Sommaire

1. Introduction et portée 2
2. Sécurité des informations pour un accès limité 2
3. Sécurité des informations générales 3
4. Sécurité du Personnel du contrat 5
5. Audit et évaluation de la sécurité 6
6. Investigation 7
7. Exigences génériques et politique de sécurité 7
8. Sécurité physique - locaux de BT 8
9. Sécurité physique - locaux du fournisseur 8
10. Dispositions pour l'environnement d'hébergement 11
11. Développement des fournitures 12
12. Accès à l'information 13
13. Accès aux systèmes de BT 15
14. Accès aux informations de BT sur les systèmes du fournisseur 16
15. Hébergement d'informations de BT par le fournisseur 17
16. Sécurité du réseau 18
17. Sécurité du réseau du fournisseur 20
18. Sécurité du cloud 21
Glossaire 21

1. Introduction et portée

1.1 Le présent document représente les exigences de base de BT en matière de sécurité, par rapport à la portée des travaux entrepris par un fournisseur. Ces exigences sont de trois niveaux.

Le 1er niveau d'exigences de la section 2 concerne les fournisseurs qui réaliseront des travaux relatifs à un volume limité d'Informations de BT et qui peuvent avoir un accès limité à des systèmes administratifs de BT et des réseaux de BT. Les fournisseurs de cette catégorie ne seront pas tenus de respecter de quelconques autres exigences du présent document.

Les sections 3 à 6 du 2e niveau sont obligatoires pour tous les types de travaux.

Pour le 3e niveau, en fonction du champ d'application des travaux, une ou plusieurs exigences des sections 7 à 18 peuvent être applicables. Votre représentant de l'Approvisionnement de BT pourra vous conseiller.

Certaines des exigences peuvent se rapporter à une Annexe de la liste suivante, fournissant des informations complémentaires : :

Annexe 1 - Classification des informations
Annexe 2 - Formation obligatoire
Annexe 3 - Transmission des demandes/problèmes à un Contact Sécurité BT
Annexe 4 - Accès aux sites et locaux de BT par des organisations qui ne font pas partie de BT - Royaume-Uni seulement
Annexe 5 - Exigences de sécurité pour l'hébergement externe

1.2 Ces exigences de sécurité sont complémentaires et s'appliquent sans préjudice des quelconques autres obligations du fournisseur prévues par le contrat (y compris, sans exclusivité toutefois, ses obligations conformément aux Conditions intitulées « Confidentialité », « Protection des données personnelles » et « Vérifications préalables à l'embauche (PEC) »).

2. Sécurité des informations pour un accès limité

Le respect de la section 2 est la seule exigence à respecter si le fournisseur réalise des travaux relatifs à un volume limité d'Informations de BT et peut avoir un accès limité à des systèmes administratifs de BT, par ex. iSupplier et les réseaux de BT (ces types de travaux sont par exemple, sans exclusivité toutefois, les fournitures de bureau, la gestion des installations, les études de site, les systèmes de coupon et les produits à prix réduit pour les employés, les fournisseurs de contenu TV de BT et les Titulaires de droits).

Sans préjudice des quelconques obligations de confidentialité qu'il doit respecter, si le fournisseur ou le Personnel du contrat a accès aux informations de BT ou à celles des clients de BT (y compris des données personnelles), le fournisseur prend les engagements suivants :
(a) S'assurer que ces informations (y compris les données personnelles) ne sont pas communiquées au Personnel du contrat qui n'est pas directement employé pour réaliser des travaux pour BT et qu'il ne peut pas y accéder.
(b) Assurer (et veiller à ce que tout le Personnel du contrat concerné assure) la sécurité et la confidentialité de ces informations (y compris les données personnelles) (y compris, sans exclusivité toutefois, en appliquant les systèmes et les procédures nécessaires pour protéger

la sécurité de toutes les informations appartenant à BT ou contrôlées par BT, dans la mesure où le fournisseur en a la possession ou le contrôle, conformément aux bonnes pratiques du secteur, et en mettant tous ces systèmes et processus en œuvre de manière rigoureuse).

Les sections 3 à 6 comprises sont applicables à tous les engagements de fournisseurs avec BT (à l'exception des fournisseurs fournissant simplement des Fournitures à accès limité).

3. Sécurité des informations générales

3.1 Le fournisseur s'engage à communiquer rapidement à BT les coordonnées du Contact Sécurité du fournisseur et à l'aviser si celles-ci changent.

3.2 Au début du contrat, le fournisseur s'engage à notifier le Contact Sécurité BT par écrit, au moyen de l'Annexe 3, des implantations géographiques où sont réalisés les principaux services, où se trouve le Personnel chargé des contrats concernés ou les lieux où sont traitées ou stockées les informations de BT. Durant le contrat, le fournisseur devra également informer le Contact Sécurité BT de toute proposition de modification d'une implantation géographique, via l'Annexe 3, afin que BT puisse réévaluer les quelconques risques pour les informations de BT ou celles des clients de BT.

3.3 Le fournisseur s'engage à s'assurer que tous les contrats avec les sous-traitants concernés comprennent des clauses écrites, exigeant que le sous-traitant se conforme aux exigences de sécurité des fournisseurs de BT, dans la mesure où elles sont applicables. Ces clauses doivent être en place entre le fournisseur et son sous-traitant avant que le sous-traitant ou ses employés puissent accéder aux systèmes et aux informations de BT.

3.4 Le fournisseur s'engage à ne pas utiliser les informations de BT à d'autres fins que celles pour lesquelles elles ont été fournies au fournisseur par BT, et dans ce cas uniquement dans la mesure nécessaire pour permettre au fournisseur d'exécuter le contrat. Le fournisseur s'engage à traiter ou à utiliser les informations de BT de manière à se conformer aux exigences de l'Annexe 1 des présentes Exigences de sécurité et conformément aux lois en vigueur.

3.5 Le fournisseur s'engage à informer le Contact Sécurité BT au moyen de l'Annexe 3 s'il fait l'objet d'une fusion, d'une acquisition ou d'un changement de propriétaire, afin de nous permettre de réévaluer les risques quelconques pour BT, ses informations ou celles des clients de BT.

3.6 Au minimum, le fournisseur s'engage à réviser une fois par an ou au moment où des modifications sont apportées aux fournitures ou à leur mode d'approvisionnement, ces Exigences de sécurité, afin de s'assurer qu'elles sont conformes à toutes les Exigences de sécurité en vigueur.

3.7 Le fournisseur s'engage à gérer en toute sécurité tous les Biens physiques de BT et/ou les Articles de BT que lui aura affectés BT.

- Les Biens physiques de BT et les Articles de BT devront être stockés en toute sécurité quand ils ne seront pas utilisés. Il s'agit par exemple, sans exclusivité toutefois, des

jetons d'accès à distance, des ordinateurs portables de BT, des équipements de réseau, des serveurs et de la documentation.

- Les Biens physiques de BT ne devront pas être retirés du lieu de travail et sortis du site sans autorisation préalable.

3.8 Au titre des fournitures, le fournisseur s'engage à avoir des procédures formelles de gestion des incidents de sécurité, avec des responsabilités définies et toutes les informations relatives à un quelconque incident de sécurité seront traitées comme étant « confidentielles ». Le fournisseur s'engage à informer le Contact Sécurité BT au moyen de l'Annexe 3, dans un délai raisonnable après avoir pris connaissance d'un quelconque incident :

i) concernant une perte matérielle, une corruption, des dommages ou un usage abusif des informations de BT, des biens matériels de BT, d'articles de BT, l'accès illicite ou non autorisé aux systèmes et informations de BT, le non-respect de quelconques obligations du fournisseur conformément à ces exigences de sécurité ; ou
ii) concernant une incapacité à fournir les fournitures conformément au contrat.
iii) toute action qui ne respecte pas les exigences du présent document relatif à la sécurité.

Si BT en fait la demande raisonnable, le fournisseur s'engage à lui fournir rapidement un rapport écrit contenant un plan de redressement, associé à un calendrier et des mesures à prendre pour éviter que l'incident se reproduise.

3.9 Le fournisseur s'engage à traiter dans les délais les plus brefs les risques identifiés pour la confidentialité, l'intégrité ou la disponibilité des informations de BT sur les processus ou les systèmes du fournisseur.

