Table des matières

1. Introduction

1.1 Ce document explique les exigences de sécurité de BT. Il s'applique à tous les tiers travaillant pour le compte ou au nom de BT Group, Openreach, EE et PlusNet inclus et pour lesquels nous utiliserons le terme générique « BT » dans le reste de ce document.

1.2 Ces exigences de sécurité s'ajoutent et sont sans préjudice d'autres obligations des tiers incluses dans le contrat.

1.3 Les normes mentionnées dans ce document peuvent être consultées à l'adresse suivante. Normes applicables aux tiers

2. Exigences relatives aux accès limités

2.1 Sans préjudice d'une obligation de confidentialité à laquelle le tiers pourrait devoir se conformer, tout membre du personnel d'un tiers amené à accéder à des informations de BT est tenu de :

2.2 veiller à ce qu'aucune information de BT ne soit divulguée au personnel du tiers, qui ne devra pouvoir y accéder que si le service pour lequel il a été mandaté l'exige et

2.3 mettre en place les systèmes et processus, tant techniques qu'organisationnels, nécessaires pour protéger les informations de BT du risque de (i) destruction accidentelle ou illégale et (ii) de perte, d'altération, de divulgation non autorisée ou d'accès aux informations de BT, conformément aux Good Industry Security Practices (Bonnes pratiques de sécurité de l'industrie).

3. Sécurité générale des informations

3.1 À la demande raisonnable de BT, le tiers fournira les copies des certifications de sécurité et déclarations de conformité applicables au service, afin de montrer son respect de ces exigences de sécurité.

3.2 En cas de changement important des technologies ou normes de sécurité du secteur, de changements significatifs des services ou de la manière dont le tiers s'en acquitte, BT peut produire un avenant au contrat pendant sa durée de validité si ces modifications entraînent une modification des exigences de sécurité applicables. Le tiers s'engage à se conformer dans des délais raisonnables aux termes de l'avenant au contrat convenu, compte tenu de la nature de la modification et du risque encouru par BT.

3.3 Le tiers doit, au moins une fois par an ou en cas de changement significatif des services ou de la manière dont le tiers s'en acquitte, réviser ces exigences de sécurité et les normes connexes, afin de veiller à ce qu'elles restent conformes aux contrôles de sécurité applicables.

3.4 Si le tiers sous-traite des obligations dans le cadre du contrat, il veillera à ce que les contrats passés avec les sous-traitants concernés et leurs sous-traitants incluent des termes écrits exigeant de la part du sous-traitant qu'il respecte les sections applicables de ces exigences de sécurité ou les exigences de sécurité équivalentes du tiers.

3.5 Les informations de BT peuvent être conservées suffisamment longtemps pour permettre l'exécution du contrat, période après laquelle elles ne devraient pas l'être

au-delà de deux ans, au plus, à moins qu'une autre période de conservation n'ait été convenue entre BT et le tiers concerné ou ne soit stipulée par la loi.

3.6 Si les services s'appliquent directement à un contrat avec le gouvernement britannique, le tiers doit se conformer à la version la plus à jour de la norme Cyber Essentials Plus.

3.7 Il incombe au tiers de veiller à ce que les informations de BT soient traitées conformément aux contrôles des normes suivantes :

- 3rd Party Information Classification and Data Handling Standard V4.0 (Norme de classification des informations et de manipulation des données applicable aux tiers)
- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

  Section 1 Rôles et responsabilités.

  Section 2 Gouvernance.

  Section 3 Gestion des incidents.

  Section 4 Gestion du changement.

  Section 5 Gestion des cyber-risques et menaces.

  Section 6 Gestion des identités et contrôle d'accès.

  Section 10 Classification et protection des données.

  Section 12 Prévention des fuites de données.

  Section 13 PCI-DSS (si le champ d'application du service l'exige).

  Section 19 Gestion des vulnérabilités.

  Section 22 Journalisation et surveillance continues.

