Table des matières

1. Introduction

1.1 Les clients de BT s'attendent à ce que BT et ses fournisseurs dispensent leurs services en utilisant des systèmes de gestion de la sécurité des informations (ISMS) conformes aux normes industrielles. Votre ISMS doit couvrir l'infrastructure, les réseaux, les équipements et les systèmes informatiques afin de protéger les services effectués et les informations des clients de BT/BT dans le cadre de ces services. 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. Vous serez informé des ensembles de contrôles de sécurité applicables au service que vous effectuez pour BT.

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

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 En cas de modifications importantes des services ou de la manière dont ils sont effectués, le tiers s'engage à revoir la présente politique relative aux exigences de sécurité afin de s'assurer qu'elle est toujours conforme à tous les 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 Dans les cas où le tiers doit sous-traiter la prestation de service à une société amenée à détenir ou traiter des informations de BT, il incombe au tiers d'obtenir l'accord de la partie prenante de BT quant à l'information pouvant être communiquée à cette autre société. Le tiers doit s'assurer qu'il a une relation contractuelle avec le sous-traitant et doit s'assurer que le sous-traitant exploite un cadre de sécurité standard de l'industrie.

3.6 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.

3.7 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 – https://www.cyberessentials.ncsc.gov.uk/

3.8 Lorsque les informations de BT sont traitées ou stockées à l'étranger, le tiers doit informer BT des emplacements géographiques, et BT se réserve le droit de rejeter les emplacements jugés à haut risque.

Traitement des informations sur BT

Sauf avis contraire de la part de BT, toutes les informations de BT sont classées comme « confidentielles ». Lorsque des données personnelles ou des données personnelles sensibles sont concernées, il convient de demander conseil à votre équipe chargée de la protection des données et de la confidentialité au cas où des contrôles supplémentaires seraient nécessaires.

Les contrôles de sécurité suivants sont des « exigences de traitement de la voix » dont la portée est limitée aux communications verbales.

3.9 S'il est nécessaire de discuter, de montrer ou d'échanger des informations sur BT à l'aide d'une plateforme de collaboration, par exemple Teams.

- Assurez-vous que seules les personnes qui ont besoin de connaître l'information sont présentes.
- Si un tiers ou un entrepreneur externe est impliqué, il doit avoir signé un contrat avec vous ou avoir conclu un accord de confidentialité avant le début des discussions.
- Vous devez vérifier qui est sur la conférence avant de commencer.

3.10 S'il est nécessaire de discuter des informations sur BT avec une personne en face à face, sur un téléphone portable ou une ligne téléphonique standard.

- Les conversations ne doivent pas être tenues ou entendues par des personnes qui n'ont pas besoin d'avoir accès à ces informations.
- Si la conversation doit avoir lieu avec un tiers ou un contractant externe, celui-ci doit avoir signé un contrat avec vous, ou un accord de confidentialité doit être mis en place avant le début des discussions.

- Les informations confidentielles ou strictement confidentielles ne doivent pas être laissées sur les services de messagerie vocale.

Les contrôles de sécurité suivants sont des « exigences de traitement écrit » et ont un champ d'application couvrant le matériel conservé sur papier. Cela comprend, sans s'y limiter, les lettres manuscrites, les procès-verbaux, les notes et les mémos. Cela comprend également les documents électroniques imprimés, tels que les documents de travail et les rapports, dès lors qu'ils se présentent sous forme de papier.

3.11 Si vous stockez des copies papier des informations de BT dans les locaux d'un tiers, celles-ci doivent être gardées de façon sécurisé dans une installation verrouillable, avec un accès limité aux seules personnes ayant besoin de consulter les documents. Les documents ne doivent pas être laissés sans surveillance.

3.12 S'il est nécessaire d'imprimer, de photocopier ou de dupliquer des informations sur BT, les contrôles de sécurité suivants s'appliquent :

- Utilisez uniquement les installations d'impression ou de copie qui se trouvent dans vos locaux.
- Les photocopies ou les impressions ne doivent pas être laissées sans surveillance sur le lieu d'impression, et doivent être récupérées au moment de la création.
- Si l'imprimante ou la photocopieuse dispose d'une capacité de mémoire permettant de rappeler et de réimprimer des documents copiés, il faut la redémarrer pour vider la mémoire dès que possible.

3.13 S'il est nécessaire de retirer des copies des informations BT des locaux d'un tiers :

- À moins que cela n'ait déjà été convenu dans le cadre de l'étendue des travaux, vous devez obtenir le consentement avéré de la partie prenante de BT.
- Si cela est approuvé, les informations ne doivent pas être identifiables pendant leur transit et doivent être conservées dans un dossier, un sac ou un étui anonyme ou ordinaire.
- Les documents ne doivent pas être laissé sans surveillance et doivent rester sous le contrôle direct de la personne qui les transporte, notamment dans les transports publics.

3.14 Lorsqu'elles ne sont plus nécessaires, les copies papier des informations BT doivent être éliminées comme suit :

- Les copies papier ne doivent pas être jetées dans les poubelles générales.
- Si vous utilisez un broyeur, il doit avoir une norme minimale de P4 DIN66399.
- Si des broyeurs agréés ne sont pas disponibles, les informations doivent être mises au rebut dans des poubelles pour déchets confidentiels.

Pour les « informations hautement confidentielles », les dispositions suivantes s'appliquent en outre.

- Les informations doivent être mises au rebut dans les poubelles confidentielles seulement après avoir été déchiquetées.
- Les informations qui doivent être déchiquetées sur place par le fournisseur doivent obtenir un certificat de destruction du fournisseur.

Les contrôles de sécurité suivants concernent les informations BT au format électronique.

3.15 Lorsque vous stockez des informations relatives à BT sur le PC ou l'ordinateur portable d'un tiers, les contrôles suivants s'appliquent :

- Le stockage est uniquement autorisé sur les appareils avec cryptage du disque dur, par exemple Bitlocker.
- Tous les documents doivent être cryptés individuellement.
- La gestion des droits de l'information (IRM) doit être appliquée au document.
- Si elles sont fournies, les informations doivent conserver l'étiquette de classification BT.

3.16 Lorsque vous enregistrez un document BT dans un emplacement de partage de fichiers interne à des fins de stockage général, de collaboration ou de partage de fichiers, les contrôles de sécurité suivants s'appliquent :

- Des autorisations d'accès doivent être implémentées à l'emplacement où les documents sont stockés afin de permettre uniquement aux personnes ayant besoin de voir ou d'utiliser les documents.
- Si elles sont fournies, les informations doivent conserver l'étiquette de classification BT.
- Tous les documents doivent être cryptés individuellement.
- La gestion des droits de l'information (IRM) doit être appliquée au document.
- Si cela fait partie du service fourni, les données relatives aux cartes PCI et aux cartes de paiement ne doivent à aucun moment être enregistrées sur des sites de stockage de fichiers.
- Si des comptes visiteurs sont nécessaires pour fournir un accès à un tiers ou à un entrepreneur externe, ils doivent avoir un contrat signé avec vous ou un accord de confidentialité doit être mis en place avant que l'accès ne soit accordé.

3.17 S'il est nécessaire d'enregistrer des informations relatives à BT sur un support amovible tiers, par exemple une clé USB, les contrôles de sécurité suivants s'appliquent :

- Le dispositif doit être crypté au même niveau que le disque dur.
- En cas de perte ou de vol, vous devez signaler un incident de sécurité.
- Vous devez avoir les preuves de l'approbation préalable de BT pour transférer des documents « hautement confidentiels » sur des supports amovibles.
- Dans le cadre du service, les documents PCI ou les données personnelles ne doivent pas être stockés sur des supports amovibles.
- Les dispositifs destinés au soutien et à la maintenance ne doivent pas être utilisés à d'autres fins.

3.18 Les informations relatives à BT ne doivent pas être stockées sur des PC personnels, des ordinateurs portables, des supports amovibles ou des appareils portables.

3.19 Les informations BT ne doivent pas être envoyées ou transférées automatiquement de votre adresse électronique d'entreprise à une adresse électronique personnelle ou à un compte de messagerie externe, à moins qu'il ne s'agisse d'un tiers ou d'un entrepreneur avec lequel vous avez signé un contrat ou un accord de confidentialité et qui est utilisé pour réaliser le service.

3.20 Pour minimiser la surface d'attaque et les possibilités pour les attaquants de manipuler le comportement humain par le biais de leur interaction avec les navigateurs internet et les systèmes de courrier électronique, mettez en place des processus pour vous assurer que seuls les navigateurs internet et les clients de courrier électronique entièrement pris en charge sont autorisés et désinstallez ou désactivez tous les plugins ou applications complémentaires de navigateur ou client de courrier électronique non autorisés.

3.21 Le tiers doit avoir mis en place des mesures de sauvegarde afin de restaurer les informations BT dans un délai de 3 jours ouvrables, en cas de corruption, perte ou dégradation.

3.22 Lors de l'élimination des données/informations de BT, des registres complets de la conservation et de l'élimination des données doivent être conservés, fournissant une piste d'audit, des preuves et un suivi. Elle doit notamment inclure :

- Une preuve de destruction et/ou d'élimination (y compris la date d'exécution et la méthode utilisée) ;
- Les journaux d'audit système de la suppression ;
- Les certificats d'élimination des données ;
- L'identité des personnes chargées de l'élimination (y compris les partenaires, tiers ou entrepreneurs de services d'élimination) ;
- Un rapport de destruction et de vérification doit être généré pour confirmer la réussite ou l'échec du processus de destruction ou de suppression (i.e. le processus d'écrasement doit fournir un rapport indiquant les secteurs qui n'ont pas pu être effacés, le cas échéant).

