Public

POUR PROTÉGER BT

Our Standard on 3rd Party Controls (Norme applicable aux contrôles imposés aux tiers)

Version : 1.1 **Propriétaire :** Mark Tilston

Cette norme définit les contrôles de sécurité de base applicables aux tiers avec lesquels nous travaillons.

Publiée et communiquée à toutes les parties concernées, elle appartiendra à son propriétaire, le Expert technique qui se chargera de l'examiner au moins une fois par an, pour veiller à ce qu'elle reste conforme aux exigences des parties concernées et aux objectifs commerciaux décrits dans l'ISMS de BT.

Elle s'applique à tous les tiers travaillant pour ou au nom de BT Group, Openreach, EE et PlusNet inclus.

Dans un souci de simplification, nous les évoquerons en utilisant le terme générique « BT » dans le reste de ce document.

Les activités destinées à être exécutées par une partie prenante de BT sont surlignées en gris.

Introduction

BT s'engage à fournir un environnement sécurisé auquel peuvent se fier ses clients et employés. Notre but est de protéger nos informations et systèmes contre le risque de destruction accidentelle ou délibérée, d'endommagement, de modification ou de divulgation. Dans cette optique, nous veillons à la mise en œuvre par les tiers avec lesquels nous travaillons, des mesures de contrôle qui conviennent pour protéger la confidentialité, l'intégrité et la disponibilité de nos informations et systèmes.

À qui cette norme s'applique-t-elle ?

Cette norme s'applique à n'importe quel tiers amené à travailler pour ou au nom de BT, ayant accès aux informations et données de BT à des fins de consultation, de traitement, de stockage ou de distribution. Nous pourrions être amenés à la modifier à l'occasion, sous réserve de tout processus de concertation convenu en interne.

Définition des termes :

Terme	Explication
doit	Ce mot, au même titre que les termes « REQUIS » ou « DEVRA » rappelle que la définition évoque une exigence absolue.
ne doit pas	Ce groupe de mots, au même titre que les termes « NE DEVRA pas » rappelle que la définition évoque une interdiction totale.
Pourrait	Ce mot, au même titre que l'adjectif « FACULTATIF » s'applique à un élément soumis à un choix.
Devrait	Ce mot, au même titre que l'adjectif « RECOMMANDÉ » indique que dans certains cas, une raison valable justifie la décision de ne pas tenir compte d'un élément spécifique, sachant toutefois que les conséquences de cette décision sont entièrement comprises et qu'une autre option a été choisie sur la base d'une évaluation réfléchie.
ne devrait pas	Ce groupe de mots, au même titre que le groupe de mots « PAS RECOMMANDÉ » indique que tous les efforts seront faits pour satisfaire aux exigences d'un contrôle, sachant toutefois qu'il pourrait parfois s'avérer impossible d'éviter l'action décrite. Dans les cas où un contrôle ne peut pas être respecté, les conséquences seront évaluées et entièrement comprises.

Champ d'application

Ce document décrit, à un haut niveau, les contrôles de sécurité minimum requis pour gérer la sécurité au sein de la chaîne logistique des tiers de BT.

Le personnel de BT trouvera les normes à l'appui, ainsi que les références, documents de processus et lignes directrices décrivant la mise en œuvre des contrôles à lire conjointement à cette norme, sur le site Internet dédié à la sécurité.

Les parties prenantes de BT qui souhaitent demander l'exclusion d'un tiers par rapport à cette norme, sont priées de recourir au Processus d'exemption

Que contient ce document ?

1. Rôles et responsabilités

Les tiers doivent être conscients des exigences de cette norme 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.

Il incombe aux parties prenantes de BT de veiller au respect de cette norme et d'œuvrer avec leurs tiers, pour améliorer ce respect et mettre en œuvre les mesures d'atténuation qui s'imposent en cas de lacunes.

Les cadres de BT sont responsables de veiller à ce que leurs effectifs connaissent et respectent les exigences de cette norme, des politiques et normes connexes.

2. Gouvernance

2.1. 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.

2.2. 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.

2.3. 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.

2.4. Le tiers doit veiller à ce que BT soit informée (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.

3. Gestion des incidents

3.1. 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).