4. Sécurité du personnel de tiers

4.1 Le tiers veillera à ce que ses effectifs aient mis en place les accords de confidentialité nécessaires, avant de commencer à travailler dans les locaux de BT, sur des systèmes de BT ou de pouvoir accéder à des informations de BT. Les preuves de ces accords de confidentialité, qui doivent être conservés par le tiers, doivent être mises à la disposition de BT à des fins d'audit.

4.2 Le tiers traitera les violations des contrôles et normes de sécurité BT applicables en appliquant les processus formels et notamment, les mesures disciplinaires qui s'imposent, susceptibles d'entraîner les interdictions suivantes :

4.2.1 interdiction d'accès aux systèmes de BT et informations de BT ou

4.2.2 interdiction d'exécuter des travaux se rapportant à la prestation du service.

En outre, le tiers vérifiera que les processus pertinents ont été mis en place pour faire en sorte que le personnel du tiers visé par ces interdictions ne puisse plus, ultérieurement, accéder aux systèmes de BT, aux informations de BT ou ne soit autorisé à travailler dans le cadre de la prestation du service.

4.3 Le tiers veillera, dans les limites autorisées par la loi, à mettre au service de son personnel, une cellule confidentielle pour permettre à ce dernier de signaler, de manière anonyme, qu'il a été invité à agir en contradiction avec ou en violation de ces exigences de sécurité. Rapports pertinents à signaler à BT.

- Quand un membre du personnel du tiers cesse d'être affecté au service, les actifs corporels de BT ou informations de BT dont dispose ce membre du personnel du tiers doivent être, à la discrétion de BT: remis à l'équipe opérationnelle de BT qui convient ;
- détruits conformément à la norme 3rd Party Information Classification and Data Handling Standard V4.0 (Norme de classification des informations et de manipulation des données applicable aux tiers).

4.4 S'agissant du personnel du tiers, le tiers veillera à ce que les processus qui conviennent soient en place pour veiller à l'exécution des contrôles afférents aux normes suivantes :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

  Section 15 Médias sociaux.

  Section 23 Formation et sensibilisation.

5. Audit et examen de la sécurité

5.1 Sans préjudice d'un autre droit ou d'un audit quelconques de BT, afin d'évaluer le respect par le tiers de ces exigences de sécurité et normes connexes, le tiers accordera à BT ou à ses représentants, l'accès ou l'aide nécessaire et qui convient pour faciliter les examens de la sécurité basés sur des documents ou audits sur site. Le tiers sera informé de l'imminence d'un audit régulier sur site au moins 30 jours ouvrés avant la date programmée.

L'audit aura pour finalité l'examen des divers aspects des politiques, procédures et système(s) du tiers (sous réserve du tiers protégeant la confidentialité des informations n'ayant aucun rapport avec la prestation du service dont il s'acquitte vis-à-vis de BT), ayant un rapport avec le service fourni.

5.2 Le tiers coopèrera avec BT pour mettre en œuvre les recommandations convenues et exécuter les actions correctives, identifiées comme étant nécessaires à la suite des examens basés sur les documents ou audits sur site, dans les 30 jours après en avoir été informé par BT ou dans les délais convenus entre les parties et ce aux frais du tiers.

5.3 Au cas où BT se voyait obligée d'exécuter un audit indépendant du tiers concluant qu'il ne respecte pas les principes et pratiques de la norme ISO/IEC 27001:2013, le tiers s'engage à prendre, à ses propres frais, les mesures qui s'imposent pour restaurer l'état de conformité nécessaire et à rembourser, intégralement, les frais dont BT aurait pu devoir s'acquitter relativement à un tel audit.

6. Droit d'inspection

6.1 Le tiers doit donner à BT le droit d'inspection, conformément à la norme suivante :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 24 Droit d'inspection.