3.23 Lors de la mise au rebut d'équipements contenant des données/informations de BT, une piste d'audit doit être indiquée pour les types d'équipements suivants :

- Supports amovibles ;
- Lecteurs de disque ;
- Bandes de sauvegarde ;
- Composants d'ordinateur.
- Un registre détaillé doit pouvoir servir de piste d'audit et fournir les renseignements suivants, au minimum :
- Le nom de l'application ou du service qui utilisaient l'équipement concerné ;
- Le type d'équipement (ordinateur de bureau, ordinateur portable, serveur, bande, routeur, etc.) ;
- Le nombre de disques durs présents sur l'équipement (le cas échéant) ;
- L'équipement identifié par son numéro de série ;
- Les composants détachables de l'équipement identifiés par leur numéro de série ;
- Un suivi intégral des actifs relatifs à tous les équipements et composants détachables, d'un bout à l'autre du cycle d'élimination de l'équipement ;
- Une preuve de destruction et/ou d'élimination (y compris la date d'exécution et méthode utilisée) ;
- Les coordonnées des personnes chargées de l'élimination (y compris les partenaires, tiers ou entrepreneurs de services d'élimination) ;

- Un rapport de destruction et de vérification doit être généré pour confirmer la réussite ou l'échec du processus de recyclage/d'assainissement ou de destruction. Par exemple, le processus d'écrasement doit fournir un rapport indiquant les secteurs qui n'ont pas pu être effacés, le cas échéant. Ces rapports doivent notamment renseigner sur la capacité, la marque, le modèle et le numéro de série du support concerné.

Rôles et responsabilités

3.24 Les tiers doivent être conscients des exigences de ces contrôles de sécurité et les comprendre. Il leur incombe de veiller à ce que les personnes participant à la prestation d'un service destiné à BT, connaissent et respectent les exigences pertinentes de cette norme.

Gouvernance

3.25 Le tiers doit disposer d'une structure de sécurité aux normes du secteur établie et cohérente, applicable à la gouvernance de l'information et des mesures de cybersécurité, couvrant les composants suivants :

- Politiques et procédures liées aux informations et à la cybersécurité appropriées, approuvées et communiquées.
- Stratégie de sécurisation des informations.
- Exigences légales et réglementaires pertinentes liées à l'information et à la cybersécurité (confidentialité incluse), lesquelles doivent être comprises et gérées.
- Processus de gouvernance et de gestion du risque, traitant les risques liés à l'information et à la cybersécurité.

3.26 Le tiers doit veiller à ce que les rôles et responsabilités liés à l'information et à la cybersécurité soient définis et mis en œuvre. Il disposera notamment :

- À plein temps, d'un Chief Information Security Officer (Responsable de la sécurité) (ou équivalent) suffisamment haut placé dans la hiérarchie et responsable du programme de sécurité de l'information ;
- D'un groupe de travail de haut niveau, d'un comité ou d'un organisme équivalent chargés de coordonner l'ensemble de l'activité de sécurité de l'information du tiers, présidés par un membre du personnel suffisamment haut placé dans la hiérarchie et se réunissant régulièrement ;
- D'une fonction de sécurité de l'information spécialisée dont les rôles et responsabilités sont adaptés et définis.

3.27 Le tiers doit veiller à ce que chaque personne impliquée soit individuellement responsable de l'information et des systèmes, en veillant à l'appropriation qui convient des environnements critiques pour l'entreprise, de l'information et des systèmes et qu'ils soient affectés à des personnes compétentes.

3.28 Le tiers doit veiller à ce que BT soit informé (par écrit), dès que les considérations légales lui permettent de le faire, si le tiers fait l'objet d'une fusion, d'une acquisition ou d'un autre transfert de propriété quelconque.

Gestion des incidents

3.29 Le tiers doit disposer d'une structure de gestion des incidents établie et cohérente, servant à veiller à ce que les incidents soient efficacement gérés, maîtrisés, atténués et couvrant les composants suivants :

- Veiller à ce que les employés connaissent leur rôle et le déroulement des opérations lorsqu'une intervention s'avère nécessaire.
- Veiller à ce que les incidents signalés répondent aux critères établis.
- Veiller à ce que l'impact de l'incident soit compris.
- Veiller à ce que les procédures d'analyse soient suivies en cas de besoin, en interne ou en recourant à une fonction spécialisée.
- Veiller à ce que les enseignements tirés des incidents soient intégrés aux meilleures pratiques.
- Veiller à ce que l'information se rapportant à un incident impactant BT soit traité comme un événement « Confidential » (Confidentiel).

3.30 Le tiers prendra les mesures raisonnables pour veiller à ce que la ou les personnes qui conviennent soient nommées et à ce qu'elles assument la responsabilité de point de contact du risque de sécurité, de gestion des incidents et de la conformité. Le tiers communiquera à la partie prenante de BT les coordonnées de contact de la ou des personnes concernées et de tout changement en la matière, le cas échéant.

3.31 Le tiers informera BT de l'incident par courriel à security@bt.com ou par téléphone au +44 800 321 999, dans des délais raisonnables après avoir pris conscience d'un incident impactant le service dont il s'acquitte auprès de BT ou sur les informations de BT et quoi qu'il en soit, pas plus tard que vingt-quatre (24) heures après avoir pris connaissance de l'incident.

3.32 Le tiers, sans délai déraisonnable, prendra les mesures correctives qui s'imposent et au bon moment, pour atténuer les risques et effets liés à l'incident, afin d'en réduire la gravité et la durée.

3.33 Dans les 30 jours suivant un incident, le tiers fournira un rapport à la partie prenante de BT concernant tout incident ayant un impact sur le service de BT ou sur les informations de BT, incluant :

la date et l'heure, le lieu, le type d'incident, l'impact, le statut et le résultat (y compris les recommandations de résolution ou les mesures prises).

3.34 Le tiers doit effectuer une analyse des causes profondes de tous les incidents de sécurité. Les résultats de cette analyse doivent être transmis au niveau de gestion approprié au sein de votre organisation.

Gestion du changement

3.35 Il incombe au tiers de veiller à ce que les changements et modifications informatiques soient approuvés et éprouvés, abandon des échecs de modification incluses avant leur implémentation, pour éviter de perturber le service ou une violation de la sécurité et qu'un processus existe pour entreprendre, de manière contrôlée, les mises à jour d'urgence.

3.36 Le tiers doit veiller à ce que les changements et modifications soient reproduits dans les environnements de production et de reprise d'activité.

3.37 Le tiers doit veiller à ce que la maintenance et la réparation des actifs organisationnels soient exécutées et consignées en recourant aux outils approuvés et contrôlés.

3.38 Le tiers doit veiller à ce que la maintenance à distance des actifs organisationnels soit approuvée, consignée et exécutée selon une méthode empêchant les accès non-autorisés.

Gestion des cyber-risques et menaces

3.39 Le tiers doit veiller à l'existence d'une structure d'évaluation permanente du risque de cybersécurité et de la menace en la matière, pour faire en sorte que le profil de risque de cybersécurité lié aux opérations, actifs, locaux et effectifs de l'entreprise soit compris et géré :

- En évaluant les vulnérabilités des actifs.
- En identifiant les menaces internes et externes.
- Par la sensibilité des informations/données concernées.
- En évaluant les conséquences possibles pour l'entreprise.
- Les menaces, vulnérabilités, probabilités et impacts servent à déterminer le risque.
- En veillant à ce que la structure de gestion du cyber-risque et de la menace soit convenue au bon échelon de l'organisation.

3.40 Le tiers doit veiller à ce que tous les risques et menaces identifiés dans le cadre de l'évaluation du risque de cybersécurité et de la menace soient hiérarchisés et à ce que les mesures soient prises en conséquence, pour atténuer les risques dans les délais adéquats.

3.41 Le tiers doit avertir la partie prenante de BT s'il n'est pas en mesure de remédier ou de réduire les domaines de risque significatifs susceptibles d'impacter le service fourni.

Gestion des identités et contrôle des accès

3.42 Le tiers doit disposer d'une structure établie et cohérente, pour faire en sorte que les identités et informations d'identification soient gérées de manière sécurisée par le personnel autorisé :

- En n'accordant, ne réactivant, ne changeant et ne désactivant les droits d'accès que sur la base d'approbations documentées et autorisées.
- En veillant à ce que les comptes sans mouvement soient désactivés.
- En désactivant les comptes du personnel qui ont quitté l'entreprise.
- En mettant en œuvre des processus et des outils pour suivre, contrôler, prévenir et corriger l'utilisation, l'attribution et la configuration des privilèges administratifs sur les ordinateurs, les réseaux et les applications.
- En veillant à ce qu'une évaluation régulière des accès soit en place, pour vérifier l'aptitude à l'usage des accès.
- En veillant à ce que les accès aux comptes soient recertifiés au moins une fois par an, ou une fois par trimestre pour les comptes privilégiés.
- En veillant à ce que les informations d'identification et les secrets persistants (par exemple, pour l'accès par effraction) soient protégés par un stockage protégé par

du matériel et ne soient mis à la disposition de la ou des personnes responsables qu'en cas d'urgence.