3.10 BT pourra réaliser des évaluations des risques sur une quelconque partie pertinente de la prestation (pouvant inclure des sous-traitants pertinents à la prestation), afin d'identifier les risques supplémentaires pour BT, liés à l'approvisionnement des fournitures, le cas échéant. BT pourra alors stipuler des contre-mesures supplémentaires pour gérer de quelconques risques. Tous les coûts associés à la mise en œuvre de contre-mesures devront faire l'objet d'un accord entre les deux parties.

3.11 Le fournisseur s'engage à mettre en place des politiques et processus de sécurité et à tenir des documents (dont les copies doivent être disponibles en langue anglaise), faisant la preuve du respect des présentes Exigences de sécurité et permettant à BT d'accéder aux éléments probants nécessaires, conformément à la Section 7 ci-dessous.

3.12 Le fournisseur s'engage à ce que des procédures et des contrôles soient en place pour protéger le Transfert des informations de BT par messages électroniques, communication vocale, par fax et vidéo. (Par ex. lors des conférences téléphoniques, il faut s'assurer que toutes les personnes y participant sont autorisées à discuter des informations de BT). Pour un complément d'information sur le traitement des informations de BT, voir l'Annexe 1.

3.13 Le fournisseur s'engage à avoir des procédures en place pour gérer les menaces pour la sécurité concernant ou visant BT ou contre un tiers qui travaille pour le compte de BT, dans le but de protéger correctement les informations de BT.

3.14 Le fournisseur s'engage à s'assurer que les activités réalisées à distance ou à domicile et concernant les informations et les systèmes de BT font l'objet des contrôles de sécurité appropriés au sein de l'organisation du fournisseur, y compris, mais sans exclusivité, des procédures fortes de vérification de l'identité des utilisateurs qui ont un accès à distance.

3.15 À la résiliation ou à l'expiration du contrat, le fournisseur s'engage à détruire, et veillera à ce que ses quelconques employés du Personnel du contrat et ses sous-traitants détruisent, en toute sécurité les quelconques informations de BT dont le fournisseur ou ses sous-traitants ont la possession ou le contrôle, conformément à l'Annexe 1 des présentes Exigences de sécurité, sauf indication contraire par BT ou selon de quelconques obligations légales ou réglementaires. Les informations archivées doivent être entièrement écartées pour ne pas être utilisées dans le cadre des activités courantes.

3.16 Le fournisseur s'engage à conserver les informations de BT aussi longtemps qu'il le faudra pour exécuter la prestation, mais pas plus longtemps que deux ans maximum, sauf si une durée de conservation différente a été prescrite par BT ou est nécessaire pour satisfaire des exigences légales ou réglementaires.

3.17 Le fournisseur s'engage à garantir la disponibilité, la qualité, l'intégrité et la capacité adéquate pour réaliser les performances requises du système ou l'approvisionnement des fournitures, sans interruption, en s'assurant que :

- Un plan de secours est en place
- Les données critiques des systèmes sont protégées le cas échéant
- Un scénario de reprise est mis en œuvre s'il s'agit d'une exigence convenue
- Le système ou le service est récupérable suite à une panne grave ou une catastrophe
- Le plan est mis en pratique au moins une fois par an
- Des copies de sauvegarde des informations et des logiciels seront réalisées, le cas échéant, et mises à l'épreuve régulièrement, conformément à une politique de sauvegarde convenue, afin de veiller à la restauration des données sans modification.

4. Sécurité du Personnel du contrat

4.1 L'accès ne sera pas accordé aux membres du Personnel du contrat tant qu'ils n'auront pas suivi la formation sur la Sécurité de BT, détaillée à l'Annexe 2 des présentes Exigences de sécurité. La formation sur la Sécurité des informations de BT peut être remplacée par une formation équivalente sur la sécurité des informations, propre au fournisseur, sous réserve de sa validation par le service de Sécurité BT. Ensuite, la formation obligatoire doit être renouvelée conformément à l'Annexe 2. Le fournisseur s'engage à tenir des registres de formation, qui seront mis à la disposition de BT pour réaliser un audit.

4.2 Le fournisseur s'engage à s'assurer que tous les membres du Personnel du contrat signeront un Accord de confidentialité du fournisseur avant de commencer des travaux dans les locaux de BT ou sur les systèmes de BT, ou d'avoir accès aux informations de BT. Ces accords de confidentialité doivent être conservés par le fournisseur et être mis à la disposition de BT pour évaluation dans le cadre d'un audit.

4.3 Le fournisseur s'engage à gérer les manquements aux politiques et procédures de sécurité par le biais de processus formels, y compris des mesures disciplinaires le cas échéant.

4.4 Le fournisseur s'engage à maintenir une assistance téléphonique confidentielle, mise à la disposition de tout son personnel, dans la mesure autorisée par la loi, que le Personnel du contrat pourra utiliser s'il lui est demandé d'agir d'une manière contraire aux présentes Exigences relatives à la sécurité. Il faudra adresser au Contact Sécurité BT les rapports pertinents au moyen de l'Annexe 3.

4.5 Une fois que les membres du Personnel du contrat ne seront plus affectés aux fournitures, le fournisseur s'engage à révoquer l'accès aux informations de BT et à s'assurer que les quelconques biens, articles ou informations de BT que les membres du Personnel du contrat ont en leur possession sont retournés à l'équipe opérationnelle BT concernée ou détruits conformément à l'Annexe 1 des présentes Exigences de sécurité. Dans la mesure du possible, le fournisseur s'engage à mettre en œuvre une procédure de sortie contrôlée, comportant une demande écrite adressée au Responsable opérationnel BT pour la suppression des accès à BT et de l'identité. Les membres du Personnel du contrat doivent être informés que l'accord de confidentialité qu'ils ont signé continue à être en vigueur et qu'il leur est interdit de divulguer les informations BT acquises dans le cadre des travaux sur les Fournitures.

4.6 Dans le cadre de l'octroi de l'accès, le fournisseur s'engage à tenir et fournir des registres de tous les membres du Personnel du contrat qui doivent accéder ou qui fournissent les Fournitures BT, y compris leur nom, leur lieu de travail, leur adresse électronique professionnelle, leur numéro de téléphone professionnel direct et leur poste (le cas échéant) et/ou leur numéro de téléphone portable, la date où leur identifiant d'utilisateur (UIN) (le cas échéant) a été demandé, la date à laquelle le projet BT leur a été affecté, la date à laquelle ils ont terminé la formation obligatoire, la date à laquelle ils ont quitté le projet BT et la déclaration du contrôle préalable à l'embauche. Le Contact sécurité du fournisseur s'engage à s'assurer qu'en toutes circonstances, seuls les membres pertinents du Personnel du contrat sont autorisés.

5. Audit et évaluation de la sécurité

5.1 Le fournisseur s'engage, au titre des fournitures et sous réserve qu'il assure la confidentialité des informations relatives à ses autres clients, à permettre (et à s'assurer que tous les membres du Personnel du contrat permettent) à BT ou à ses représentants autorisés, sur demande raisonnable, l'accès aux locaux, systèmes et dossiers du fournisseur et d'un quelconque sous-traitant concerné, qui contiennent des informations de BT et des clients de BT (y compris des données personnelles), qui sont raisonnablement nécessaires pour évaluer le respect des présentes Exigences de sécurité par le fournisseur.

Il pourra s'agir des évaluations de tous les éléments des contrôles physiques et logiques et de la validation des systèmes du fournisseur contenant des informations de BT. Le fournisseur contribuera à cette évaluation en autorisant BT à recueillir, conserver et analyser les informations relatives à l'approvisionnement des fournitures, le cas échéant, afin d'identifier les risques potentiels pour la sécurité et fournira à BT les rapports et participera aux réunions éventuellement demandés par BT, de manière raisonnable.

Si BT en fait la demande, le fournisseur s'engage à participer à un bilan de santé en ligne, afin d'établir le respect fondamental des clauses de sécurité dans les présentes Exigences de sécurité.