7. Certifications de sécurité

7.1 Les systèmes, le service, les services connexes, processus et emplacements physiques du tiers doivent être continuellement conformes à la norme ISO/IEC 27001:2013 (ou aux certification(s) attestant de contrôles équivalents, avec rapport d'audit indépendant à

l'appui), ainsi qu'à toute version ultérieure ou modifiée de la norme délivrée. Cette conformité doit être assurée par l'un des moyens suivants :

7.1.1 certification du système ISMS du tiers par UKAS ou un organisme international de certification équivalent agréé, le champ d'application et la déclaration d'applicabilité ayant été validés par BT ou

7.1.2 processus d'audit et d'essai bilatéral spécifié par BT.

7.2 le tiers doit soumettre un certificat en cours de validité au début du contrat et à chaque renouvellement de certification ultérieur.

7.3 En cas de changement, à n'importe quel moment, du champ d'application ou de la déclaration d'applicabilité, le tiers doit faire valider le changement en recourant à la procédure de contrôle du changement (ou, à défaut de procédure de contrôle du changement, par le biais du processus de modification). Le tiers doit informer BT, dans les deux jours ouvrés, de toute occurrence de non-conformité identifiée par l'organisme de certification ou lui-même.

8. Sécurité physique – locaux de BT

8.1 Dans les cas où le tiers travaille dans les locaux de BT, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 25. Sécurité physique – locaux de BT

9. Sécurité physique – locaux de tiers

9.1 Dans les cas où les locaux du tiers servent à la prestation du service, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 9. Sécurité physique dans les locaux du tiers **exception étant faite** des contrôles 9.10 et 9.11 pour la mise à disposition d'un environnement d'hébergement destiné aux équipements de BT.

10. Mise à disposition d'un environnement d'hébergement destiné aux équipements de BT

10.1 Dans les cas où les locaux du tiers servent à la mise à disposition d'un environnement d'hébergement d'équipements, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 9. Sécurité physique dans les locaux du tiers - contrôles 9.10 et 9.11 pour la mise à disposition d'un environnement d'hébergement destiné aux équipements de BT.

11. Développement de logiciels sécurisé

11.1 Dans les cas où le tiers fournit des logiciels ou systèmes, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 17 (17.1 et 17.2) Développement de logiciels sécurisé

12. Entiercement (ESCROW)

12.1 Dans les cas où l'entiercement s'impose pour protéger les différentes parties, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 17 (17.3 uniquement) Développement de logiciels sécurisé

13. Accès aux systèmes de BT

13.1 Dans les cas où les systèmes tiers ou le personnel du tiers doivent accéder ou se connecter aux systèmes de BT, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 8 Accès aux systèmes de BT

14. Systèmes tiers détenant des informations de BT

14.1 En cas d'utilisation de systèmes tiers détenant des informations de BT, les contrôles des normes suivantes s'imposent :

3rd Party Information Classification and Data Handling Standard V4.0 (Norme de classification des informations et de manipulation des données applicable aux tiers).

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 7 Gestion d'actifs informatiques

Section 11. Cryptographie.

Section 16 Configuration système.

Section 18 Protection anti-programme malveillant**.**

Section 21 Atténuations du déni de service.

15. Tiers hébergeant des informations de BT

15.1 Dans les cas où un tiers héberge des informations de BT, les locaux doivent détenir un certificat ISO/IEC 27001 en cours de validité de gestion de sécurité (ou une/des certification(s) attestant des contrôles équivalents, appuyés par un rapport d'audit indépendant).

15.2 Les contrôles de la norme suivante s'imposent :

- 3rd Party Information Classification and Data Handling Standard V4.0 (Norme de classification des informations et de manipulation des données applicable aux tiers).
- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

Section 7 Gestion d'actifs informationnels

Section 11. Cryptographie.

Section 16 Configuration système.

Section 18 Protection anti-programme malveillant**.**

Section 21 Atténuations du déni de service.

16. Sécurité du réseau – réseau appartenant à BT.

16.1 Dans les cas où le tiers doit installer des équipements sur, configurer, entretenir, réparer ou surveiller le réseau de BT, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

  Section 26 Sécurité du réseau – réseau appartenant à BT.