3.43 Le stockage central des informations d'identification persistantes doit être protégé par des moyens matériels. Par exemple, sur un hôte physique, le lecteur pourrait être crypté à l'aide d'un module de plate-forme de confiance (TPM), tel que défini dans l'annexe A du Code de pratique pour la sécurité des télécommunications. Lorsqu'une machine virtuelle (MV) est utilisée pour la prestation d'un service de stockage central, cette MV et les données qu'elle contient doivent également être cryptées, utiliser un démarrage sécurisé et être configurées de manière à ce qu'elles ne puissent être démarrées que dans un environnement approprié. Le tiers doit veiller à ce que les accès à distance soient gérés de manière à ce que seules les personnes autorisées puissent se connecter à distance aux systèmes du tiers, à ce que les connexions soient sécurisées et protégées contre le risque de fuite de données et à ce que les contrôles des accès appropriés, comme l'authentification multi-facteur, aient été mis en place.

- L'authentification à deux facteurs doit dépendre d'un identifiant utilisateur, d'un mot de passe et d'une des méthodes suivantes :
- Générateur de mot de passe à usage unique, dont la consultation nécessite la saisie d'un code confidentiel (PIN) ou d'un mot de passe.
- Carte dotée d'une puce à la norme ISO 7816, lecteur de cartes et logiciel associés. Les cartes à puce sans contact ne sont pas autorisées.
- Authentification par certificat délivré conformément à votre politique de certification Infosec.

Pour éviter toute ambiguïté si l'accès au support s'effectue à distance, cet accès doit dépendre d'une connexion sécurisée et d'une authentification à deux facteurs.

3.44 Le tiers doit s'assurer que les permissions et autorisations d'accès, tous systèmes confondus (outils, applications, bases de données, systèmes d'exploitation, matériels, etc. inclus), sont gérées en incorporant les principes du privilège minimal et de la séparation des tâches.

3.45 Le tiers doit s'assurer que chaque transaction peut être attribuée à une personne unique et identifiable. S'il existe des justificatifs partagés, vérifiez qu'il existe des contrôles compensatoires appropriés (y compris des procédures de bris de glace). Le partage d'informations d'identification pour un accès privilégié n'est pas autorisé.

3.46 Le tiers doit veiller à ce que les authentifications soient gérées proportionnellement au risque associé à la transaction, notamment en appliquant la longueur et la complexité de mot de passe qui conviennent, par la fréquence des changements de mots de passe, l'authentification multi-facteur, la gestion sécurisée des informations d'identification de mot de passe ou d'autres contrôles. L'accès privilégié doit se faire via des comptes sécurisés par une authentification multifactorielle. Les comptes d'utilisateurs privilégiés « de type break-glass » doivent être dotés d'informations d'identification solides et uniques pour chaque point d'accès à l'équipement du réseau.

3.47 Les contrôles appropriés doivent avoir été mis en place pour traiter les échecs d'authentification, notamment par avertissement à l'écran, consignation des échecs et verrouillage de l'utilisateur.

3.48 Des processus et contrôles doivent avoir été mis en place pour gérer et autoriser les comptes invités et de service.

Classification et protection des données

3.49 Le tiers doit disposer d'un cadre/d'un programme de classification et de manipulation des informations établi et cohérent (aligné sur les bonnes pratiques de l'industrie et les exigences de BT), composé des composants suivants :

- Lignes directrices relatives à la manipulation des informations.
- L'information est protégée conformément à son niveau de classification.
- Veiller à ce que le personnel sache que la finalité des informations de BT se limite à l'usage pour lequel elles ont été fournies.

Prévention des fuites de données

3.50 Le tiers doit disposer d'une structure établie et cohérente pour veiller à la protection des données contre les fuites inappropriées. Cette protection doit inclure (entre autres, mais pas exclusivement), les vecteurs suivants :

- Courriel, Internet / Passerelle Web (y compris le stockage en ligne et le webmail), USB, optique et autres formes de ports / stockage portable, etc., informatique mobile et BYOD, services d'accès à distance, mécanismes de partage de fichiers et médias sociaux.
- Les périphériques non autorisés ne doivent pas être connectés au réseau (réseau professionnel du fournisseur ou systèmes/réseau de BT) ou utilisés pour accéder à des informations privées.

PCI DSS

3.51 S'il doit traiter les données de paiement par carte, le tiers doit vérifier sa conformité appropriée à la norme PCI-DSS. De plus, le tiers doit enregistrer les activités liées aux cartes de paiement auprès de l'équipe de gouvernance et d'assurance PCI par courriel à Group PCI Compliance group.pci.compliance@bt.com.

Gestion des vulnérabilités

3.52 Le tiers doit disposer d'une structure établie et cohérente de gestion des vulnérabilités, basée sur les composants suivants :

- Politiques et procédures de processus.
- Rôles et responsabilités définis.
- Outils appropriés, tels que les systèmes de détection d'intrusion et systèmes d'analyse des vulnérabilités.

3.53 La structure de gestion des vulnérabilités du tiers doit veiller à ce que les éléments suivants soient régulièrement surveillés, pour détecter les événements de cybersécurité potentiels :

- Principaux systèmes et actifs.
- Connexions non autorisées.
- Logiciels/applications non autorisées.
- Activité réseau.

3.54 La structure de gestion des vulnérabilités du tiers doit veiller :

- À ce que des processus soient établis pour recevoir, analyser et répondre aux vulnérabilités divulguées à l'organisation par des sources internes ou externes (ex. essais en interne, bulletins de sécurité ou experts en sécurité informatique).
- À ce que seuls les outils, technologies, utilisateurs autorisés soient permis.
- À ce que les vulnérabilités identifiées soient atténuées ou documentées comme risques acceptés.

Journalisation et surveillance continues

3.55 Le tiers doit veiller à disposer d'une structure établie et cohérente d'audit et de gestion des registres, visant à faire en sorte que les systèmes clés, applications incluses, soient configurés de manière à journaliser les événements clés (accès privilégiés et activité personnelle inclus), sachant que ces journaux doivent être conservés pendant 13 mois. Les journaux des équipements de réseau dans les fonctions critiques pour la sécurité doivent être entièrement enregistrés et mis à disposition pour un audit pendant 13 mois. Au minimum, le tiers doit veiller à ce que les journaux (au besoin) renseignent sur les événements suivants :

- Un audit établi et cohérent et des points de départ et d'arrêt du processus d'enregistrement.
- Changements applicables au type d'événements enregistrés, dictés par la piste d'audit (paramètres de démarrage et changements y afférents, par exemple).
- Démarrage et arrêt du système.
- Ouverture de session réussie.
- Tentatives d'ouverture de session échouées (erreur d'identifiant ou de mot de passe, par exemple).
- Création, modification et suppression sur/de comptes utilisateurs.
- À quel actif accédait-il (ex. données).
- D'où a-t-il accédé à l'actif (ex. adresse IP).
- Quand (ex. horodatage).

3.56 La structure d'audit et de gestion des journaux doit inclure les composants suivants :

- Les journaux d'événements clés sont examinés par une fonction indépendante au moins une fois par mois, pour détecter les activités non autorisées, les cibles et les types d'attaques.
- Les exceptions constatées font l'objet d'une enquête jusqu'à leur résolution.
- Veiller à ce que les journaux soient collectés et corrélés à partir de sources et détecteurs multiples, stockés de manière sécurisée et infalsifiables pour permettre la reconstruction de tels événements.
- Veiller à ce que l'impact des événements soit déterminé compte tenu de seuils d'alerte d'incident établis et déclenche une intervention opportune, basée sur la criticité de l'alarme.

4. Sécurité du personnel 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 en place en appliquant les processus officiels et notamment, les mesures disciplinaires qui s'imposent, susceptibles d'entraîner les interdictions suivantes pour l'individu :

- interdiction d'accès aux systèmes de BT et informations de BT ; ou
- interdiction d'exécuter des travaux se rapportant à la prestation du service.

En outre, le tiers vérifiera que des 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. Les informations pertinentes doivent être signalées à BT.

4.4 Quand un membre du personnel du tiers cesse d'être affecté à la prestation du service, les actifs physiques 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 ; ou détruits de manière sécurisée conformément aux contrôles de sécurité 3.22 et 3.23.

4.5 Le tiers doit disposer d'un cadre établi et cohérent sur l'utilisation acceptable des réseaux sociaux personnels et d'entreprise, en veillant à ce que le personnel :

- ne publie aucun contenu diffamatoire, obscène ou insultant à propos de l'organisation, de ses clients internes ou externes.
- n'utilise pas les logos des organisations ou des clients sans autorisation préalable.
- ne diffuse pas d'informations non publiques sur l'organisation ou le client sans autorisation préalable.
- ne publie pas d'avis sur l'organisation, ses clients internes ou externes, susceptibles d'être raisonnablement considérés comme des commentaires officiels formulés par l'organisation ou ses clients.
- Ne publie pas d'informations « Confidential » (Confidentiel) ou « Highly Confidential » (Strictement confidentiel) de BT.

4.6 Le tiers doit veiller à ce que chaque employé sous son contrôle, suive, dans le mois suivant son embauche, la formation obligatoire à la sécurité de l'information ; laquelle inclura les meilleures pratiques de cybersécurité et de protection des données à caractère personnel, avec une remise à niveau une fois par an, au minimum Cette formation concernant notamment les :

- utilisateurs privilégiés ;
- parties prenantes du tiers (c.-à-d. sous-traitants, clients, partenaires) ;
- cadres supérieurs ; et

- membres du personnel chargés de la sécurité physique et de la cybersécurité.