6. Investigation

6.1 Si BT a des raisons de soupçonner un manquement de la part du fournisseur ou d'un quelconque sous-traitant aux dispositions des présentes Exigences de sécurité, qui aurait un impact sur les systèmes et/ou les informations de BT, BT en informera le Contact sécurité du fournisseur. Le fournisseur s'engage à coopérer entièrement avec BT dans le cadre d'une quelconque investigation menée à ce titre par BT et/ou un service chargé de faire respecter la loi, pouvant nécessiter l'accès aux informations de BT dans les locaux du fournisseur, après avoir donné au fournisseur un préavis raisonnable.

Pendant l'investigation, le fournisseur s'engage à coopérer avec BT, en lui apportant une assistance raisonnable et les ressources nécessaires pour mener l'enquête par rapport au manquement. BT pourra demander au fournisseur de mettre en quarantaine pour évaluation de quelconques biens matériels et immatériels appartenant au fournisseur, afin d'aider à l'enquête et le fournisseur s'engage à ne pas refuser ou retarder sans raison la réponse à la demande.

La description de chacune des clauses des sections 7 à 18 précise le type de fourniture concerné par celles-ci.

7. Exigences génériques et politique de sécurité

Le fournisseur est tenu de respecter les clauses de la section 7 s'il a accès à des « Informations sensibles » (selon la définition du terme) ou fournit des fonctions de développement, installation, maintenance, soutien du réseau ou des services informatiques professionnels.

7.1 Le fournisseur s'engage à avoir la certification ISO27001 ou à respecter les exigences de sécurité de la certification ISO27001 ou des politiques de sécurité conformes à la norme ISO27001 et/ou à travailler à l'obtention de la certification ISO27001 dans des délais convenus avec BT.

7.2 Si elles existent, BT pourra occasionnellement mettre à jour les politiques relatives à la sécurité, les directives, les exigences de sécurité et autres exigences. BT s'engage à intégrer les mises à jour pertinentes à une version mise à jour des présentes Exigences de sécurité par une demande de modification du contrat, dont BT informera le fournisseur par

écrit. Tous les coûts associés à la mise en œuvre de nouvelles exigences de sécurité devront faire l'objet d'un accord entre les deux parties.

7.3 Le fournisseur s'engage à mettre à la disposition de BT des copies des certifications relatives à la sécurité et une déclaration d'applicabilité concernant les services fournis, afin de faire la preuve du respect du présent plan.

8. Sécurité physique - locaux de BT

Le fournisseur est tenu de respecter les clauses de la section 8 s'il fournit des fournitures dans les locaux de BT.

8.1 Tous les membres du Personnel du contrat travaillant dans les locaux de BT devront être en possession d'une carte d'identification fournie par un fournisseur autorisé ou par BT. Cette carte devra être utilisée comme moyen de vérification de leur identité dans les locaux de BT en toutes circonstances et devra contenir une photographie, qui devra être claire et fidèle à l'apparence du membre du Personnel du contrat. Il sera également possible de remettre aux membres du Personnel du contrat une carte d'accès électronique et/ou un badge de visiteur d'une durée limitée, qu'ils devront utiliser conformément aux consignes locales de délivrance.

8.2 Une connexion directe (branchement sur le port LAN ou connexion sans fil) sur les domaines de BT n'est autorisée qu'avec des serveurs dont la construction est approuvée par BT, des PC Webtop de BT et des Terminaux sécurisés. Il est interdit au fournisseur de connecter des équipements qui ne sont pas approuvés par BT à un domaine de BT sans l'autorisation préalable écrite du Contact Sécurité BT (qu'il contactera en remplissant l'Annexe 3). Le cas échéant, le fournisseur s'engage à s'assurer que son Personnel de Contrat respecte cette clause. Le Contact Sécurité BT fournira une autorisation écrite lors du lancement de la procédure de concession par rapport à la politique de sécurité au sein de BT par le contact BT du fournisseur.

8.3 Il est interdit de retirer des locaux de BT de quelconques informations de BT et de retirer ou d'installer dans les locaux de BT des équipements ou des logiciels sans l'autorisation préalable de BT.

8.4 Il est impératif de respecter les directives de protection physique et celles relatives au travail dans les locaux de BT, par ex. obligation d'être escorté pour se rendre dans des zones sécurisées. Tous les ordres ou consignes que BT donnera à un représentant du fournisseur seront considérés comme ayant été donnés au fournisseur.

8.5 Si le fournisseur est autorisé à fournir à son Personnel du contrat un accès non hébergé à des zones du patrimoine de BT, le signataire et le Personnel du contrat concerné, non autorisés par BT, devront respecter les quelconques directives et consignes fournies par BT. En outre, le signataire et le Personnel du contrat concerné, non autorisés par BT, devront subir au minimum les vérifications préalables à l'embauche de niveau L2.

9. Sécurité physique - locaux du fournisseur

Le fournisseur est tenu de respecter les clauses de la section 9, ainsi que tous les membres du Personnel du contrat, ses sous-traitants, ses employés et ses agents, s'il fournit des fournitures à partir de locaux qui n'appartiennent pas à BT.

9.1 Tout accès aux locaux qui n'appartiennent pas à BT (sites, bâtiments ou zones internes) où sont fournies les fournitures ou bien où sont stockées ou traitées les informations de BT devra se faire au moyen d'une carte d'identification fournie par un fournisseur autorisé. Cette carte devra être utilisée comme moyen de vérification de l'identité dans les locaux concernés en toutes circonstances et par conséquent, la photographie qu'elle contiendra devra être claire et fidèle à l'apparence de l'employé concerné. Il sera également possible de remettre à des employés une carte d'accès électronique autorisée, dans le seul but de leur permettre d'accéder aux locaux concernés ou bien un accès par code de sécurité, associé à des processus pour contrôler l'autorisation, la dissémination et un changement régulier ou ponctuel du code.

9.2 Le fournisseur s'engage à s'assurer que l'accès aux sites, bâtiments ou zones internes où sont réalisées les fournitures ou bien où sont stockées ou traitées les informations de BT est autorisé et respecte les processus et procédures relatifs à la sécurité, y compris les sous-traitants autorisés à accéder à ces zones (par ex. contrôle environnemental, entretien, sociétés responsables des alarmes).

9.3 Si le responsable d'une entreprise ou d'un projet BT en fait la demande, le fournisseur s'engage à s'assurer que les membres concernés du Personnel du contrat sont séparés de manière sécurisée des autres employés du fournisseur.

9.4 Les zones sécurisées des locaux du fournisseur (par ex. les salles de communication par réseau) devront être séparées et protégées par des contrôles appropriés de l'accès, afin de veiller à ce que seuls les membres autorisés du Personnel du contrat puissent accéder à ces zones sécurisées. L'accès à ces zones par un quelconque membre du Personnel du contrat devra faire l'objet d'un audit régulier et le renouvellement de l'autorisation des droits d'accès à ces zones devra être effectué au moins une fois par an.

9.5 Le fournisseur s'engage à utiliser des systèmes de sécurité par vidéosurveillance et les supports d'enregistrement qui leur sont associés, en réponse à des incidents de sécurité, en tant qu'outil de surveillance de la sécurité, comme outil de dissuasion ou pour permettre d'appréhender des personnes en flagrant délit. Si les images de vidéosurveillance sont enregistrées (que ce soit sur bande ou sur un support numérique), elles devront être conservées pendant au moins 20 jours. Il sera néanmoins possible de prolonger ce délai dans les situations suivantes :
i) Si les preuves fournies par la vidéosurveillance doivent être conservées dans le cadre d'une enquête concernant un incident ou un délit.
ii) Si la loi l'exige.

Toutes les bandes de vidéosurveillance permettant l'enregistrement des images devront être stockées dans une armoire verrouillée et la clé devra être conservée dans un endroit sécurisé et contrôlé. L'accès à l'armoire devra être restreinte au personnel autorisé.
Tous les enregistreurs de vidéo numérique ou de vidéo de la vidéosurveillance devront être positionnés de manière discrète afin d'éviter un accès non autorisé et la possibilité que les écrans de vidéosurveillance associés puissent être vus « accidentellement ».

9.6 La zone qui entoure les installations du fournisseur utilisées pour les produits et/ou les services, selon le cas, devra être inspectée régulièrement par le fournisseur au titre des risques et des dangers qu'elle présente.

