définitions suivantes s'appliqueront ; par ailleurs, ces Exigences de sécurité seront régies par les conditions du Contrat et tous les termes et expressions utilisés dans ces Exigences de sécurité auront la même signification que celle qui leur est donnée dans le Contrat.

« **Accès** » – traitement, manipulation ou stockage des Informations de BT par une ou plusieurs des méthodes suivantes :

- Par interconnexion avec les Systèmes de BT
- Fournies sous format papier ou non électronique
- Informations de BT sur les Systèmes du Fournisseur
- par support portable

et/ou accès aux locaux }de BT pour fournir les Fournitures, à l'exception de la livraison du matériel et pour assister aux réunions.

« **Autorisé** » - BT a autorisé l'Accès, soit dans le cadre du processus d'Interconnexion des Systèmes de BT, soit une autorisation écrite a été donnée par le Contact de sécurité de BT. Le terme « **autorisation** » doit être interprété en conséquence. Le niveau d'accès fourni sera pertinent et limité à celui qui est strictement nécessaire pour fournir les Fournitures.

« **Systèmes administratifs de BT** » – Cette expression désigne la plateforme de facturation de BT (actuellement iSupplier), ou les autres systèmes convenus avec BT et d'ordre purement administratifs ;

« **Client de BT** » – Pour les besoins de ces Exigences de sécurité, cette expression inclut toute personne physique ou morale à qui BT fournit des biens ou des services.

« **Informations de BT** » – Toutes les informations relatives à BT ou aux Clients de BT transmises au Fournisseur et toutes les Informations que le Fournisseur traite ou manipule pour le compte de BT ou des Clients de BT en vertu du Contrat.

« **Réseaux de BT** » - Le réseau contrôlé ou administré par BT.

« **Actifs physiques de BT** » - Tous les actifs physiques (y compris notamment les routeurs, interrupteurs, serveurs, clefs des boîtiers, jetons pour ordinateurs portables, cartes d'accès, plans ou documentation) détenue par le Fournisseur et appartenant à BT.

« **Sécurité de BT** » - L'organisation de sécurité fondée au sein de BT.

« **Contact de sécurité de BT** » – Le spécialiste en garantie des informations au sein de l'unité de Sécurité de BT ou de l'unité commerciale, dont les coordonnées ont été communiquées au Fournisseur ou le service central de Sécurité (0800

321999 [+44 1908 641100]) qui sera l'interlocuteur unique pour les questions liées à ces Exigences de sécurité et tout incident de sécurité majeur.

« **Systèmes de BT** » – Les services et composants, produits, réseaux, serveurs, processus, systèmes sur papier ou systèmes informatiques du service détenus et/ou exploités (totalement ou en partie) par BT ou tout autre système susceptible d'être hébergé dans les locaux de BT, y compris iSupplier (tel que ce terme est défini dans la Condition intitulée « **Paiement et facturation** »).

« **Registres en bloc** » – Ce terme désigne plus de 1 000 registres individuels d'Informations de BT classés comme Confidentiels ou 100 registres individuels d'Informations de BT classés comme Strictement confidentiels.

« **CCTV** » - télévision en circuit fermé.

« **Personnel sous contrat** », « **Personnel sous contrat concerné** » - Tel que défini dans le contrat.

« **Cyber Essentials Plus** » – Désigne le plan soutenu par le gouvernement britannique destiné à aider les organisations à se protéger contre les cyber-attaques communes et actuellement disponible sur https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

« **Bonnes pratiques du secteur en matière de sécurité** » – Signifie à l'égard de tout engagement et dans toutes circonstances, la mise en place de pratiques, politiques, normes et outils de sécurité pouvant raisonnablement et normalement être attendu d'une personne compétente et expérimentée engagée dans le même type d'activité dans les mêmes circonstances ou des circonstances similaires.

« **Informations** » – Informations, tangible ou autre, y compris notamment, des spécifications, des rapports, des données, des notes, des documents, des plans, des logiciels, des résultats informatiques, des dessins, des schémas de circuits, des modèles, des schémas, des échantillons, des inventions (pouvant ou non être brevetées) et le savoir-faire, ainsi que les supports (le cas échéant) sur lesquels ces informations sont transmises.

« **Interne** », « **Public** », « **Confidentiel** » et « **Strictement confidentiel** » – Ces termes ont les définitions qui leur sont données dans le document « 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement).

« **ISO 27001** » – Dernière version de la norme internationale pour les systèmes internationaux de gestion de la sécurité définie par l'Organisation internationale pour la standardisation et la commission électrotechnique internationale.

« **Actifs du réseau** »- Dispositif ou autre composant du Réseau de BT exécutant des activités liées au réseau.

« **Sécurité du réseau** » - La sécurité des voies et nœuds de communication qui connectent ensemble logiquement des technologies pour l'utilisateur final et des systèmes de gestion associés.

« **Traiter** », « **Traité** » ou «**Traitement** », « **Annexe relative au traitement** » et « **Données personnelles** » - auront le sens qui leur a été donné dans la Condition intitulée « **Protection des Données personnelles** ».

« **Incident de sécurité majeur** » - Violation de sécurité constatée ou présumée dans les systèmes ou services, et des événements de sécurité qui ont un impact sur les Fournitures ou l'exécution du Contrat (y compris les pertes, dommages, vols ou détournements réels ou présumés des Informations de BT ou Systèmes de BT), y compris notamment :

- une perte de service, d'équipements ou d'installations ;
- corruption, dommages ou détournement des Actifs physiques de BT ;
- dysfonctionnements ou surcharges du système ;
- erreurs humaines ;
- non-conformités vis-à-vis des exigences de sécurité décrites dans le présent document ;
- violations de mesures de sécurité physiques ;
- modifications non contrôlées du système ;
- dysfonctionnements du logiciel ou du matériel ;
- violations des accès ; et
- pertes de données avérées ou présumées liées aux systèmes associés à BT et à la(aux) connexion(s) entre BT et le Fournisseur.

« **Accès à distance** » - Accès à distance depuis une maison ou un autre site via un réseau public (par ex., Internet) ou accès à distance du réseau du Fournisseur à un Système de BT.

« **Exigences de sécurité** » - Les présentes exigences de sécurité de BT, telles qu'elles pourront être dûment mises à jour de temps en temps.

« **Fournitures** » – Ce terme désigne chacun et tous les « **Services** », « **Fournitures** », « **Biens** » et « **Tâches** » définis dans le Contrat et toute exécution du Contrat.

« **Systèmes du Fournisseur** » – Tout ordinateur, toute application ou tout système de réseau appartenant au Fournisseur utilisé pour accéder, stocker ou traiter les Informations de BT ou impliqué dans la mise à disposition des Fournitures.

« **Contact de sécurité du Fournisseur** » – La personne dont les coordonnées doivent être transmises par le Fournisseur à BT, de temps en temps, et qui sera l'interlocuteur unique pour les questions liées à ces Exigences de sécurité et tout Incident de sécurité majeur.

« **Transmission** » ou « **Transmis** » - Déplacement des Informations de BT en possession du Personnel sous contrat (y compris notamment les Données personnelles) d'un site ou d'une personne à un/une autre, par tout moyen physique, vocal ou électronique ; l'octroi d'Accès aux Informations de BT en possession du Personnel sous contrat (y compris notamment les Données personnelles) d'un site ou d'une personne à un/une autre, par tout moyen physique, vocal ou électronique.

« 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement) - Désigne les exigences relatives au traitement des informations par le Fournisseur, tel que cela est décrit dans https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm et selon les mises à jour régulières.