4.7 Le tiers doit veiller à ce qu'un test existe pour vérifier que l'utilisateur comprend la formation et la sensibilisation.

5. Audit et examen de la sécurité

5.1 Sans préjudice de tout autre droit d'audit que BT peut avoir, pour évaluer la conformité du tiers aux contrôles de sécurité de la présente politique sur les exigences de sécurité, le tiers fournira à BT, ou à ses représentants, l'accès et l'assistance nécessaires et appropriés pour permettre la réalisation d'examens de sécurité basés sur des documents, ou d'audits sur site. Le tiers sera informé de l'imminence d'un audit sur site au moins 30 jours ouvrés avant la date programmée.

L'audit aura pour finalité l'examen des divers aspects des règles, 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 verrait obligée d'exécuter un audit indépendant du tiers concluant qu'il ne respecte pas les principes et pratiques de la norme ISO/IEC 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 autoriser BT, sur demande raisonnable ou immédiatement à la suite d'un incident, à se livrer à l'inspection de l'environnement de contrôle dans lequel les services dont développés, fabriqués ou exécutés pour exécuter les essais de conformité du dispositif de sécurité et/ou les évaluations.

6.2 Le tiers est responsable des frais consécutifs au rattrapage, dans les délais convenus par les deux parties, des failles de sécurité éventuellement identifiées par BT.

6.3 En cas d'incident grave, le tiers s'engage à coopérer à 100% avec BT dans le cadre d'éventuelles enquêtes entreprises par BT, un organisme de réglementation et/ou une administration répressive, en autorisant l'accès et en contribuant en fonction des besoins et comme il convient pour enquêter sur l'incident. BT pourrait devoir demander que les actifs pertinents du tiers soit mis en quarantaine à des fins d'évaluation, et pour faciliter l'enquête, demande que le tiers s'engage à ne pas refuser ou entraver.

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 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 la certification ISMS du tiers par un service d'accréditation britannique (UKAS) ou un organisme de certification agréé international équivalent, dont le champ d'application et la déclaration d'applicabilité englobe la prestation des services sur les sites où ils seront effectués.

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 Si le champ d'application du certificat ou de la déclaration d'applicabilité sont modifiés pendant la durée du contrat dans la mesure où il ne couvre plus tous les services effectués aux endroits où ils sont fournis, le tiers doit en informer BT dans un délai raisonnable. Le tiers doit informer BT dans les 2 jours ouvrables de toute non-conformité majeure identifiée par l'organisme de certification ou le tiers, qui pose un risque pour la prestation des services.

8. Sécurité physique – locaux de BT

8.1 Le tiers doit se conformer à toutes les instructions pertinentes qui lui sont fournies en ce qui concerne l'accès aux locaux de BT et aux systèmes d'entrée des bâtiments. Les employés du tiers amenés à travailler dans les locaux de BT seront en possession d'une carte d'identification fournie par le tiers ou par BT, qu'ils devront positionner bien en vue, incluant une photo claire et ressemblant à l'employé du tiers titulaire de la carte.

8.2 BT peut également fournir au personnel du tiers une carte d'accès électronique et/ou une carte de visiteur à durée de validité limitée, à utiliser conformément aux consignes de délivrance locales

8.3 Le tiers est tenu d'informer BT dans les 24 heures lorsqu'un individu du tiers n'a plus besoin d'accéder aux bâtiments de BT et/ou aux systèmes d'entrée de BT.

8.4 Seuls les serveurs approuvés construits par BT, PC BT Webtop et Trusted End Devices (dispositif d'extrémité sécurisé) peuvent être directement reliés (par raccordement à un port LAN ou connexion sans fil) aux domaines de BT. Le tiers ne doit pas, sans autorisation écrite préalable fournie par BT, raccorder un équipement quelconque non approuvé par BT à un domaine de BT, quel qu'il soit.

8.5 La protection physique et les normes relatives au travail dans les locaux de BT doivent être respectées et doivent inclure, entre autres mais pas exclusivement, l'accompagnement des employés du tiers et l'adoption des pratiques de travail qui conviennent dans les zones sécurisées.

8.6 Dans les cas où le tiers est autorisé à fournir à son personnel un accès non accompagné à certaines zones des locaux de BT, le signataire autorisé du tiers et le personnel du tiers doivent respecter les termes du document d'orientation : Supplier access to BT' s sites - Mandatory security guide (Accès des fournisseurs aux sites de BT - guide de sécurité obligatoire) Vendre à BT.

9. Sécurité physique – locaux de tiers

9.1 Le tiers doit avoir mis en place un processus d'accès physique couvrant les méthodes et autorisations d'accès aux locaux (sites, bâtiments ou zones internes) où les services sont fournis ou servant au stockage ou au traitement des informations de BT. La méthode d'accès doit inclure au moins un des éléments ci-dessous :

- Carte d'identification autorisée par le tiers sur laquelle figure une photo claire et ressemblant au titulaire de la carte.
- Carte d'accès électronique autorisée, pour accéder aux zones applicables des locaux concernés.
- Accès par clavier de sécurité, lequel doit prendre en charge les processus : d'autorisation, de dissémination de changements de code (qui doit se produire au moins une fois par mois) et les changements de code ad hoc.
- Reconnaissance biométrique.

9.2 Le tiers doit avoir mis en place des processus et procédures de contrôle et de surveillance des visiteurs et autres personnes étrangères à l'entreprise, y compris celles du tiers, disposant d'un accès physique aux zones sécurisées ou à des fins de maintenance de contrôle de l'environnement, des alarmes et de nettoyage.

9.3 Les zones sécurisées des locaux du tiers servant à l'exécution du service (ex. salles de communication réseau), doivent être séparées des zones d'accès général et protégées par des contrôles d'entrée appropriés, visant à faire en sorte que seules les personnes autorisées puissent y entrer. Les accès à ces zones doivent faire l'objet d'un audit régulier ; une évaluation du renouvellement des droits d'accès à ces zones doit être entreprise au moins une fois par an.

9.4 Le tiers disposera d'un système de télésurveillance aux endroits servant au stockage et à la manipulation des informations de BT. Les enregistrements et enregistreurs doivent être placés en lieu sûr pour éviter toute modification, suppression ou la consultation « désinvolte » des écrans de télésurveillance associés. L'accès aux enregistrements doit être contrôlé et strictement limité aux personnes autorisées. Les enregistrements des caméras de télésurveillance doivent être conservés pendant au moins 20 jours.

9.5 Le tiers doit avoir pris les mesures qui conviennent pour assurer la sécurité physique des éléments suivants :

- Mesures de prévention des incendies et notamment, mais pas exclusivement, alarmes, matériel de détection et de prévention.
- Conditions climatiques, en tenant compte de la température, de l'humidité, de l'électricité statique et des mesures de gestion, de surveillance et de réponse associées aux conditions extrêmes (arrêt automatique, alarmes par exemple).
- Équipement de contrôle et notamment, mais pas exclusivement, climatisation et détection d'eau.
- Prévention des dégâts des eaux, repérage des réservoirs, canalisations d'eau, etc. dans les locaux.

9.6 Le tiers doit s'assurer que l'accès physique aux zones d'hébergement des informations de BT nécessite le recours à une carte à puce ou de proximité (ou à un système de sécurité équivalent ou plus poussé) et doit entreprendre des contrôles mensuels pour veiller à ce que seules les personnes autorisées ne disposent de cet accès.

9.7 Le tiers doit veiller à ce que la photographie et/ou la capture d'image des informations de BT soient interdites. Si une raison commerciale oblige à pratiquer la capture d'images pour les enregistrer, l'autorisation de le faire doit être confirmée par écrit par BT.

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

10.1 Le tiers doit, dans les cas où il prévoit dans ses locaux, une zone d'accès sécurisée destinée à l'hébergement des équipements de BT ou des clients de BT :

- Fournir à BT un schéma d'implantation de l'espace fonctionnel prévu dans la zone sécurisée des locaux.
- Veiller à ce que les armoires prévues pour BT et les clients de BT dans les locaux soient constamment verrouillées et uniquement ouvertes par le personnel autorisé de BT, les représentants agréés de BT et le personnel habilité du tiers.
- Mettre en œuvre un processus sécurisé de gestion des clés.

10.2 BT fournira au tiers :

- La liste des actifs physiques de BT et/ou du client de BT détenus dans les locaux du tiers.
- Les détails des employés, sous-traitants et agents de BT devant accéder aux locaux du tiers (de façon permanente).

11. Développement de logiciels sécurisé

11.1 Le tiers doit s'assurer que les environnements de production et de non-production sont suffisamment contrôlés, en veillant à ce que les composants suivants soient en place :

- Ségrégation des environnements de production, de non-production et des tâches.
- Aucune donnée en temps réel n'est utilisée pour les essais, sans l'accord préalable des propriétaires des données et contrôles proportionnels à l'environnement de production.
- Ségrégation des tâches de développement de production et de non-production.

11.2 Le tiers doit disposer d'une structure établie et cohérente de développement, pour éviter les vulnérabilités de sécurité et violations de la cybersécurité, basée sur les aspects suivants :

- Les systèmes sont développés en adéquation avec les meilleures pratiques de développement sécurisé (ex. , OWASP).
- Le code est stocké de manière sécurisée et soumis à l'assurance qualité.
- Le code est suffisamment protégé contre toute modification non autorisée après validation des essais et livraison en production.