17. Sécurité de réseau tiers

17.1 Dans les cas où le réseau du tiers doit servir pour accéder à des informations de BT ou dans le cadre de la prestation du service, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

  Section 16 Configuration système.

  Section 20 Intégrité du réseau

18. Sécurité dans le Cloud

18.1 Dans les cas où le tiers fournit à BT des services dans le Cloud, les contrôles de la norme suivante s'imposent :

- Our Standard on 3rd Party Controls V1.1 (Norme applicable aux contrôles imposés aux tiers) – Sections

  Section 14. Informatique dans le Cloud/en ligne.

19. Centre de contact

19.1 Dans les cas où le tiers fournit à BT des services de centre de contact, les contrôles de la norme suivante s'imposent :

- Contact Centre 3rd Party Standard V1.0 (Norme applicable aux centres de contact tiers).

20. Information classée dans la catégorie OFFICIAL (Officiel) ou dans une catégorie supérieure par HMG (Le Gouvernement de Sa Majesté).

20.1 Les exigences de sécurité complémentaires définies à l'Annexe 1 de ces exigences de sécurité s'appliquent à tout tiers amené à stocker, traiter ou transmettre des informations classées dans la catégorie « Official Sensitive » (Officiel sensible), conformément au Security Classifications Scheme (Barème de classification de sécurité) du Gouvernement de Sa Majesté et aux mises à jour ponctuelles y afférentes.

20.2 Le tiers veillera à ce que les systèmes et l'infrastructure utilisés dans le cadre de la prestation du service, soient intégrés à un réseau logique dédié. Ce réseau ne sera

composé que des systèmes dédiés à la mise à disposition d'installations sécurisées de traitement des données des clients.

21. Termes définis et leur interprétation

21.1 À moins d'avoir été définis autrement ci-dessous, les mots et expressions utilisés dans ces exigences de sécurité ont le même sens que dans le contrat :

« **Accès** » s'applique au traitement, à la manipulation ou au stockage des informations de BT, en recourant à au moins une des méthodes suivantes :

a. par interconnexion avec les systèmes de BT ;

b. fournies sur papier ou dans une forme non électronique ;

c. informations de BT sur les systèmes du fournisseur ou

d. sur médias mobiles ;

et/ou l'accès aux locaux de BT à des fins d'approvisionnement en fournitures, à l'exception des livraisons de matériel et de la présence aux réunions.

« **Informations de BT** » s'applique à toute information se rapportant à BT ou à un client de BT fournie au fournisseur et toute information, traitée ou manipulée par le fournisseur au nom de BT ou un client de BT en vertu du contrat.

« **Systèmes de BT** » s'applique aux services et aux composants du service, produits, réseaux, serveurs, processus, systèmes sur support papier ou systèmes informatiques (intégralement ou partiellement), appartenant à et/ou exploités par BT ou tout autre système éventuellement hébergé dans les locaux de BT.

« **Contrat** » s'applique au contrat signé par les parties et se rapportant à la fourniture de biens, logiciels ou services faisant référence à ces exigences de sécurité.

« **Cyber Essentials Plus** » s'applique au programme appuyé par le gouvernement britannique, pour aider les organisations à se protéger contre les cyberattaques les plus communes.

« **Entiercement** » s'applique au contrat de dépôt de code source, signé conformément au contrat et couvrant l'utilisation, la copie, la conservation et la modification dudit code source pour satisfaire aux finalités commerciales de BT (droit de compiler ledit code source inclus).

« **Good Industry Security Practices** » (Bonnes pratiques de sécurité de l'industrie) fait allusion à la mise en œuvre des pratiques, politiques, normes et outils de sécurité raisonnablement et normalement attendus de la part d'une personne qualifiée et expérimentée, engagée dans le même type d'activité, dans des circonstances identiques ou similaires, quels que soient l'engagement ou les circonstances.

« **Sécurité réseau** », s'applique à la sécurité des voies et nœuds de communication reliant logiquement les technologies de l'utilisateur final les unes aux autres et aux systèmes de gestion connexes.