9.7 Les câbles d'alimentation et de télécommunication transportant des données ou soutenant les services d'information ou les services de radio/satellite utilisés dans l'approvisionnement des fournitures devront être évalués par le fournisseur en ce qui concerne le niveau de protection, afin d'éviter toute interruption des opérations de l'entreprise. Il faudra mettre en œuvre des mesures de protection de la sécurité physique compatibles à la criticité commerciale des opérations qu'elles couvrent, selon les procédures suivantes :
i) Les regards, le blindage des câbles, les boîtiers dans la chaussée ou sur les trottoirs contenant des câbles critiques pour l'entreprise devront être protégés.
ii) L'accès aux chambres des câbles ou aux armoires de câbles ascendants dans les bâtiments opérationnels devra être restreint au moyen de lecteurs électroniques pour le contrôle de l'accès ou d'une gestion efficace des clés.
iii) Les liens de communication par ordinateur et les équipements de communication au sein d'installations informatiques devront être dotés d'une protection physique et environnementale.
iv) Les liens de communications par radio et par satellite et les équipements de communication devront être correctement protégés.

9.8 Des services de sécurité par surveillance humaine sont jugés nécessaires pour compléter les mesures de sécurité électronique et physique dans les implantations du fournisseur dans les circonstances suivantes :

- L'implantation présente une importance opérationnelle
- Les informations de BT qui y sont traitées peuvent avoir un impact sur la marque et sa réputation
- Le volume d'informations de BT qui y est traité est élevé (par ex. processus commercial externalisé)
- Des exigences contractuelles du client
- Des risques ou dangers spécifiques au site
- Le fournisseur est en possession d'informations de BT qui sont extrêmement sensibles.

9.9 Afin de protéger les équipements de BT (tels que les serveurs ou les commutateurs de BT) dans les locaux du fournisseur contre les menaces ou les dangers environnementaux et contre la possibilité d'un accès non autorisé, les équipements de BT devront être positionnés dans une zone protégée et séparée des équipements utilisés pour de quelconques systèmes appartenant à des organisations autres que BT. Le degré de séparation devra garantir qu'il est impossible de compromettre la sécurité des équipements de BT, que ce soit de manière délibérée ou accidentelle, en raison de l'accès accordé aux organisations autres que BT. Cette séparation pourra prendre par exemple la forme d'une cloison sécurisée, d'armoires pouvant être verrouillées ou d'une cage métallique.

9.10 Il faudra employer des mesures de prévention et de détection pour empêcher la panne des installations causée par l'interruption de services essentiels ou d'autres influences environnementales.

- incendie ;
- gaz ;
- inondation ;
- panne d'électricité ;

Des alarmes devront être installées et connectées à un poste bénéficiant d'une surveillance humaine afin de détecter les problèmes suivants :

- incendie ;

- gaz ;
- panne d'électricité ;
- panne de l'alimentation sans interruption (ASI) ;
- panne de la climatisation/du contrôle de l'humidité et de la température.

9.11 Il faudra utiliser des périmètres de sécurité (des barrières telles que des murs, clôtures, portails d'entrée contrôlés par carte ou bureaux de réception avec des employés) afin de protéger les zones contenant des informations de BT et des installations de traitement des informations.

9.12 Les points d'accès tels que les baies de déchargement et de chargement, ainsi que d'autres points où des personnes sans autorisation peuvent pénétrer dans les locaux devront être contrôlés et, dans la mesure du possible, isolés des installations de traitement des informations, afin d'éviter un accès non autorisé ou des attaques délibérées.

9.13 Veiller à ce que l'accès physique aux zones qui permettent d'accéder aux informations de BT se fasse uniquement par carte à puce ou de proximité (ou un système de sécurité équivalent) et que le fournisseur effectue régulièrement un audit interne, pour s'assurer du respect de ces dispositions.

9.14 Le fournisseur s'engage à interdire toute photographie et/ou saisie d'images relatives à des informations de BT ou des informations de clients de BT. Dans des circonstances exceptionnelles, en cas d'exigences commerciales pour la saisie de ces images, il faudra obtenir une dérogation temporaire écrite à cette clause de la part du Contact Sécurité BT, au moyen de l'Annexe 3.

9.15 Le fournisseur s'engage à maintenir une politique du bureau propre et de l'écran vide, afin de protéger les informations de BT.

10. Dispositions pour l'environnement d'hébergement

Le fournisseur est tenu de respecter les clauses de la section 10 s'il fournit un environnement d'hébergement pour les équipements de BT ou des clients de BT.

10.1 Le fournisseur s'engage, s'il fournit une zone d'accès sécurisée dans ses locaux pour l'hébergement des équipements de BT ou des clients de BT (« Site fournisseur ») à :
(a) s'assurer que tous les membres du Personnel du contrat qui accèdent au site fournisseur sont en possession d'une carte d'identification ou d'une carte électronique de contrôle des accès. Cette carte devra être utilisée comme moyen de vérification de leur identité sur le site fournisseur en toutes circonstances et par conséquent, la photographie qu'elle contiendra devra être claire et fidèle à l'apparence du membre du Personnel du contrat concerné.
(b) avoir mis en œuvre des procédures pour traiter les menaces sécuritaires à l'encontre des équipements de BT ou des clients de BT ou à l'encontre d'un tiers travaillant pour le compte de BT, afin de préserver les informations de BT ou des clients de BT sur le site fournisseur.
(c) utiliser des systèmes de sécurité par vidéosurveillance et les supports d'enregistrement qui leur sont associés au site fournisseur, en réponse à des incidents de sécurité, en tant qu'outil de surveillance de la sécurité, comme outil de dissuasion ou pour permettre d'appréhender des personnes en flagrant délit. Le fournisseur s'engage à ce que les 20 jours d'enregistrement de la vidéosurveillance soient efficaces comme outil dans le cadre d'une investigation.
(d) fournir à BT un plan au sol de l'espace attribué dans la zone sécurisée du site fournisseur.

(e) s'assurer que les armoires de BT et des clients de BT sur le site fournisseur sont tenues verrouillées et que seuls les membres autorisés du personnel de BT, les représentants approuvés par BT et les membres concernés du Personnel du contrat peuvent y accéder.
(f) mettre en œuvre une procédure de gestion sécurisée des clés au site fournisseur.
(g) inspecter régulièrement la zone avoisinante du site fournisseur pour y relever d'éventuels risques ou dangers.
(h) documenter et maintenir des procédures opérationnelles (dans la langue du pays d'où proviennent les travaux de BT), afin de se conformer aux exigences de sécurité détaillés dans l'alinéa 12, et permettre à BT, à sa demande, de consulter ces documents.

10.2 BT s'engage à fournir au fournisseur :
(a) un registre des biens physiques de BT et des clients de BT détenus au site fournisseur ;
(b) des détails des employés, sous-traitants et agents de BT devant avoir accès au site fournisseur (en permanence).

11. Développement des fournitures

Le fournisseur est tenu de respecter les clauses de la section 11 s'il traite du développement des fournitures destinées à BT et/ou aux clients de BT. (Il s'agit notamment des « composants disponibles dans le commerce », de la configuration des logiciels et des composants nécessaires à la fabrication des fournitures)

11.1 Le fournisseur s'engage à mettre en œuvre les mesures de sécurité approuvées, de sorte à préserver la confidentialité, la disponibilité et l'intégrité des fournitures par les moyens suivants :

(i) la tenue d'une documentation appropriée (dans la langue du pays d'où proviennent les travaux de BT) dans le cadre de la mise en œuvre de la sécurité ; le fournisseur s'engage aussi à veiller à ce que cette documentation et la sécurité associée soient conformes aux bonnes pratiques du secteur
(i) minimiser les opportunités permettant à des personnes non autorisées (par ex. des pirates) d'accéder aux systèmes de BT ou aux informations de BT, aux réseaux de BT ou aux services de BT
(iii) minimiser le risque de l'utilisation abusive des systèmes de BT et des informations de BT, des réseaux de BT ou des services de BT, pouvant potentiellement causer une perte de revenus ou de service.

11.2 Sur demande, le fournisseur s'engage à faire la preuve qu'un quelconque logiciel ou matériel fabriqué (à la fois propriétaire et disponible dans le commerce) et livré à BT correspond aux caractéristiques prévues avec BT. Le fournisseur s'engage à maintenir l'intégrité des conceptions, notamment les mises à jour, les systèmes d'exploitation et les applications, de l'usine au bureau.