12. Escrow

12.1 Dans les cas où l'entiercement s'impose pour protéger les parties (pour l'entiercement de première partie ou de tierce partie) (ex. pour la propriété intellectuelle/le code source, etc.), le tiers doit disposer d'une structure établie et cohérente basée sur les éléments suivants :

- Exécution de l'entente d'entiercement auprès d'un agent indépendant, neutre et de bonne réputation.
- Mise à disposition et mises à jour suivies du code source et d'autres supports auprès de l'agent d'entiercement, pour garantir l'actualisation des informations.
- Stockage sécurisé du code source et des autres supports, jusqu'à ce que les conditions de publication soient remplies.
- Conditions de publication appropriées.
- Mises à jour, paiements et révisions appropriés de l'entente d'entiercement en continu.

13. Accès aux systèmes de BT

13.1 Le tiers respectera toutes les consignes qui lui auront été fournies en matière d'accès et d'utilisation des systèmes de BT.

13.2 Le tiers est responsable d'informer BT dans les 24 heures lorsqu'un individu du tiers n'a plus besoin d'accès.

13.3 Le tiers veillera à ce que l'identifiant utilisateur, les mots de passe, codes confidentiels (PIN), jetons et accès aux conférences soient octroyés individuellement à son personnel et que ce dernier ne les partage pas. Les détails doivent être stockés de manière sécurisée et séparément du périphérique utilisé à des fins d'accès. Si une autre personne connaît le mot de passe, il doit être changé immédiatement.

Connectivité entre systèmes

13.4 La liaison inter-domaines aux systèmes de BT est interdite, sauf après approbation et autorisation spécifiques de BT.

13.5 Le tiers doit recourir à tous les moyens raisonnables pour veiller à ce qu'aucun virus ou code malveillant (expressions généralement comprises dans le secteur de l'informatique) ne soit introduit dans les systèmes de BT.

13.6 En cas de connectivité entre les systèmes du tiers et de BT, la connectivité sera assurée par des liaisons sécurisées, les données étant protégées par un cryptage conforme aux contrôles cryptographiques des articles 14.9, 14.10, 14.11, 14.12 et 14.13.

13.7 Le tiers veillera à ce que les systèmes et l'infrastructure utilisés 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.

14. Systèmes tiers détenant des informations de BT

14.1 Le tiers doit veiller à ce que les versions les plus récentes des correctifs de sécurité soient appliqués aux systèmes/actifs/applications réseau au bon moment et :

- À utiliser des correctifs obtenus auprès de : fournisseurs directement pour les systèmes propriétaires et correctifs (i) signés numériquement ou (ii) vérifiés en recourant à un hash fournisseur (les hash MD5 ne doivent pas être utilisés) pour la mise à jour, de manière à ce que le correctif puisse être identifié comme provenant d'une communauté de support de logiciels open - source de bonne réputation.
- À soumettre les correctifs à des essais sur les systèmes représentant exactement la configuration des systèmes de production ciblés, avant déploiement du correctif aux systèmes de production et à ce que l'utilisation correcte du service corrigé soit vérifiée après une activité de correction quelconque.
- À surveiller les fournisseurs concernés et autres sources d'informations pertinentes par rapport aux alertes de vulnérabilité.
- Si un système ne peut pas être corrigé, les contre-mesures qui s'imposent doivent être déployées.
- Le tiers fournira les correctifs de sécurité critiques séparément des versions de fonctionnalités afin de maximiser la vitesse à laquelle le correctif peut être déployé.

14.2 Le tiers doit veiller à ce qu'au moins une fois par an, une évaluation indépendante de la sécurité des technologies de l'information ou un test d'intrusion soit commandé pour tester l'infrastructure et les applications du tiers utilisés dans le cadre de la prestation des services, sites de reprise de l'activité inclus, pour identifier les vulnérabilités susceptibles d'être exploitées pour compromettre les données/services et éviter toute violation de sécurité par cyberattaque. Le tiers doit, consécutivement à une demande raisonnable de BT, autoriser cette dernière à accéder aux rapports des tests d'intrusion se rapportant aux services dont il s'acquitte auprès de BT.

14.3 Le tiers doit veiller à la sécurisation des accès aux ports de diagnostic et de gestion, au même titre qu'aux outils de diagnostic.

14.4 Le tiers doit veiller à ce que l'accès aux outils de vérification soit limité au personnel du fournisseur qui convient et à ce que leur utilisation soit surveillée.

14.5 Le tiers doit veiller à ce que les serveurs utilisés dans le cadre de la prestation du service ne soient pas déployés sur des réseaux non autorisés (réseau en dehors de votre périmètre de sécurité, au-delà des limites de votre sphère de contrôle administratif, ex. accès via Internet) sans les contrôles de sécurité qui s'imposent.

Gestion des actifs

14.6 Le tiers doit tenir un inventaire précis et à jour de tous les actifs technologiques susceptibles de stocker ou de traiter des informations, afin que seuls les dispositifs autorisés puissent y accéder et que les dispositifs non autorisés et non gérés soient repérés et empêchés d'y accéder. Cet inventaire doit inclure tous les actifs matériels, qu'ils soient connectés ou non au réseau de l'organisation. Le cas échéant, tout équipement BT hébergé dans des locaux de tiers doit être inclus dans l'inventaire.

14.7 Le tiers doit faire en sorte que l'inventaire des actifs informatiques prévoit l'inventaire ou le catalogage des composants suivants :

- Dispositifs et systèmes physiques, plateformes et applications logicielles, systèmes d'information externes.
- Ressources (ex. matériel, périphériques, données, temps et logiciels) hiérarchisées sur la base de leur classification, de leur criticité et de leur valeur pour l'entreprise.
- Flux de données organisationnelles et de communication, dont les flux de données externes/de tiers.
- Processus manuels servant à manipuler les données de BT ou de ses clients.

14.8 Le tiers doit maintenir un inventaire précis et à jour des actifs logiciels pour tous les logiciels sur le réseau afin que seuls les logiciels autorisés soient installés et puissent s'exécuter, et que les logiciels non autorisés et non gérés soient trouvés et empêchés d'être installés ou exécutés.

Cryptographie

14.9 Le tiers doit s'assurer que les informations de BT classées comme confidentielles ou strictement confidentielles sont cryptées de manière appropriée (en transit et en attente) et que tout cryptage est effectué à l'aide d'algorithmes cryptographiques et de chiffrement puissants et modernes utilisant des mécanismes de protection de l'intégrité robustes et conformes aux normes industrielles pour la négociation et la gestion sécurisées des clés et des protocoles. Pour les données en transit, les options TLS suivantes ne sont pas autorisées : TLS v1.0, TLS v1.1,et SSL (toutes versions). Le SSH suivant (SFTP) les options ne sont pas autorisées : SSH V1. Les options IPSEC suivantes ne sont pas autorisées : IK Version 1.

14.10 La longueur des clés de chiffrement doit correspondre voire dépasser les longueurs minimales suivantes :

- Les clés symétriques (ex. , AES) doivent être longues d'au moins 256 bits.
- Les clés asymétriques (ex. , RSA) doivent être longues d'au moins 2048 bits.
- Les clés à courbe elliptique doivent être longues d'au moins 224 bits.

14.11 Si NIST annonce qu'un algorithme de chiffrement n'est plus sûr, il ne doit pas être utilisé dans le cadre de nouveaux déploiements. Les déploiements existants doivent évaluer l'utilisation continue d'algorithmes de chiffrement obsolètes et fournir un plan d'atténuation visant à abandonner les algorithmes de chiffrement obsolètes au profit d'une solution plus sûre.

14.12 S'agissant du chiffrement symétrique, les algorithmes suivants sont interdits : 3DES-168 (à moins d'avoir été mandaté par une norme internationale), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed et ARIA.

14.13 Les hachages salés doivent être utilisés pour protéger les données stockées, par exemple les mots de passe. Le hachage peut aussi servir pour anonymiser les données avant traitement, MSISDN ou paiement, par exemple. Les algorithmes de hachage suivants ne sont pas autorisés MD2, MD4, MD5 et SHA-1.

Configuration système

14.14 Le tiers doit disposer d'un cadre établi et cohérent pour garantir que les systèmes sont configurés de manière appropriée, y compris les éléments suivants :

- Les systèmes, périphériques réseau sont configurés pour fonctionner conformément aux principes de sécurité (c.-à-d. au concept de la moindre fonctionnalité et aucun logiciel non autorisé).
- Veiller à ce que l'horloge des périphériques soit cohérente et à l'heure.
- Veiller à ce que les systèmes soient exempts de logiciels malveillants.
- Veiller à ce que les contrôles et la surveillance appropriés soient en place, pour préserver l'intégrité des versions/périphériques.

Protection contre les logiciels malveillants.

14.15 Le tiers doit veiller à ce que la protection anti-programme malveillant la plus à jour soit appliquée à tous les actifs informatiques concernés, pour éviter la perturbation du service ou une violation de la sécurité, et faire en sorte que les procédures de sensibilisation des utilisateurs soient mises en place.

NB. La protection anti-programme malveillant devra inclure (entre autres, mais pas exclusivement) la détection des codes mobiles non autorisés, virus, logiciels espions, logiciels enregistreurs de frappe, botnets, vers, chevaux de Troie, etc.