3.2. 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. Ces coordonnées doivent inclure : -
le nom, la responsabilité, le rôle et l'adresse électronique au sein du groupe et/ou le numéro de téléphone.

3.3. Le tiers informera de l'incident la partie prenante de BT, 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 douze (12) heures après avoir pris connaissance de l'incident.

3.4. 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.

3.5. Le tiers fournira un rapport à la partie prenante de BT consécutivement aux incidents impactant le service dont il s'acquitte auprès de BT ou sur les informations de BT et l'informant au minimum des éléments suivants :

- date et l'heure de l'incident
- endroit où l'incident a été constaté
- type d'incident
- impact
- classification des informations impactées (cf.3rd Party Information Classification and Data Handling Standard Norme de classification des informations et de manipulation des données applicable aux tiers)
- état
- résultat (recommandations relatives à la résolution ou mesures prises incluses).

3.6. 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 veiller à établir une relation contractuelle avec cet autre sous-traitant et s'assurer que ce dernier dispose d'une structure de sécurité conforme aux normes de l'industrie.

4. Gestion du changement

4.1. 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.

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

4.3. Le tiers doit avertir BT, immédiatement, des changements significatifs du service (notamment, mais pas exclusivement), des changements portant sur la méthode d'accès à travers les pare-feux, fourniture de la traduction des adresses réseau incluse.

4.4. 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.

4.5. 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.

5. Gestion des cyber-risques et menaces

5.1. 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-elles 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.

5.2. 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.

5.3. 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.

6. Gestion des identités et contrôle des accès

6.1 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 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.

6.2 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)/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.

6.3 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.

6.4 Le tiers doit veiller à ce que chaque transaction ne puisse être liée qu'à une seule personne identifiable et, en cas d'informations d'identification partagées, que des contrôles de compensation appropriés soient en place (procédures « break the glass » consistant à casser les permissions d'accès en cas d'urgence incluses).

6.5 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.

6.6 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.

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

7. Gestion des actifs informatiques

7.1. Le tiers doit disposer d'un inventaire des actifs informatiques (qui, le cas échéant, devrait inclure les équipements de BT éventuellement hébergés dans les locaux du tiers) et veiller à ce qu'il soit soumis, au moins une fois par an, à une vérification visant à confirmer que l'inventaire des actifs informatiques est à jour, complet et exact.

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

- Périphériques 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.

8. Accès aux systèmes de BT

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

8.2 Il incombe au tiers d'informer BT, dans les 24 heures, lorsqu'une personne du tiers n'a plus besoin de son droit d'accès.

8.3 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

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

8.5 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.

8.6 En cas de connectivité entre les systèmes du tiers et de BT, cette connectivité dépendra d'une liaison sécurisée et d'une protection des données par chiffrement conforme aux contrôles exposés dans la **Section 11 Cryptographie**.

8.7 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.

9. Sécurité physique des 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.

9.5 Les enregistrements des caméras de télésurveillance doivent être conservés pendant au moins 20 jours. Cette période peut néanmoins être prolongée, dans les cas suivants :

- si les enregistrements des caméras de télésurveillance doivent servir de preuve à la suite d'un incident ou dans le cadre d'une enquête criminelle ou
- Si la législation l'impose spécifiquement.

9.6 Les enregistrements et enregistreurs de télésurveillance 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.

9.7 Le tiers doit avoir pris les mesures qui conviennent pour assurer la sécurité physique des aspects 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.

9.8 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.

9.9 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 la partie prenante de BT.

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

9.10 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.

9.11 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).

10.Classification et protection des données

10.1 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/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.
- Les informations de BT doivent être manipulées conformément à la 3rd Party Information Classification and Data Handling Standard (Norme de classification des informations et de manipulation des données applicable aux tiers) du tiers.

11. Cryptographie

11.1 Le tiers doit veiller, lorsque le niveau de risque oblige à recourir au chiffrement, à ce que les données concernées soient correctement chiffrées (en transit et au repos) et, en cas de recours aux clés de chiffrement, à ce que ces clés soient conçues et implémentées conformément aux exigences de sécurité de la norme NIST FIPS 140-2, niveau 2 ou supérieur.

11.2 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.

11.3 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.