11.3 S'assurer que le développement des systèmes destinés à être utilisés par BT ou la conception et la maintenance de matériels appartenant à BT sont renforcés conformément aux Exigences de sécurité informatique de BT, si l'équipe opérationnelle de BT les fournit ou conformes aux bonnes pratiques du secteur

11.4 S'assurer que les environnements de développement et de test ne contiennent pas de données réelles et sont séparés de l'environnement des données réelles. Les données de

test fournies par BT doivent être supprimées après un délai déterminé par le propriétaire des données de BT.

11.5 Le fournisseur garantit qu'il a mis en œuvre tous les efforts raisonnables pour s'assurer que les logiciels et/ou le matériel (et la documentation fournie sous format électronique) sont dépourvus des problèmes suivants (la liste n'est pas exhaustive) sous toutes leurs formes :

(i) « possession électronique » ou « bombe logique »

(i) « virus » et « vers informatiques » qui auraient pu être détectés au moyen de la dernière version (à la date de l'expédition) d'un logiciel de détection des virus disponible dans le commerce

(iii) « logiciels espions », « logiciels publicitaires » et autres programmes malveillants. (Ces expressions seront interprétées selon la définition couramment utilisée dans le secteur de l'informatique.) Le fournisseur garantit qu'à partir du moment où il a donné son acceptation, les logiciels et/ou le matériel fonctionneront conformément au Cahier des charges fonctionnel pendant la période de garantie. Le fournisseur s'engage à utiliser exclusivement des matériaux de bonne qualité, de bonnes techniques et les Exigences de sécurité dans l'exécution du contrat et à appliquer en toutes circonstances les Exigences de sécurité en matière de soins, compétences et diligence, qui sont requises pour de bonnes pratiques informatiques et des méthodologies de codage sécurisées.

11.6 Le fournisseur s'engage à collaborer avec BT pour veiller au respect des exigences de sécurité du (des) cadre(s) de sécurité approprié(s) aux frais du fournisseur. Occasionnellement, il faudra à ce titre que les fournitures soient testées par rapport aux exigences de sécurité.

11.7 Toute défaillance par rapport à la sécurité identifiée par BT ou le fournisseur dans les fournitures devra être redressée aux frais du fournisseur, dans les délais raisonnables requis par BT.

12. Accès à l'information

Clauses applicables si les exigences le prévoient.

12.1 Dans un délai de 14 jours à compter de la demande écrite de BT et au gré de BT, il faudra que :

(a) les parties s'engagent, en prenant à leur charge leurs frais respectifs, à exécuter et fournir à l'autre un accord d'accès à l'information sous la forme de l'Accord d'accès à l'information prévu à l'Annexe 3 ; ou

(b) le fournisseur s'engage, à ses frais, à conclure un contrat d'entiercement, essentiellement sous la forme du contrat prévu à l'annexe 21, pour toutes les informations et tous les documents relatifs aux fournitures (y compris, sans exclusivité toutefois, pour les logiciels, tous les codes sources, les données des liens, les listes de logiciels, l'ensemble des données techniques, les notes des programmeurs, toutes les informations et les documents relatifs aux logiciels, qui sont nécessaires pour la tenue, la modification et la correction des logiciels et la fourniture de tous les niveaux de prise en charge pour les logiciels) (« les informations entiercées ») et à confier à NCC Escrow International Limited (« le tiers séquestre ») une version mise à jour des informations entiercées. Le fournisseur s'engage à s'assurer que les informations entiercées permettront à BT et/ou à tous les tiers compétents agissant pour le compte de BT de :

(i) s'acquitter des quelconques obligations que le fournisseur doit encore assumer en vertu du contrat, y compris, mais sans exclusivité, les obligations qui auraient existé (y compris l'exigence de satisfaire de quelconques commandes que BT aurait placées conformément au contrat) si le contrat n'avait pas été résilié par BT (en dehors des conditions prévues à l'alinéa 4 de la clause intitulée « Résiliation ») avant l'expiration de sa durée naturelle (qui couvrira toutes les prolongations de la durée dans le cadre d'une option quelconque dont dispose BT pour prolonger la durée initiale) ;
(ii) comprendre facilement les informations entiercées, tenir (y compris les mises à jour), modifier, améliorer et corriger les informations entiercées et les fournitures.

12.2 Le fournisseur garantit que les informations entiercées confiées à BT ou au tiers séquestre, selon le cas, sont et seront tenues de manière à être suffisantes pour permettre à un programmeur ou à un analyste raisonnablement qualifié de tenir ou d'améliorer le logiciel, sans l'aide d'une autre personne ou d'une référence. Le fournisseur s'engage également à tenir entièrement à jour les informations entiercées pendant la durée du contrat.

12.3 À chaque fois d'un évènement permet à BT ou au tiers séquestre, selon le cas, d'utiliser et/ou de publier les informations entiercées, le fournisseur s'engage, à ses frais, à fournir immédiatement à BT, pendant une période d'une durée raisonnable, les conseils, le soutien, l'assistance, les données, les informations, l'accès aux employés clés du fournisseur ou de son concédant de licence du logiciel, dans le but de comprendre, maintenir (y compris les mises à jour), améliorer, modifier et corriger de quelconques informations entiercées et/ou le logiciel.

12.4 Sans effet sur de quelconques autres droits à sa disposition, BT aura automatiquement le droit non-exclusif, perpétuel, irrévocable et mondial d'utiliser gratuitement les informations entiercées, après leur publication, afin de maintenir et de soutenir les fournitures et le droit non-exclusif, perpétuel, irrévocable, mondial et gratuit d'utiliser, copier, maintenir (y compris la mise à jour), modifier, adapter, améliorer et corriger les fournitures et de quelconques fournitures modifiées, adaptées, améliorées et/ou corrigées, et de concéder sous licence ces fournitures à des tiers (sous réserve des limitations de quelconques licences concédées au fournisseur), ainsi que le droit d'autoriser des tiers à agir aux fins suscitées pour le compte de BT.

12.5 Cette clause continuera à être en vigueur après l'expiration ou à la résiliation du contrat.

12.6 Si c'est nécessaire afin d'assurer la conformité en matière de sécurité, le Contact de la Sécurité du réseau BT (et/ou les personnes qu'il aura désignées, qui seront toutes des employés de BT) aura des droits analogues (mutatis mutandis), si la demande en est faite dans le cadre des Fournitures, de la Familiarisation et de la Validation (selon les définitions de la Convention d'accès à l'information) au titre des Documents sources (selon la définition de la Convention d'accès à l'information).

13. Accès aux systèmes de BT

Le fournisseur est tenu de respecter les clauses de la section 13 si son Personnel du contrat a besoin d'accéder aux systèmes de BT afin de fournir les fournitures.

13.1 À son bon gré et dans la mesure qu'il définit, BT peut autoriser un accès uniquement aux fins de l'approvisionnement des fournitures, lorsque le fournisseur est autorisé à avoir cet accès.

13.2 En ce qui concerne l'accès, le fournisseur s'engage (et, le cas échéant, il prend l'engagement pour tout son Personnel du contrat) à :

a) S'assurer que les identifiants des utilisateurs, les mots de passe, les codes PIN, les jetons et les accès à la vidéo-conférence sont personnels pour les membres du Personnel du contrat et ne sont pas partagés. Ces détails doivent être stockés de manière sécurisée et séparément du dispositif utilisé pour y accéder. Si une autre personne connaît un mot de passe, il doit être changé immédiatement.

b) À la demande raisonnable de BT, lui fournir les rapports concernant le Personnel du contrat autorisé à accéder aux systèmes de BT.

c) L'interconnexion des domaines avec les Systèmes BT est interdite, sauf si le Contact de Sécurité BT donne son approbation et son autorisation spécifiques au moyen de l'Annexe 3.

d) Mettre tous les efforts raisonnables en œuvre pour s'assurer qu'aucun virus ou code malveillant (selon les expressions généralement utilisées dans le secteur de l'informatique) n'est introduit, afin de minimiser le risque de corruption des systèmes ou des informations de BT.

e) Mettre tous les efforts raisonnables en œuvre pour s'assurer que les fichiers personnels qui contiennent des informations, des données ou des supports qui n'ont aucun rapport avec les fournitures ne sont pas stockés sur les serveurs de BT, les ordinateurs portables et PC fournis par BT, les installations de stockage centralisé de BT ou les systèmes de BT.