Atténuations du déni de service.

14.16 Le tiers doit veiller à ce que les systèmes de clé soient protégés contre les attaques par déni de service (DoS) et déni de service distribué (DDoS).

15. Tiers hébergeant des informations de BT

15.1 En plus des contrôles de la section 14. Systèmes tiers détenant des informations de BT, lorsque le tiers héberge les informations de BT dans un centre de données ou une solution infonuagique, les locaux doivent détenir un certificat ISO/IEC 27001 valide pour la gestion de la sécurité (ou une ou plusieurs certifications démontrant des contrôles équivalents, soutenus par un rapport d'audit indépendant).

16. Sécurité du réseau – réseau appartenant à BT.

Lorsque des tiers installent des équipements, configurent, entretiennent, gèrent, réparent ou surveillent le réseau de BT, les contrôles suivants s'appliquent :

16.1 Sur demande, le tiers doit fournir à BT les noms, adresses et autres détails que BT peut raisonnablement exiger de tous les membres individuels du personnel du tiers qui :

- seront de temps à autre directement impliqués dans le déploiement, la maintenance et/ou la gestion du ou des services avant leur engagement respectif.
- assureront la liaison avec BT en ce qui concerne les discussions sur les vulnérabilités identifiées par BT et/ou par des tiers dans le(s) service(s).

16.2 S'il s'agit de ses activités de support au Royaume-Uni, le tiers maintiendra une équipe de sécurité qualifiée composée d'au moins un ressortissant du R.-U., disponible pour se charger de la liaison avec l'équipe devant assister aux réunions ponctuelles éventuellement programmées par BT, à la demande raisonnable de ce dernier.

16.3 Le tiers doit fournir à BT un calendrier (mis à jour si nécessaire de temps à autre) de tous les composants actifs compris dans le(s) service(s) et leurs sources respectives.

16.4 Le tiers doit fournir à BT des informations opportunes (c'est-à-dire dès que possible pour permettre la correction avant la publication) concernant les vulnérabilités du ou des services et se conformer (aux frais du tiers) aux exigences raisonnables concernant les vulnérabilités qui peuvent être notifiées par BT.

16.5 Le tiers veillera à ce que les composants de sécurité compris dans le service, tels qu'identifiés par BT ou signalés à BT à l'occasion soient, aux frais du tiers, évalués indépendamment à la satisfaction raisonnable de BT.

16.6 Le tiers fournira à BT rapidement et quoi qu'il en soit pas plus tard que dans les sept jours ouvrés, une explication complète des caractéristiques et/ou fonctionnalités des services (ou ajoutées à la feuille de route des services) qui sont périodiquement :

- Portées à la connaissance du tiers ; ou
- Que BT croit raisonnablement qu'elles ont été conçues pour pouvoir être utilisées à des fins d'interception légale ou de toute autre forme d'interception du trafic des télécommunications. Ces détails devront inclure les informations raisonnablement nécessaires pour permettre à BT de comprendre parfaitement la nature, la composition et l'importance de ces caractéristiques et/ou fonctionnalités.

16.7 Le tiers ne doit utiliser aucun outil de surveillance du réseau capable de lire les informations des applications.

16.8 Le personnel du tiers qui construit, développe et/ou soutient le réseau de BT doit subir au minimum un contrôle de pré-embauche L2. Des vérifications préalables à l'emploi L3 seront requises pour les rôles identifiés par BT.

16.9 Le tiers doit permettre à BT d'installer un logiciel de sécurité conforme aux spécifications de BT, sur toute infrastructure virtuelle du tiers (y compris, mais sans s'y limiter, les machines virtuelles et les conteneurs) ou sur tout système d'exploitation installé par le tiers et fonctionnant sur les réseaux de BT.

Loi sur les télécommunications (sécurité) 2021 (TSA)

Lorsque le service tiers relève du champ d'application de la loi sur les télécommunications (sécurité) de 2021 (TSA), les contrôles de sécurité suivants s'appliquent.

16.10 Lorsque le tiers supporte plus d'un opérateur, des contrôles doivent être mis en place pour empêcher un opérateur ou son réseau de nuire à un autre opérateur ou à son réseau.

16.11 Lorsque le tiers fournit une fonction administrative pour plus d'un opérateur, les contrôles suivants s'appliquent :

- Mettre en œuvre une séparation logique au sein du réseau tiers pour séparer les données et les réseaux des clients.
- Mettre en œuvre la séparation entre les environnements de gestion tiers utilisés pour les différents réseaux d'opérateurs.
- Mettre en œuvre et appliquer des fonctions de renforcement de la sécurité à la frontière entre le réseau du tiers et le réseau de l'opérateur.

- Mettre en place des contrôles techniques pour limiter le potentiel des utilisateurs ou des systèmes à avoir un impact négatif sur plus d'un opérateur.
- Mettre en place des postes de travail à accès privilégié logiquement indépendants par opérateur.
- Mettre en place des domaines et des comptes administratifs indépendants par opérateur.

16.12 Lorsqu'ils fournissent des équipements de réseau, les tiers doivent fournir une déclaration de sécurité à BT sur la manière dont l'équipement est produit et dont la sécurité de l'équipement est assurée tout au long de sa durée de vie. Cette déclaration de sécurité doit couvrir les exigences de l'évaluation de la sécurité du fournisseur publiée à l'annexe B du code de pratique de la sécurité des télécommunications.

16.13 Lorsque le tiers fournit des équipements de réseau, les contrôles suivants sont applicables :

- Le tiers garantit qu'il adhérera à une norme qui ne sera pas inférieure à la « déclaration de sécurité » qu'il a publiée.
- Le tiers fournira des conseils actualisés sur la façon dont l'équipement doit être déployé en toute sécurité.
- Le tiers assurera le soutien de tous les équipements et de tous les sous-composants logiciels et matériels pendant la durée du contrat.
- Le tiers fournira des détails pour tous les principaux composants tiers et dépendances, y compris, mais sans s'y limiter, le produit et la version, les composants open-source et le niveau de soutien et la période.
- Le tiers remédiera à tous les problèmes de sécurité qui posent un risque de sécurité pour le réseau ou le service d'un fournisseur et qui sont découverts dans leurs produits dans un délai raisonnable après avoir été notifiés, en fournissant des mises à jour régulières sur les progrès réalisés en attendant - ce délai doit être convenu entre BT et le tiers agissant tous deux raisonnablement. Cela inclut tous les produits touchés par la vulnérabilité, et pas seulement le produit pour lequel la vulnérabilité a été signalée.

16.14 Si le tiers a obtenu des évaluations ou des certifications de sécurité internationalement reconnues pour les équipements (par exemple, Critères communs ou NESAS), cela doit être publié publiquement, y compris les conclusions complètes qui attestent de cette évaluation ou de ce certificat.

16.15 Lorsque le réseau d'un tiers est susceptible d'avoir un impact sur les réseaux de BT, le tiers devra, selon les conseils de BT, subir le même niveau de test que BT applique aux réseaux de BT et remédier aux vulnérabilités identifiées, comme convenu entre les deux parties.

16.16 Le tiers autorise BT à partager les détails des problèmes de sécurité, le cas échéant, lorsque cela est nécessaire aux fins de la sécurité du réseau.

16.17 L'infrastructure et les systèmes utilisés pour entretenir les réseaux de BT doivent être situés au Royaume-Uni.

16.18 Lorsque le tiers effectue les fonctions de surveillance du réseau de BT, l'équipement utilisé pour cette fonction doit être situé au Royaume-Uni et exploité par du personnel basé au Royaume-Uni.

16.19 Lorsque le tiers est responsable de la sécurité du réseau et des journaux d'audit, ceux-ci sont stockés au Royaume-Uni et protégés conformément à la législation britannique.

17. Sécurité de réseau tiers

17.1 Le tiers doit veiller à ce que l'intégrité du réseau soit établie et préservée, en s'assurant que les composants suivants sont soumis aux contrôles appropriés :

- Les connexions externes au réseau sont documentées, acheminées à travers un pare-feu, vérifiées et approuvées avant d'être établies, pour éviter toute violation de la sécurité des données.
- Le réseau est conçu sur la base des principes de « défense en profondeur », pour faire en sorte que les violations de cybersécurité soient limitées au maximum, en recourant aux contrôles qui conviennent d'empêcher l'occurrence d'une attaque, notamment du type « segmentation réseau ».
- L'étude et l'implémentation du réseau font l'objet d'une évaluation annuelle, au minimum.
- Tout accès sans fil au réseau dépend de protocoles d'autorisation, d'authentification, de segmentation et de chiffrement visant à éviter les violations de la sécurité.
- En recourant aux communications sécurisées entre les périphériques et les stations de gestion.
- En recourant aux communications sécurisées entre les périphériques selon les besoins, incluant le chiffrement des accès d'administrateur autres que ceux de la console.
- En recourant à un modèle d'architecture robuste, hiérarchisé et segmenté, associé à une configuration efficace de gestion des identités et de système d'exploitation, laquelle doit être correctement renforcée et documentée.
- En désactivant (dans la mesure du pratique) les services, applications et ports qui ne seront pas utilisés.
- En désactivant ou supprimant les comptes invités.
- En évitant les relations d'approbation entre les serveurs.
- En recourant au meilleur principe de sécurité du « moindre privilège » pour exécuter une fonction.
- En veillant à ce que les mesures appropriées soient en place pour détecter et/ou protéger contre les intrusions.
- S'il y a lieu, consigner la surveillance de l'intégrité pour détecter d'éventuels ajouts, modifications ou suppressions de fichiers ou données systèmes critiques.
- En changeant les mots de passe par défaut ou fournis par le fournisseur, avant le lancement des composants réseau.