11.4 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.

11.5 Les hash salés doivent être utilisés pour protéger les données stockées ex. 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.

11.6 Gestion de clé - création et mise en service

- Les clés de sessions et valeurs uniques (nonces) doivent être créées avec un générateur de nombres pseudo-aléatoires sécurisé. Il doit être amorcé avec au moins autant de bits d'entropie ou le caractère inattendu d'un message, que le nombre effectif de bits de sécurité fourni par l'algorithme utilisateur de la clé.
- Recourir à une clé plus courte de 64 bits et la combiner de manière non-chiffrée avec la même clé de 64 bits pour obtenir 128 bits, n'est pas permis.
- Tous les bits de la clé doivent être utilisés par l'algorithme.
- Le remplissage ou d'autres bits utilisés par l'algorithme ne comptent pas dans le calcul de la longueur de la clé.

11.7 Gestion des clés – caractère aléatoire

- Une source robuste de données aléatoires doit être utilisée pour produire les clés de la partie symétrique du chiffrement hybride, les sels ou les vecteurs d'initialisation.
- Les générateurs de nombres pseudo-aléatoires (PRNG) peuvent être utilisés, mais pour être considéré comme étant sécurisé, le PRNG ne doit pas permettre à la personne malveillante :
  - De deviner l'output postérieur du générateur sur la base de la partie connue de l'output précédent.
  - De calculer les états précédents du générateur, sur la base de l'état actuel connu.
  - De distinguer l'output du PRNG par rapport à des variables réellement aléatoires. (l'utilisation de la fonction rand() n'est pas permise.

11.8 Gestion des clés - échange de clés

- Les clés de session générées pour être utilisées avec un algorithme symétrique doivent être échangées à l'aide d'un protocole d'échange de clés sécurisé.

11.9 Gestion des clés - stockage de clés

- Lorsque les clés sont utilisées pour protéger les données au repos, la clé de chiffrement de données (DEK) doit être protégée à l'aide d'une clé de chiffrement à clé, laquelle doit être stockée sur un serveur séparé ou dans un module de plateforme sécurisée (TPM).
- Si la clé de chiffrement à clé est stockée sur un serveur séparé, elle doit être protégée en transit vers le serveur chargé d'héberger les données.

11.10 Gestion des clés - rotation des clés (régénération)

- La clé doit pouvoir être régénérée conformément aux meilleures pratiques de l'industrie sur la durée de vie de la clé.
- Les données à protéger doivent pouvoir être rechiffrées avec la clé générée.
- La régénération ad hoc de la clé et le rechiffrement des données doivent être possibles si la clé de chiffrement d'origine risque d'avoir été compromise.
- Pour AES GCM, la probabilité que la fonction de chiffrement authentifiée soit jamais invoquée avec le même IV et la même clé sur deux (ou plus) ensembles distincts de données d'entrées, ne doit pas dépasser 232.

11.11 Gestion des clés - modules de sécurité matériel (HSM)

- Les clés cryptographiques doivent être chargées sur un module de sécurité matériel à l'aide d'une carte à puce.
- L'accès aux cartes à puce doit dépendre de la saisie d'un code confidentiel (PIN).

- Les codes confidentiels (PIN) doivent être choisis conformément à la politique de contrôle des accès.
- Les codes confidentiels (PIN) et cartes à puce doivent être stockés dans un coffre-fort évalué par notre équipe Infosec.
- Les clés de chiffrement ne doivent pas pouvoir être extraites d'un module de sécurité matériel.
- Toute tentative d'ouverture du boîtier doit déclencher la destruction des clés de chiffrement par les modules de sécurité matériel.
- S'agissant des modules de sécurité matériel contenant des clés sensibles, les codes confidentiels (PIN) et cartes à puce utilisés pour les protéger ne doivent être configurés et stockés que par les membres du personnel de sécurité des technologies.
- Dans les cas où les modules de sécurité matériel doivent servir à protéger des données très sensibles, un quorum minimum de deux cartes à puce et leurs codes confidentiels associés doit être atteint pour modifier les modules. Les membres du quorum doivent avoir été approuvés au niveau enquête renforcée.