« **Official Sensitive Declaration** » (Déclaration officiel sensible) s'applique à la déclaration écrite que doit fournir le fournisseur, par rapport aux fonctions identifiées par ce dernier pour lesquelles devra être fourni un accès à des informations classées dans la catégorie « Official Sensitive » (Officiel sensible) ou bénéficiant de privilèges supérieurs d'accès à une infrastructure servant à stocker, traiter ou transmettre des informations classées dans la catégorie « Official Sensitive » et dont un modèle figure à l'Annexe 1.

« **Exigences de sécurité** » s'applique à ce document et à ses modifications ponctuelles.

« **Sous-traitant** » s'applique aux sous-traitants du fournisseur amenés à exécuter ou participer à la mise à disposition des fournitures, qui emploient ou embauchent des personnes participant à l'approvisionnement en fournitures.

« **Personnel du tiers** » s'applique aux personnes, quelles qu'elles soient, engagées par le fournisseur ou ses sous-traitants à des fins d'exécution des obligations du fournisseur conformément au contrat.

« **Service** désigne, sans distinction, les « **biens** », « **logiciels** » ou « **services** » définis par le contrat.

« **Système tiers** » désigne les ordinateurs, applications ou systèmes réseau appartenant au fournisseur pour lui permettre d'accéder, de stocker ou de traiter les informations de BT ou utilisés dans le cadre de l'approvisionnement en fournitures.

Interprétation

21.2 Les mots figurant après les termes « inclus », « inclut », « en particulier », « par exemple » ou toute autre expression similaire sont à considérer pour leur valeur explicative et ne limitent en rien le sens des mots, descriptions, définitions, phrases ou termes qui les précèdent.

21.3 À chaque occurrence d'un droit ou d'une obligation exprimés comme « **pouvant** » être exercés ou exécutés, l'option de l'exercer ou de l'exécuter est à la seule discrétion de la partie concernée.

21.4 Toute référence à un hyperlien (« **URL** ») renvoie à une ressource en ligne accessible par le biais de cette URL ou à toute autre URL de remplacement éventuellement signalée à la partie concernée.

ANNEXE 1 – autres exigences de sécurité

Dans les cas où le tiers doit accéder, stocker, traiter ou transmettre des informations « HMG Official Sensitive » (classées officiel sensitive par le Gouvernement de Sa Majesté), le tiers s'engage d'une part à respecter ces exigences de sécurité et toute autre exigence portée à l'Annexe 1 et de l'autre, à fournir à BT le document Official Sensitive Declaration (Déclaration officiel sensible) rempli avant la signature des contrats. Dans tous les cas, le contrôle au plus haut niveau remplacera les exigences documentées ailleurs dans ces exigences de sécurité, par rapport aux services et systèmes définis dans le document Official Sensitive Declaration.

1. PERSONNEL

1.1. Les fonctions identifiées par le tiers pour lesquelles devra être fourni un accès à des informations classées dans la catégorie « Official Sensitive » (Officiel sensible) ou bénéficiant de privilèges supérieurs d'accès à une infrastructure servant à stocker, traiter ou transmettre des informations classées dans la catégorie « Official Sensitive », devront être documentées dans le document Official Sensitive Declaration (Déclaration officiel sensible).

1.2. Le personnel de tiers occupant un poste répertorié dans la déclaration officiel sensible :

1.2.1. doit, au moins, être au soumis à un contrôle de préemploi à la norme Baseline Personnel Security Standard (BPSS - norme de sécurité du personnel de référence) ;

1.2.2. doit signer la déclaration du Official Secrets Act (loi de protection des secrets d'État) et

1.2.3. s'il n'est pas en mesure d'obtenir les autorisations de sécurité nécessaires, ne doit pas être autorisé à accéder aux informations ou systèmes.