17.2 Lorsque le tiers fournit des services qui sont soumis à la loi sur les télécommunications (sécurité) de 2021, les contrôles de sécurité supplémentaires suivants s'appliquent :

- Les systèmes tournés vers l'extérieur, à l'exception des équipements de locaux des clients (CPE), sont soumis à des tests de sécurité tous les deux ans ou en cas de changement important.
- Les ensembles de données sensibles et les fonctions sensibles ou critiques ne sont pas hébergés sur des équipements situés à la périphérie exposée du réseau.
- S'il n'y a pas de protection cryptographique, une séparation physique et logique doit être mise en place entre la bordure exposée (« Exposed Edge ») et les fonctions sensibles ou critiques.
- Une séparation de sécurité utilisant des fonctions d'application de la sécurité doit être mise en œuvre entre la bordure exposée et les fonctions sensibles ou critiques.

17.3 Le réseau tiers devra être conforme aux exigences légales, réglementaires et :

- Être équipé au mieux pour empêcher les personnes non-autorisées (ex. pirates) d'accéder au(x) réseau(x) du tiers.
- Être équipé au mieux pour réduire le risque d'utilisation abusive du ou des réseaux du tiers par les personnes autorisées à y accéder.
- Être équipé au mieux pour détecter une éventuelle violation de la sécurité et faire en sorte que les violations soient rapidement rectifiées, tout en identifiant les individus qui ont pu y accéder et comment ils y sont parvenus.

18. Sécurité dans le Cloud

18.1 Le tiers doit être certifié à la version la plus récente de la norme ISO27017 ou disposer d'une structure établie et cohérente pour veiller à ce que toute utilisation de la technologie Cloud et de données privées stockées dans le Cloud soit approuvée et soumise aux contrôles appropriés, équivalents à la version la plus récente de la matrice de contrôle Cloud Controls Matrix (CCM) de Cloud Security Alliance.

18.2 Les contrats de niveau de service réseau et d'infrastructure (en interne ou externalisés) devront clairement documenter les contrôles de sécurité, la capacité, les niveaux de service ainsi que les exigences de l'entreprise et des clients.

18.3 Le tiers doit mettre en œuvre des mesures de sécurité portant sur tous les aspects de ses prestations, afin de protéger la confidentialité, la disponibilité, la qualité et l'intégrité ; en limitant au maximum le risque que des personnes non autorisées (ex. autres clients du Cloud) puissent accéder aux informations de BT et aux services utilisés par cette dernière.

18.4 Dans la mesure où le tiers fournit des applications ou des services hébergés à BT, qu'ils soient à locataire unique ou à locataires multiples, y compris des logiciels en tant que service, des plates-formes en tant que service, des infrastructures en tant que service et des offres similaires, pour collecter, transmettre, stocker ou traiter des données confidentielles, le tiers doit fournir à BT la capacité :

- d'isoler logiquement ces données confidentielles des données des autres clients du tiers.
- de restreindre, enregistrer et surveiller l'accès à ces données confidentielles à tout moment, y compris l'accès par le personnel d'un tiers.

- à créer, activer, désactiver et supprimer la clé de chiffrement la plus élevée (appelée clé gérée par le client) utilisée pour chiffrer et déchiffrer les clés suivantes, y compris la clé de chiffrement des données la plus basse.
- de restreindre, d'enregistrer et de surveiller l'accès à la clé gérée par le client à tout moment ; et à aucun moment une clé de chiffrement ultérieure, une clé de chiffrement dans une hiérarchie de clés inférieure à celle de la clé gérée par le client, ne doit être stockée dans le même système que les données confidentielles, à moins qu'elles ne soient chiffrées par la clé gérée par le client, également connue comme étant enveloppée par la clé gérée par le client.

19. Services de téléphonie mobile

19.1 Lorsque le tiers fournit des cartes SIM, les contrôles suivants sont applicables :

- Pour les cartes SIM à profil fixe, le tiers doit s'assurer que les données SIM sensibles sont protégées de manière appropriée par le fabricant de la carte SIM.
- Pour les cartes SIM à profil fixe, le tiers doit s'assurer que la confidentialité, l'intégrité et la disponibilité des données sensibles de la carte SIM partagées avec le fabricant de la carte SIM sont protégées à chaque étape de leur cycle de vie.

20. Information classée dans la catégorie OFFICIAL (Officiel) ou dans une catégorie supérieure par HMG (/His Majesty's Government).

20.1 Lorsque le fournisseur est tenu d'accéder, de stocker, de traiter ou de transmettre des informations classifiées HMG OFFICIAL ou supérieures, le fournisseur doit effectuer une évaluation des risques liés à la sécurité du personnel pour tous les rôles identifiés dans la déclaration officielle sensible, paragraphe 2, conformément aux exigences définies dans le document CPNI National Security Clearance - A guide (Habilitation de sécurité nationale CPNI - Un guide, 4e édition - juin 2013 ou ultérieure).

20.2 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 HMG et aux mises à jour ponctuelles y afférentes.

20.3 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 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 »** et **« Accédé »** 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.

« Partie prenante de BT » ou **« BT »** désigne le représentant de BT qui est propriétaire de l'étendue du travail que vous entreprenez.

« **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.

« Réseaux de BT » désigne tout réseau public de communications électroniques exploité par BT, tel que défini par la section 32 de la loi de 2003 sur les communications.

« BYOD » signifie "apportez votre propre appareil".

« **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.

« **Équipement des locaux des clients** » désigne l'équipement fourni aux clients par le fournisseur, et géré par le fournisseur, qui est utilisé, ou destiné à être utilisé, dans le cadre du réseau ou du service. Cela exclut les appareils électroniques grand public tels que les téléphones mobiles et les tablettes, mais inclut des appareils tels que les pares-feux de périphérie, les équipements SD-WAN et les kits d'accès sans fil fixes.

« **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.

La **« cybersécurité »** est la manière dont les individus et les organisations réduisent le risque de cyber-attaque. La fonction essentielle de la cybersécurité est de protéger les appareils que nous utilisons tous (smartphones, ordinateurs portables, tablettes et ordinateurs), ainsi que les services auxquels nous accédons - en ligne et au travail - contre le vol ou les dommages.

« **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).

« Bordure exposée » Équipement qui se trouve soit dans les locaux du client, soit directement accessible à partir de l'équipement du client/de l'utilisateur, soit physiquement vulnérable. Les équipements physiquement vulnérables comprennent les équipements situés dans des armoires en bordure de route ou fixés au mobilier urbain. La périphérie exposée comprend les CPE, les équipements de station de base, les équipements OLT et les équipements MSAN/DSLAM.

« **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.

« **NDA** » signifie qu'un accord de non-divulgation est un contrat contraignant entre deux ou plusieurs parties qui empêche le partage d'informations sensibles avec d'autres.

« **Bien de réseau** » désigne un article faisant partie d'un ensemble de composants interconnectés tels que des ordinateurs, des routeurs, des concentrateurs, du câblage et des contrôleurs de télécommunications qui constituent un réseau.

« **Fonction de surveillance du réseau** » désigne les composants du réseau de BT qui supervisent et contrôlent les fonctions critiques de sécurité, ce qui leur confère une importance vitale dans la sécurité globale du réseau. Ils sont essentiels pour que BT puisse comprendre le réseau, le sécuriser ou le récupérer.

« **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.

« **NIST** » signifie l'Institut national des normes et de la technologie - une unité du ministère du Commerce des États-Unis. Anciennement connu sous le nom de National Bureau of Standards, le NIST assure la promotion et la maintenance des instruments de mesure. Il dispose également de programmes actifs pour encourager et aider l'industrie et la science à développer et à utiliser ces normes.

« **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.

Par « **poste de travail à accès privilégié (PAW)** », on entend les postes de travail par lesquels un accès privilégié est possible.

« Fonction critique pour la sécurité » désigne toute fonction du réseau ou du service de BT dont le fonctionnement est susceptible d'avoir un impact important sur le bon fonctionnement de l'ensemble du réseau ou du service ou d'une partie importante de celui-ci.

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

« **SIM** » : composant matériel ou jeton unique, et logiciel associé, utilisé pour authentifier l'accès de l'abonné au réseau. Dans le cadre du présent document, la carte SIM englobe le matériel UICC/eUICC, les applications SIM/USIM/ISIM, la fonctionnalité eSIM et RSP et toute applet SIM.

« **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.

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

« Transaction » désigne les données/informations transactionnelles qui sont capturées à partir des transactions, c'est-à-dire les données générées par diverses applications lors de l'exécution ou de la prise en charge des processus commerciaux quotidiens.

« **Tiers** » désigne un fournisseur de BT.

« **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.

« Réseau tiers » désigne tout réseau du Fournisseur.

« **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.

Version	Description	Auteur :	Date
4.0	Nouveau	Karen Tanner	02/02/2020
4.1	Clause supplémentaire pour l'ensemble des clauses HMG 20	Karen Tanner	20/02/2020
5.0	Loi sur les télécommunications (sécurité) de 2021 (TSA) et adoption du CIS par BT	Jemma Turner	25/10/2022

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 du tiers occupant un poste répertorié dans la déclaration officiel sensible :

1.2.1. Doit, au moins, être au soumis à un contrôle de pré-emploi 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 des 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 His 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.