11.12 Certificats numériques

- L'attribut Certificate Revocation List Distribution Point (Point de distribution de liste de révocation de certificats) des certificats doit être défini.
- Online Certificate Status Protocol (OCSP - Protocole de vérification de certificat en ligne) ou la Certificate Revocation List (CRL - Liste de révocation de certificats) doivent être utilisés pour déterminer l'état du certificat.
- Les propriétaires du certificat doivent suivre la validité et l'expiration des certificats détenus, pour veiller à ce que les événements d'expiration attendus ne provoquent pas une défaillance du système.
- Les consommateurs (clients) du certificat doivent suivre la validité et l'expiration des certificats utilisés, pour veiller à ce que les événements d'expiration attendus ne provoquent pas une défaillance du système.
- La durée de vie du certificat doit être sélectionnée en fonction de son usage.
- La durée de vie du certificat doit être établie avant sa délivrance.
- Le recours à l'identité standard (client, serveur) 1024 n'est pas permis.

11.13 Données en transit

- Le chiffrement des données en transit s'exécute typiquement à l'aide du chiffrement de transport ou de charge utile (message ou champ sélectif). Les exemples suivants figurent, entre autres, parmi les mécanismes de chiffrement de transport :
- Transport Layer Security (TLS - Sécurité de la couche de transport)
- Secure Tunnelling (Tunnel sécurisé IPSec)
- Secure Shell (SSH)
- Pour le chiffrement de transport, le composant symétrique doit se conformer à la section 12.14 de cette norme.
- Les protocoles de sécurité de transport doivent être configurés pour empêcher la négociation des algorithmes plus faibles et/ou des clés plus courtes, lorsque les deux extrémités prennent en charge l'option la plus puissante.
- Étant donné diverses vulnérabilités connues associées à ce protocole, le protocole SSL ne doit pas être utilisé.
- Les vecteurs d'initialisation du chiffrement par flot et AES en mode CBC ne doivent pas être prévisibles.
- IV/nonce en AES GCM doit satisfaire l'exigence d'unicité suivante :
  - Le respect de cette exigence est primordial pour la sécurité de GCM.

- Les protocoles de sécurité de transport doivent être configurés (ex. utilisation de bits de direction) pour éviter les attaques à texte clair connu sur messages connus renvoyés ex. « rien à signaler ».
- La vérification mutuelle d'identité doit être exécutée au moment de la configuration du transport.
- Pour les données courtes sensibles nécessitant le chiffrement de charge utile (clés de chiffrement, mots de passe, détails liés aux cartes de paiement), chiffrement asymétrique recourant au moins aux longueurs de clé minimales et aux algorithmes détaillés dans ce document.
- Les données de gestion système doivent être chiffrées en transit.
- Les options TLS suivantes ne sont pas permises : TLS v1.0, TLS v1.2, v6.0, TLS v6.1 et SSL (toutes versions)
- Les options SSH (SFTP) suivantes ne sont pas permises : SSH v1
- Les options IPsec suivantes ne sont pas permises : IKE Version 1

11.14 Données au repos

- Sont dites « au repos » les données stockées dans des fichiers, bases de données, emplacements provisoires et d'échange ou sur n'importe quel périphérique, dont entre autres les PC, ordinateurs portables et autres terminaux portables, serveurs, bandes, SAN, USB, CD, DVD, disquettes et autres solutions de stockage amovibles.
- Les données du niveau confidentiel ou au-delà stockées sur une mémoire non volatile, tous périphériques confondus, doivent être chiffrées.
- Les détails liés aux cartes de paiement stockés sur un périphérique, quel qu'il soit dans une mémoire non volatile, doivent être chiffrés.
- Dans les cas où des données de clé symétrique sont stockées et protégées par une clé asymétrique, cette dernière doit être aussi puissante, en termes de bits de sécurité, que la clé symétrique elle-même.
- La documentation système doit identifier la classification des données et les volumes stockés par le système.
- Les clés servant au déchiffrement ne doivent pas être stockées ou faire l'objet de copies de sauvegarde avec les données qu'elles déchiffrent. Les logiciels doivent faire l'objet de tests complets avant d'être déployés sur les systèmes de production.