13.3 Si BT a fourni au fournisseur un accès à Internet/l'intranet, le fournisseur s'engage à accéder de manière appropriée à Internet/l'intranet, pour permettre de fournir les fournitures, le cas échéant, et il s'assurera que son Personnel de contrat respecte les mêmes règles. Il relève de la responsabilité du fournisseur de s'assurer que les conseils suivants sur l'usage abusif d'Internet et des courriels sont communiqués aux membres concernés du Personnel du contrat au moins une fois par an.

Il est interdit d'accéder à des contenus qui pourraient être considérés comme étant : -

a. De nature insultante, sexuelle, sexiste, raciste ou insultante politiquement.
b. Un acte pouvant nuire à l'honorabilité de BT ou de ses employés.
c. La gestion d'une entreprise privée.
d. Une violation des droits d'auteur.
e. La téléphonie ou des messages par Internet, comme Skype.
f. Un contournement ou la traversée du pare-feu de BT ou d'autres mécanismes de sécurité.
g. Une contribution à des sites ou l'expression de déclarations en ligne pouvant être raisonnablement attribuées aux opinions de BT.
h. Inacceptables ou dangereux et devant être bloqués pour empêcher l'utilisateur d'y accéder.

13.4 Le fournisseur s'engage à informer immédiatement BT si un quelconque membre concerné du Personnel du contrat n'a plus besoin de bénéficier de droits d'accès aux

systèmes de BT ou qu'il change de fonctions pour une raison quelconque, par rapport à la Convention, permettant ainsi à BT de désactiver ou de modifier les droits d'accès aux systèmes de BT.

14. Accès aux informations de BT sur les systèmes du fournisseur

Le fournisseur est tenu de respecter les clauses de la section 14 si les informations de BT sont stockées ou traitées sur les systèmes du fournisseur.

14.1 Si les membres du Personnel du contrat sont autorisés à accéder aux systèmes du fournisseur dans le cadre de la livraison des produits et/ou des prestations de services du fournisseur à BT, le fournisseur s'engage à :

a) S'assurer que chaque employé(e) possède un identifiant et un mot de passe uniques (conforme aux bonnes pratiques du secteur), connus uniquement de lui/d'elle, réservés exclusivement à son usage dans le cadre de la procédure de connexion sécurisée.

b) Permettre l'accès aux systèmes appartenant au fournisseur qui contiennent ou permettent d'accéder aux informations de BT ou aux systèmes de BT, uniquement dans la mesure nécessaire pour permettre aux membres du Personnel du contrat de s'acquitter de leurs fonctions dans le cadre de la Convention.

c) Maintenir des procédures formelles pour contrôler l'attribution, la révision, la révocation et/ou la résiliation des droits d'accès.

d) S'assurer que l'attribution et l'utilisation des privilèges avancés et l'accès aux outils et installations sensibles dans les systèmes du fournisseur sont contrôlés et limités exclusivement aux utilisateurs qui en ont besoin dans le cadre professionnel. L'accès et l'exploitation des consoles des systèmes doivent s'effectuer dans un cadre sécurisé, compatible aux actifs ainsi gérés. Une sécurité physique appropriée doit être mise en place pour empêcher tout accès non autorisé.

e) S'assurer que l'attribution des mots de passe pour accéder aux systèmes appartenant au fournisseur, contenant des informations de BT ou permettant d'y accéder, est contrôlée par une procédure de gestion formelle, permettant un audit.

f) Évaluer régulièrement les droits d'accès des utilisateurs.

g) S'assurer que l'accès physique au matériel informatique permettant d'accéder aux informations de BT ou de les stocker s'effectue exclusivement au moyen de cartes à puce ou de proximité (ou des systèmes de sécurité équivalents) et que le fournisseur réalise régulièrement un audit interne pour veiller au respect de ces dispositions.

h) Faire la preuve que les utilisateurs respectent les bonnes pratiques en matière de sécurité dans la gestion de leurs mots de passe.

i) Mettre en œuvre un système de gestion des mots de passe, procurant des installations interactives sécurisées et efficaces, pour garantir la qualité des mots de passe.

j) S'assurer que les sessions des utilisateurs sont fermées après une période d'inactivité définie.

k) Assurer la production de journaux d'audit afin d'enregistrer l'activité des utilisateurs et les évènements relatifs à la sécurité et s'assurer qu'ils sont gérés de manière sécurisée. Les journaux devront être conservés pendant une période raisonnable afin de faciliter une quelconque investigation sans aucune capacité de la part du fournisseur de permettre un accès non-autorisé ou la modification des journaux d'audit.

l) S'assurer que la réalisation du suivi des journaux d'audit et des rapports d'analyse concernant des anomalies de comportement et/ou des tentatives d'accès non-autorisé est effectuée par des employés du fournisseur indépendants des utilisateurs qui font l'objet du suivi.

14.2 Le fournisseur s'engage à maintenir des systèmes qui détectent et enregistrent toute tentative d'endommagement, de modification ou d'accès non-autorisé aux informations de BT sur les systèmes du fournisseur. Il s'agit par exemple, sans exclusivité toutefois, des processus d'enregistrement et d'audit des systèmes, IDS, IPS, etc.

14.3 Le fournisseur s'engage à maintenir des contrôles permettant de détecter et de protéger contre les logiciels malveillants et à s'assurer de la mise en œuvre de procédures appropriées de sensibilisation des utilisateurs.

14.4 Le fournisseur s'engage à s'assurer qu'au moins une fois par mois, les logiciels non-autorisés sont identifiés et supprimés des systèmes du fournisseur qui détiennent ou traitent des informations de BT ou permettent d'y accéder.

14.5 Le fournisseur s'engage à veiller à ce que l'accès aux ports de diagnostic et de gestion, ainsi que les outils de diagnostic, sont contrôlés pour en garantir la sécurité.

14.6 Le fournisseur s'engage à s'assurer que l'accès aux outils d'audit du fournisseur est restreint aux membres concernés du Personnel du contrat et que leur utilisation est surveillée.

14.7 Le fournisseur s'engage à s'assurer que les révisions de codes et les tests d'intrusion sur tous les logiciels produits en interne et utilisés pour traiter les informations de BT sont réalisés par une équipe indépendante des développeurs.

14.8 Dans la mesure où de quelconques serveurs sont utilisés pour fournir les fournitures, ils ne doivent pas être déployés sur des réseaux qui ne sont pas fiables (un réseau se trouvant en dehors de votre périmètre de sécurité, qui ne sont pas sous votre contrôle administratif, par ex. sur Internet) sans des contrôles de sécurité appropriés.

14.9 Les modifications apportées aux systèmes individuels du fournisseur, contenant et traitant des informations de BT et/ou qui sont utilisés pour fournir les produits et/ou les services à BT, doivent être contrôlées et soumises à des procédures formelles de contrôle des modifications.

14.10 Les horloges internes de tous les systèmes doivent être synchronisées à partir d'une source fiable.

15. Hébergement d'informations de BT par le fournisseur

Le fournisseur est tenu de respecter les clauses de la section 15 s'il héberge à l'extérieur les informations de BT classées comme étant Confidentielles ou à un niveau supérieur dans un environnement de Services cloud ou dans l'environnement des serveurs du fournisseur ou de ses sous-traitants.

15.1 En ce qui concerne les fournitures, le fournisseur s'engage à s'assurer que les environnements où sont hébergées les informations de BT sont conformes aux exigences de l'Annexe 5.

16. Sécurité du réseau

Le fournisseur est tenu de respecter les clauses de la section 16 s'il construit, développe ou soutient les réseaux de BT ou des actifs de réseau.