22. 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 HMG (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.

23. ANNEXE 2, Loi sur les télécommunications (sécurité) 2021 - Code de pratique pour la conversion des exigences de sécurité

Code de pratique Réf.	Clause de sécurité BT Ref
M21.04 Lorsque les données sont stockées à l'étranger, le prestataire doit tenir une liste des lieux où les données sont conservées. Le risque lié à la conservation des données dans ces lieux, y compris tout risque lié à la législation locale sur la protection des données, est géré dans le cadre des processus de gestion des risques du prestataire.	3.8
M10.46 Les prestataires doivent s'assurer que leurs contrats autorisent le partage des détails des problèmes de sécurité, le cas échéant, afin de soutenir l'identification et la réduction des risques d'atteinte à la sécurité du réseau public de communications électroniques ou du service public de communications électroniques, suite à des actions ou omissions de fournisseurs tiers.	3.31
M10.13 Les prestataires doivent exiger contractuellement des prestataires tiers qu'ils trouvent et rapportent la cause profonde de tout incident de sécurité susceptible d'entraîner une compromission de la sécurité au Royaume-Uni dans un délai de 30 jours, et qu'ils rectifient toutes les faiblesses constatées.	3.33
M5.05 Outre des exigences du CAF D.2, les prestataires doivent effectuer une analyse des causes profondes de tous les incidents de sécurité. Les résultats de cette analyse doivent être transmis à un niveau approprié, qui peut inclure le conseil d'administration du prestataire.	3.34
M11.02 Tous les justificatifs et secrets persistants doivent être protégés et ne doivent être accessibles à personne, sauf à la ou aux personnes responsables en cas d'urgence.	3.42
M6.02 L'accès privilégié se fait par l'intermédiaire de comptes dotés d'un identifiant d'utilisateur unique et d'informations d'authentification pour chaque utilisateur, qui ne doivent pas être partagés.	3.45
M6.04 Tous les comptes d'utilisateurs privilégiés de type « break-glass » doivent avoir des informations d'identification uniques et solides par équipement de réseau.	3.46
M10.24 Les prestataires doivent exiger contractuellement que les administrateurs tiers mettent en œuvre des contrôles techniques pour empêcher un prestataire ou son réseau de nuire à tout autre prestataire ou à son réseau.	16.10
M10.25 Les prestataires doivent exiger contractuellement que les administrateurs tiers mettent en œuvre une séparation logique au sein du réseau de l'administrateur tiers afin de séparer les données et les réseaux des clients.	16.11
M10.26 Les prestataires doivent exiger contractuellement que les administrateurs tiers mettent en place une séparation entre les environnements de gestion des administrateurs tiers utilisés pour différents réseaux de prestataires.	16.11
M10.27 Les prestataires doivent exiger contractuellement que les administrateurs tiers mettent en œuvre et appliquent des fonctions de renforcement de la sécurité à la frontière entre le réseau de l'administrateur tiers et le réseau du prestataire.	16.11

M10.28 Les prestataires doivent exiger contractuellement que les administrateurs tiers mettent en œuvre des contrôles techniques pour limiter le potentiel des utilisateurs ou des systèmes à avoir un impact négatif sur plus d'un prestataire.	16.11
M10.29 Les prestataires doivent exiger contractuellement que les administrateurs tiers mettent en œuvre des postes de travail à accès privilégié logiquement indépendants par prestataire.	16.11
M10.30 Les prestataires doivent exiger contractuellement que les administrateurs tiers mettent en œuvre des domaines et des comptes administratifs indépendants par prestataire.	16.11
M10.36 Les prestataires doivent exiger contractuellement des fournisseurs d'équipements de réseau qu'ils partagent avec eux une « déclaration de sécurité » sur la manière dont ils produisent des équipements sécurisés et s'assurent qu'ils maintiennent la sécurité de l'équipement tout au long de sa durée de vie. Il est recommandé que toute déclaration de ce type couvre tous les aspects décrits dans l'évaluation de la sécurité du fournisseur (VSA) (voir annexe B), et les prestataires doivent encourager leurs fournisseurs à publier une réponse à la VSA.	16.12
M10.38 Les prestataires doivent s'assurer, par des dispositions contractuelles, que la déclaration de sécurité du fournisseur d'équipements de réseau est signée à un niveau de gouvernance approprié.	16.12
M10.40 Les prestataires doivent exiger contractuellement que le fournisseur d'équipements de réseau adhère à une norme qui ne soit pas inférieure à la « déclaration de sécurité » du fournisseur d'équipements de réseau.	16.13
M10.41 Les prestataires doivent exiger contractuellement des fournisseurs d'équipements de réseau qu'ils fournissent des conseils actualisés sur la manière dont l'équipement doit être déployé de manière sécurisée.	16.13
M10.42 Les prestataires doivent exiger contractuellement des fournisseurs d'équipements de réseau qu'ils assurent le support de tous les équipements et de tous les sous-composants logiciels et matériels pendant la durée du contrat. La période d'assistance pour le matériel et les logiciels doit être inscrite dans le contrat.	16.13
M10.43 Les prestataires doivent exiger contractuellement des fournisseurs d'équipements de réseau qu'ils fournissent les détails (produit et version) des principaux composants tiers et des dépendances, y compris les composants open-source, ainsi que la période et le niveau de support.	16.13
M10.44 Lorsque cela est pertinent pour l'utilisation particulière des équipements d'un fournisseur, les prestataires doivent exiger contractuellement des fournisseurs tiers qu'ils remédient à tous les problèmes de sécurité qui posent un risque de sécurité pour le réseau ou le service d'un fournisseur, découverts dans leurs produits dans un délai raisonnable après avoir été notifiés, en fournissant des mises à jour régulières sur les progrès réalisés en attendant. Cela inclut tous les produits touchés par la vulnérabilité, et pas seulement le produit pour lequel la vulnérabilité a été signalée.	16.13
M10.39 Lorsque le fournisseur d'équipements de réseau prétend avoir obtenu des évaluations ou des certifications de sécurité de ses équipements reconnues au niveau international (telles que les Critères Communs ou NESAS), les prestataires doivent exiger contractuellement des fournisseurs d'équipements qu'ils partagent avec eux les résultats complets qui attestent de cette évaluation ou de ce certificat.	16.14
M10.35 Les prestataires doivent exiger que les réseaux de l'administrateur tiers qui pourraient avoir un impact sur le prestataire soient soumis au même niveau de test que celui que le prestataire s'applique à lui-même (par exemple, le test TBEST tel que défini pour le fournisseur par Ofcom de temps à autre).	16.15

M10.46 Les prestataires doivent s'assurer que leurs contrats autorisent le partage des détails des problèmes de sécurité, le cas échéant, afin de soutenir l'identification et la réduction des risques d'atteinte à la sécurité du réseau public de communications électroniques ou du service public de communications électroniques, suite à des actions ou omissions de fournisseurs tiers.	16.16
M21.02 Les mesures à prendre par le prestataire en vertu de la Réglementation 3(3)(f) doivent normalement inclure l'assurance, dans la mesure où cela est raisonnablement possible, que l'équipement exécutant les fonctions de surveillance du réseau du fournisseur est situé au Royaume-Uni et exploité par du personnel basé au Royaume-Uni.	16.18
M21.02 Les mesures à prendre par le prestataire en vertu de la Réglementation 3(3)(f) doivent normalement inclure l'assurance, dans la mesure où cela est raisonnablement possible, que l'équipement exécutant les fonctions de surveillance du réseau du fournisseur est situé au Royaume-Uni et exploité par du personnel basé au Royaume-Uni. M16.07 Les systèmes qui collectent et traitent les données de journalisation et de surveillance doivent être traités comme des fonctions de surveillance du réseau.	16.18 et 16.19
M1.02 Les tests de sécurité sur les systèmes tournés vers l'extérieur, à l'exclusion du CPE, doivent normalement être effectués au moins tous les deux ans, et en tout cas peu de temps après un changement important.	17.2
M1.03 Les équipements situés dans la bordure exposée ne doivent pas héberger de données sensibles ou de fonctions critiques pour la sécurité.	17.2
M1.04 Une séparation physique et logique doit être mise en place entre la bordure exposée et les fonctions critiques pour la sécurité. (Notez que cette exigence peut ne pas être nécessaire lorsque les ensembles de données et les fonctions peuvent être protégés de manière cryptographique contre la compromission).	17.2
M1.05 Des frontières de sécurité doivent exister entre la bordure exposée et les fonctions critiques ou sensibles qui mettent en œuvre des mesures de protection.	17.2
M8.12 Pour les cartes SIM à profil fixe, le prestataire doit s'assurer que les données SIM sensibles sont protégées de manière appropriée tout au long de leur cycle de vie, à la fois par le vendeur de la carte SIM et au sein du réseau de l'opérateur, étant donné le risque pour la résilience du réseau et la confidentialité en cas de perte de ces informations.	19.1
M8.13 Pour les cartes SIM à profil fixe, la confidentialité, l'intégrité et la disponibilité des données sensibles de la carte SIM partagées avec le fournisseur de la carte SIM doivent être protégées à chaque étape de leur cycle de vie.	19.1