12. Prévention des fuites de données

12.1 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 :

- E-mail
- Internet/passerelle Web Gateway (stockage en ligne et messagerie Web)
- Ports/stockage portable USB, optique et autres, etc.
- Informatique mobile et BYOD
- Services d'accès à distance
- Mécanismes de partage de fichiers et médias sociaux

NB. Les supports amovibles/périphériques portables doivent être désactivés par défaut et uniquement activés pour des raisons professionnelles légitimes. Toute donnée stockée sur un support amovible ou un périphérique portable doit être chiffrée proportionnellement au risque. 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. Voir 3rd

Party Information Classification and Data Handling Standard (Norme de classification des informations et de manipulation des données applicable aux tiers) pour de plus amples détails sur la manipulation des supports amovibles.

13. PCI DSS

13.1 S'il doit traiter les données de paiement par carte, le tiers doit vérifier sa conformité appropriée à la norme PCI-DSS.

14.Informatique dans le Cloud/en ligne

14.1. 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.

14.2. 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.

14.3. 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.

15. Médias sociaux

15.1. Le tiers doit disposer d'une structure établie et cohérente régissant l'utilisation acceptable des médias sociaux par l'entreprise et les personnes, notamment :

- 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.
- Par rapport à l'utilisation sans permission préalable des logos de l'organisation ou de clients.
- Par rapport à la diffusion sans consentement préalable, d'informations privées de l'organisation ou des clients.
- Par rapport à la publication d'options sur l'organisation, ses clients internes ou externes, susceptibles d'être raisonnablement considérés comme des commentaires officiels formulés par l'organisation ou ses clients.
- Par rapport à l'interdiction de publier des informations de BT portant la marque « Confidential » (Confidentiel) ou « Highly Confidential » (Strictement confidentiel).

16.Configuration système

16.1. Le tiers doit disposer d'une structure établie et cohérente pour veiller à ce que les systèmes soient correctement configurés (systèmes du tiers et systèmes fournis à BT), laquelle tiendra notamment compte des composants 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.

17. Développement de logiciels sécurisé

17.1. 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 live 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.

17.2. Le tiers doit disposer d'une structure établie et cohérente de développement, pour éviter les vulnérabilités de la 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 à la production.

17.3. 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 composants 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 suivies, paiements et révisions appropriés de l'entente d'entiercement.

18. Protection anti-programme malveillant

18.1. 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.

19. Gestion des vulnérabilités

19.1. 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.

19.2. 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

19.3. 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.

19.4. 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.

19.5. Le tiers doit veiller à ce qu'au moins une fois par an, une évaluation indépendante de la sécurité des technologies de l'information/un test d'intrusion soit commandé pour éprouver 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.

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

19.7. 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.

19.8. 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.

20.Intégrité du réseau

20.1. 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 capables 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, chiffrement des accès d'administrateur autres que ceux de la console inclus.
- 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 principe de sécurité meilleure pratique 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.

20.2. Le réseau tiers devrait 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.

21. Atténuation du déni de service

21.1. 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).

22. Journalisation et surveillance continues

22.1. Le tiers doit veiller à disposer d'une structure établie et cohérente d'audit et de gestion des journaux, 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 12 mois. Au minimum, le tiers doit veiller à ce que les journaux (au besoin) renseignent sur les événements suivants :

- Points de départ et de fin du processus enregistré.
- 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).

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

- Veiller à ce que les journaux d'événements clés soient examinés par une fonction indépendante au moins une fois par mois, pour détecter les activités non autorisées, les cibles et les types d'attaques.
- Veiller à ce que les exceptions soient consignées et examinées jusqu'à 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.

23. Formation et sensibilisation

23.1. 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 la protection des données à caractère personnel, avec remise à niveau une fois par an, au minimum, cette formation concernant notamment s'il y a lieu les :

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

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

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

24. Droit d'inspection

24.1. Le tiers doit autoriser BT, au moins une fois par an, 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 (ou immédiatement à la suite d'un incident).

24.2. 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.

24.3. 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, pour faciliter l'enquête, demande que le tiers s'engage à ne pas refuser ou entraver.

25. Sécurité physique – locaux de BT

25.1 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, bien en vue, avec photo claire et ressemblant à l'employé du tiers titulaire de la carte. BT peut aussi 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.