2. FORMATION SÉCURITÉ

2.1. Le tiers organisera la formation à la sécurité au moment de l'embauche et au moins une fois par an, couvrant les exigences de manipulation des informations classées dans les catégories « Official » (Officiel) ou « Official sensitive » (Officiel sensible), en adéquation avec les exigences du Security Classifications Scheme (Barème de classification de sécurité du gouvernement britannique) dont l'explication fait l'objet du guide relatif à la protection des informations du Gouvernement de Sa Majesté.

2.2. Le tiers se chargera de mettre à jour les descriptions de postes se rapportant aux fonctions documentées dans le document Official Sensitive Declaration (Déclaration officiel sensible), pour assurer la participation à la formation décrite au paragraphe 2.1 précédent. Le tiers gardera une trace des formations, laquelle devra être fournie à BT à la demande de cette dernière.

3. CONTRÔLE D'ACCÈS.

3.1. En cas de départ ou de transfert d'un employé, ses droits d'accès doivent être révoqués des systèmes tiers concernés, dans un délai d'un (1) jour ouvré.

3.2. Dans les cas où les employés du tiers, sous-traitants et intérimaires inclus, bénéficient de privilèges de haut niveau d'accès à l'infrastructure de BT, le tiers doit avertir BT, par écrit et dans un délai d'un (1) jour que ces employés n'ont plus besoin d'accéder aux systèmes de BT (ex. départ ou transfert de personnel).

3.3. Dans les cas où les employés du tiers, sous-traitants et intérimaires inclus, disposent d'une carte d'accès permanent aux locaux de BT, le tiers doit avertir BT, par écrit et dans

un délai d'un (1) jour ouvré que ces employés n'ont plus besoin d'accéder aux locaux de BT (ex. départ ou transfert de personnel).

4. ÉVALUATION ET CLASSIFICATION DES ACTIFS

4.1. Le tiers mettra en œuvre des procédures complémentaires de manipulation des données répondant aux exigences des informations des catégories « Official » (Officiel) ou « Official Sensitive » (Officiel sensible), conformément aux exigences du programme Her Majesty's Government Security Classifications Scheme (Barème de classification de sécurité du gouvernement britannique) et des mises à jour publiées de temps à autre à ce propos.

5. INTERVENTION ET SIGNALEMENT D'INCIDENTS – CONTRAT DE NIVEAU DE SERVICE (SLA)

5.1. Le tiers sera informé des contrats de niveau de service spécifiques visant à appuyer le processus d'intervention en cas d'incident. Ces contrats peuvent remplacer tout contrat précédent exposé dans ces exigences de sécurité.

6. AUDIT, ESSAIS ET SURVEILLANCE

6.1. Le tiers assurera en 24/7 la surveillance de sécurité conformément aux consignes de BT.

6.2. L'infrastructure du tiers soumise à la surveillance de sécurité en 24/7 sera documentée dans le document Official Sensitive Declaration (Déclaration officiel sensible).

7. CONTINUITÉ ET REPRISE DE L'ACTIVITÉ

7.1. Le tiers produira un plan de continuité et de rétablissement après sinistre conforme à la norme BS ISO 22301, dans les 30 jours consécutifs à la signature du contrat.

8. EMPLACEMENT

8.1. Sauf consigne contraire formulée par BT, le service doit se situer dans les limites physiques du Royaume-Uni ou, s'il y a lieu, de l'EEE.

ANNEXE 1, PIÈCE 1 – MODÈLE DE DÉCLARATION OFFICIEL SENSIBLE

1. Systèmes/services concernés

Veuillez fournir la liste des systèmes et services fournis au client du Gouvernement de Sa Majesté.

Système	Service

2. Fonction du tiers nécessitant la détention d'un niveau d'autorisation de sécurité.

Fonction	Niveau d'autorisation de sécurité requis
* *e.g. DBA*	*SC*

3. Gestion des vulnérabilités

Système	Type d'évaluation des vulnérabilités	Fréquence

4. Audit, essais et surveillance

Systèmes à surveiller en 24/7, conformément aux recommandations de BT.