16.1 En ce qui concerne les fournitures, le fournisseur s'engage à mettre en œuvre les mesures de sécurité approuvées pour l'ensemble des éléments fournis, de sorte à préserver la confidentialité, la disponibilité et l'intégrité des réseaux de BT et/ou des actifs 21CN. Le fournisseur s'engage à fournir à BT toute la documentation relative à la mise en œuvre de la sécurité du réseau en ce qui concerne les fournitures et il s'engage à s'assurer que cette sécurité et lui-même :

(a) sont conformes à toutes les exigences légales et réglementaires ;
(b) mettent en œuvre tous les efforts pour empêcher des personnes non-autorisées (par ex. des pirates) d'accéder aux éléments de gestion du réseau et à d'autres éléments auxquels on accède via les réseaux de BT et/ou 21CN ;
(c) mettent en œuvre tous les efforts pour réduire le risque d'usage abusif des réseaux de BT et/ou de 21CN, pouvant entraîner potentiellement une perte de revenus ou de service, par les personnes qui ont le droit d'y accéder ;
(d) mettent en œuvre tous les efforts pour détecter de quelconques violations de la sécurité, permettant ainsi de rectifier rapidement de quelconques problèmes en résultant, d'identifier les personnes qui ont obtenu cet accès et de déterminer la manière dont elles l'ont obtenu ; et
(e) minimisent le risque d'erreur de configuration des réseaux de BT, par ex. en accordant le minimum de permissions requises pour s'acquitter du rôle prévu par le contrat.

16.2 Le fournisseur devra prendre toutes les mesures raisonnables pour sécuriser toutes les interfaces sur les éléments fournis et ne devra pas présumer que les éléments fournis sont exploités dans un environnement sécurisé.

16.3 Le fournisseur s'engage à fournir au Contact de la Sécurité du réseau BT le nom, l'adresse (et les autres détails éventuellement demandés par BT) de tous les membres du Personnel du contrat qui seront le cas échéant impliqués directement dans le déploiement, la maintenance et/ou la gestion des fournitures, avant qu'ils soient engagés respectivement dans ce déploiement, cette maintenance et/ou cette gestion.

16.4 En ce qui concerne les activités de soutien basées au Royaume-Uni, le fournisseur engagera une équipe de sécurité compétente, comprenant au moins un ressortissant britannique, qui sera disponible pour faire la liaison avec le Contact de la sécurité du réseau BT (ou les personnes qu'il aura désignées) et pour participer aux réunions que le Contact de la sécurité du réseau BT exigera le cas échéant, de manière raisonnable.

16.5 Le fournisseur s'engage à fournir au Contact de la Sécurité du réseau BT un calendrier (mis à jour occasionnellement si nécessaire) de tous les éléments actifs compris dans les fournitures et leurs sources respectives.

16.6 Le fournisseur fournira des détails des membres de son personnel qui feront la liaison avec l'équipe chargée de la gestion de la vulnérabilité de BT (CERT) par rapport aux discussions à propos de BT et aux vulnérabilités identifiées par le fournisseur au titre des fournitures. Le fournisseur s'engage à fournir à BT dans les délais impartis des informations sur les vulnérabilités et à se conformer aux exigences éventuellement prescrites par le Contact de la sécurité du réseau BT, le cas échéant, au titre de ces vulnérabilité, aux frais du fournisseur. Le fournisseur s'engage à informer BT des quelconques vulnérabilités dans un délai suffisant pour permettre de mettre en place des contrôles correctifs, avant que le fournisseur rende les vulnérabilités publiques.

16.7 Le fournisseur s'engage à donner au Contact de la sécurité du réseau BT et aux personnes qu'il aura désignées le cas échéant un accès complet et sans restriction aux locaux où les fournitures sont développées, construites ou fabriquées, afin de réaliser des tests de conformité à la sécurité et/ou des évaluations. Le fournisseur s'engage à coopérer (et veillera à ce que tous les membres concernés du Personnel du contrat coopèrent) à ces tests de conformité.

16.8 Le fournisseur s'engage à s'assurer que les quelconques éléments relatifs à la sécurité qui sont compris dans les fournitures, tels qu'ils sont identifiés par BT ou à l'adresse de BT le cas échéant, sont évalués par un tiers externe, aux frais du fournisseur et à la satisfaction raisonnable de BT.

16.9 En ce qui concerne les quelconques informations fournies par ou obtenues de BT qui portent la mention « STRICTEMENT CONFIDENTIELLES » ou qu'il est facile d'interpréter comme étant confidentielles, le fournisseur s'engage à s'assurer que :

(a) seuls les membres du Personnel de sécurité spécifiquement autorisés par BT à les consulter et à les traiter sont autorisés à y accéder et qu'un registre est tenu de cet accès ;
(b) elles sont traitées, utilisées et stockées avec la plus grande attention et qu'elles sont chiffrées avant leur stockage au moyen de PGP ou de WinZip 9, dans des conditions permettant un grand degré de résistance à une compromission délibérée (c.-à-d. au moyen de l'algorithme de chiffrement le plus fiable qui soit / d'un mot de passe fort) et rendant la détection d'une compromission avérée ou d'une tentative de compromission plus probable ;
(c) lors de leur transmission, elles subissent une sécurité adéquate par un chiffrement au moyen de Secure Email, PGP ou WinZip 9 ; et
(d) elles ne sont pas exportées en dehors de la Zone économique européenne sans l'autorisation écrite de BT.

16.10 Le fournisseur s'engage à fournir rapidement, et dans tous les cas dans un délai de sept jours ouvrables, au Contact de la Sécurité du réseau BT l'ensemble des détails des quelconques caractéristiques et/ou fonctions des fournitures (ou qui sont prévues dans le Programme pour de quelconques fournitures) dont le cas échéant :

(a) le fournisseur a connaissance ; ou
(b) le Contact de la Sécurité du réseau BT pense raisonnablement qu'elles visent à une interception illégale ou toute autre interception du trafic de télécommunication, qu'elles pourraient être utilisées à ces fins, et en informera le fournisseur. Ces détails devront inclure toutes les informations qui sont raisonnablement nécessaires pour permettre au Contact de la Sécurité du réseau BT de comprendre parfaitement la nature, la composition et l'étendue de ces caractéristiques et/ou de ces fonctions.

16.11 Afin de maintenir l'accès aux réseaux et/ou systèmes de BT, le fournisseur s'engage à informer immédiatement BT de toute modification de sa méthode d'accès à travers les pare-feu, y compris la fourniture de la traduction d'adresse réseau.

16.12 Il est interdit d'utiliser des outils de surveillance du réseau permettant de consulter les informations des applications.

16.13 Il est impératif de désactiver la fonction IPv6 des systèmes d'exploitation sur les hôtes (périphériques d'utilisateur final, serveurs) se connectant aux domaines du réseau de BT et de la désactiver quand elle n'est pas requise.

16.14 Le fournisseur s'engage à se conformer et à s'assurer que les fournitures se conforment aux politiques de BT si elles sont fournies, ainsi qu'aux Exigences de sécurité. Toute non-conformité doit être convenue lors de la signature du contrat ou dans le cadre d'un contrôle des modifications.

16.15 Le fournisseur s'engage à s'assurer que tous les membres du Personnel du contrat ont subi des vérifications préalables à l'embauche appropriés au niveau de l'accès http://www.selling2bt.bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf

Les fournisseurs chargés de la construction, du développement ou de la prise en charge des réseaux de BT ou des actifs de réseau s'engagent à s'assurer que tous les membres du Personnel du contrat ont subi au minimum des vérifications préalables à l'embauche de niveau L2. Les vérifications préalables à l'embauche de niveau L3 seront obligatoires pour les fonctions identifiées par le Contact de la Sécurité du réseau BT. Si le fournisseur n'a pas la capacité de déterminer directement la cote de sécurité des membres du Personnel du contrat dans le cadre des vérifications de niveau L3, BT lui apportera son assistance à ce titre, aux frais du fournisseur.

17. Sécurité du réseau du fournisseur

Le fournisseur est tenu de respecter les clauses de la section 17 si son réseau doit être utilisé afin de fournir les fournitures (il s'agit notamment du LAN, WAN, des réseaux Internet, sans fil et radio)

17.1 En ce qui concerne les fournitures, le fournisseur s'engage à mettre en œuvre des mesures de sécurité sur l'ensemble de ses réseaux, de sorte à préserver la confidentialité, la disponibilité et l'intégrité des informations de BT. Les mesures devront :

(a) être conformes à toutes les exigences légales et réglementaires ;
(b) mettre en œuvre tous les efforts pour éviter que des personnes non autorisées (par ex. des pirates) accèdent au réseau ;
(c) mettre en œuvre tous les efforts pour réduire le risque d'usage abusif des réseaux, pouvant entraîner potentiellement une perte de revenus ou de service, par les personnes qui ont le droit d'y accéder ;
(d) mettre en œuvre tous les efforts pour détecter de quelconques violations de la sécurité, permettant ainsi de rectifier rapidement de quelconques problèmes en

résultant, d'identifier les personnes qui ont obtenu cet accès et de déterminer la manière dont elles l'ont obtenu.

18. Sécurité du cloud

Le fournisseur est tenu de respecter les clauses de la section 18 s'il fournit à BT des services relatifs au cloud. Pour la définition du cloud, consultez la publication NIST http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf)

18.1 Les fournisseurs s'engagent à fournir des justificatifs appropriés, prouvant que les services cloud fournis respectent les exigences de contrôle prescrites par la Matrice de contrôle cloud (CCM) de la Cloud Security Alliance, conformément à la version la plus récente publiée sur le site https://cloudsecurityalliance.org , en plus du respect de l'Annexe 5 des présentes exigences de sécurité.

18.2 Les informations de BT concernées par le commerce électronique utilisant les réseaux publics devront être protégées conformément à l'Annexe 1 pendant leur transfert et leur stockage (y compris les sauvegardes) contre toute activité frauduleuse, une divulgation, un accès ou une modification qui n'a pas été autorisé(e).

18.3 Les accords de niveau de service pour les réseaux et les infrastructures (internes ou externalisés) devront documenter clairement les contrôles de sécurité, la capacité et les niveaux de service, les exigences de l'entreprise ou des clients.

18.4 Le fournisseur s'engage à autoriser les tests d'intrusion et/ou l'accès aux rapports existants du fournisseur sur les tests d'intrusion par rapport aux fournitures fournies, la portée et la date des tests devant être fixées par un accord mutuel avec BT.

18.5 Le fournisseur s'engage à mettre en œuvre les mesures de sécurité convenues pour tous les éléments fournis, de manière à préserver la confidentialité, la disponibilité, la qualité et l'intégrité des fournitures, en minimisant les occasions permettant à des personnes non autorisées (par ex. d'autres clients du cloud) d'accéder aux informations et aux services de BT.

Glossaire

Dans les présentes Exigences de sécurité, les définitions suivantes seront applicables, sinon les conditions du contrat s'appliqueront aux présentes Exigences de sécurité. Tous les mots et expressions utilisés dans les présentes Exigences de sécurité auront la même signification que celle qui leur est donnée dans le contrat :

[« **Accès** » : le traitement ou le stockage des informations de BT par l'une ou plusieurs des méthodes suivantes :

- Par interconnexion avec les systèmes de BT
- Fourni sous format papier ou non électronique
- Informations de BT sur les systèmes du fournisseur
- Par support mobile

et/ou accès aux locaux de BT pour fournir les services (à l'exclusion de la livraison de matériel et la participation à des réunions)

« **Autorisé** » : BT a approuvé l'accès soit dans le cadre du processus d'Interconnexion des systèmes de BT, soit par autorisation écrite reçue de la part de l'entreprise BT ou du propriétaire du projet BT ; le terme « **autorisation** » sera interprété en conséquence. Le niveau d'accès fourni sera pertinent et limité aux besoins nécessaires pour fournir les fournitures.]
« **Articles de BT** » : tous les articles fournis au fournisseur par BT et tous les articles détenus par le fournisseur qui appartiennent à BT. (Par ex. les clés des armoires, les jetons des ordinateurs portables, les cartes d'accès, les plans, les documents de processus.)
« **Contact de la Sécurité du réseau BT** » : un professionnel de l'assurance de l'information du service Sécurité de BT, contacté en remplissant et en envoyant le formulaire de demande de l'Annexe 3, ou toute autre personne dont l'identité et les coordonnées peuvent être communiquées occasionnellement au Contact commercial du fournisseur.
« **Biens physiques de BT** » : tous les biens physiques appartenant à BT que détient le fournisseur. (Par ex. routeurs, commutateurs, serveurs ou documentation.)
« **Sécurité BT** » : le service de sécurité au sein de BT.
« **Contact de sécurité BT** » : un professionnel de l'assurance de l'information du service Sécurité BT, contacté en remplissant et en envoyant le formulaire de demande de l'Annexe 3.
« **Politique de sécurité de BT** » : la politique de sécurité du réseau concerné de BT, fournie par BT.
« **Systèmes de BT** » : les services et les éléments du service, les produits, les réseaux, les serveurs, les processus, le système sous format papier ou les systèmes informatiques (en totalité ou en partie) qui sont la propriété de BT et/ou qui sont exploités par ou pour le compte de BT, du BT Group plc ou d'une quelconque entité du BT Group plc, ou tout autre système éventuellement hébergé dans les locaux de BT (y compris iSupplier (selon la définition de « iSupplier » de la section de la Convention intitulée « Paiement et facturation ») et utilisé dans le contexte de « l'accès » (voir la définition ci-dessus).
« **Vidéosurveillance** » : surveillance par système de télévision en circuit fermé
« **Date de début** » : voir la définition dans le contrat.
« **Personnel du contrat** » « **Membre concerné du Personnel du contrat** » : voir la définition dans le contrat.
« **Information** » : les informations sous une forme matérielle ou autre, y compris, mais sans exclusivité toutefois, les cahiers des charges, les rapports, les données, les notes, la documentation, les plans, les logiciels, les politiques, les procédures, les processus, les normes, les sorties d'ordinateur, les conceptions, les schémas de circuit, les modèles, les gabarits, les échantillons, les inventions (qu'elles puissent être brevetées ou pas) et le savoir-faire, ainsi que les supports (le cas échéant) sur lesquels cette information est fournie.
« **ISO 27001** » : une norme internationale de gestion de la sécurité de l'Organisation internationale de normalisation et de la Commission électrotechnique internationale.
« **Commande(s)** » : une commande de BT au fournisseur pour les fournitures, passée conformément au contrat.
« **Sécurité du réseau** » : la sécurité de l'interconnexion des voies et des nœuds de communication qui connectent ensemble de manière logique les technologies d'utilisation finale et les systèmes de gestion associés.
« **Données personnelles** » : les définitions sont celles de la Directive 95/46/CE ou des quelconques lois ultérieures s'y rapportant (« la directive »).
« **Processus** », « **Traité(e)(s)** » ou « **Traitement** » : n'importe quelle opération ou ensemble d'opérations, réalisée(s) sur les informations de BT, que ce soit ou pas par des moyens automatiques, tels que la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la communication par

transmission, la dissémination ou bien la mise à disposition, l'alignement ou l'assemblage, le blocage, la suppression, le retour ou la destruction.
« **Informations sensibles** » : n'importe quelle information de BT qui porte la mention « Document confidentiel » ou celle d'une classification supérieure, y compris les données personnelles.
« **Sous-traitant** » : voir la définition dans le contrat.
« **Systèmes du fournisseur** » : les quelconques ordinateurs, applications ou systèmes de réseau appartenant au fournisseur, utilisés pour accéder, stocker ou traiter les informations de BT ou impliqués dans l'approvisionnement des fournitures.
« **Contact de la sécurité du fournisseur** » : une personne dont les coordonnées seront communiquées occasionnellement à BT par le fournisseur et qui sera le point de contact unique pour les questions relatives à la sécurité.
« **Fournitures** » : tous les éléments, matériaux, matériels, outils, équipements de test, documents, micrologiciels, logiciels, pièces détachées, pièces et objets à fournir à BT en vertu du contrat, ainsi que toutes les informations et travaux qui doivent être fournis ou réalisés pour BT en vertu du contrat.
« **Transfert** » ou « **Transféré** » :
(a) Le déplacement des informations de BT dont le Personnel du contrat a la possession (y compris, mais sans exclusivité toutefois, les données personnelles) d'un lieu ou d'une personne à un ou une autre, que ce soit par des moyens physiques, vocaux ou électroniques ;
(b) la concession du droit d'accès aux informations de BT dont le Personnel du contrat a la possession (y compris, mais sans exclusivité toutefois, les données personnelles) en un lieu ou par une personne, que ce soit par des moyens physiques, vocaux ou électroniques.