25.2 Dans les cas où le personnel du tiers a reçu une carte d'accès fournie par BT, il incombe au tiers d'avertir BT rapidement et au plus tard dans les cinq jours ouvrés, quand l'employé concerné n'a plus besoin d'accéder aux locaux de BT.

25.3 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.

25.4 La protection physique et les lignes directrices 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.

25.5 Dans les cas où le tiers est autorisé à fournir du personnel disposant d'un accès non hébergé à des zones des installations 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).

D'autre part, le signataire autorisé du tiers et le personnel du tiers auront, au minimum, satisfait aux exigences des contrôles de préemploi L2.

26. Sécurité du réseau – réseau appartenant à BT

26.1 Le tiers fournira au contact de BT Security les noms, l'adresse (et toutes autres coordonnées demandées par BT) de tous les employés du tiers qui, à l'occasion, doivent être amenés à participer

directement au déploiement, à la maintenance et/ou à la gestion du service, avant de les faire participer à de telles opérations de déploiement, de maintenance et/ou de gestion.

26.2 S'agissant 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 le contact de BT Security (ou la personne désignée), l'équipe devant assister aux réunions ponctuelles éventuellement programmées par le contact de Security BT, à la demande raisonnable de ce dernier.

26.3 Le tiers fournira au contact de BT Security la liste (mise à jour ponctuellement si nécessaire) des composants actifs inclus dans le service et/ou les services et de leurs sources respectives.

26.4 Le tiers fournira les détails de chaque employé amené à échanger avec l'équipe de gestion des vulnérabilités de BT (CERT), à propos des vulnérabilités identifiées par BT et le tiers dans le cadre du et/ou des services. Le tiers fournira à BT les informations opportunes sur les vulnérabilités et se conformera (à ses propres frais) aux exigences raisonnables éventuellement signalées par le contact de BT Security relativement aux vulnérabilités. Le tiers informera BT des vulnérabilités, le cas échéant, suffisamment rapidement pour que puissent être appliqués ou installés les contrôles d'atténuation avant que le tiers n'annonce publiquement les vulnérabilités.

26.5 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.

26.6 Le tiers fournira au contact de BT Security 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 portée à la feuille de route des services) périodiquement :

- Portées à la connaissance du tiers ou
- Que le contact de BT Security croit raisonnablement et en informe le tiers, avoir été conçues ou 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 au contact de BT Security de comprendre parfaitement la nature, la composition et l'importance de ces caractéristiques et/ou fonctionnalités.

26.7 Afin de préserver l'accès aux réseaux et/ou systèmes de BT, le tiers avertira BT immédiatement de toute modification de sa méthode d'accès à travers les pare-feux, communication de la traduction de l'adresse réseau incluse.

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

26.9 Le tiers s'assurera que la fonctionnalité Ipv6 incluse dans les systèmes d'exploitation est désactivée sur les hôtes (périphériques ou serveurs d'utilisateur final, par exemple) se connectant au réseau de BT et les domaines inutilisés doivent être désactivés.

26.10 Le personnel du tiers chargé de construire, développer ou supporter les réseaux ou actifs réseau de BT, veillera à ce que chaque membre du personnel réponde, au minimum, aux conditions des contrôles de préemploi de niveau 2 (L2). Les contrôles de préemploi de niveau 3 (L3) seront demandés pour les rôles identifiés par le contact de BT Security. Dans les cas où le tiers n'est pas apte à s'acquitter directement de l'habilitation de sécurité de son personnel par rapport aux contrôles de niveau 3, BT l'aidera à l'obtenir aux frais du tiers.

26.11 Le tiers entretiendra le matériel et les logiciels conformément aux spécifications des fabricants.

26.12 Le tiers n'utilisera aucun support amovible (disques, lecteurs USB, etc.) destiné au support et à la maintenance, pour un autre usage quel qu'il soit.

27. Glossaire

Terme	Définition
Authentification à deux facteurs	Parfois appelée vérification en deux étapes ou double authentification. Il s'agit d'un processus de sécurité par lequel l'utilisateur fournit deux facteurs d'authentification différents, pour s'autovérifier et mieux protéger ses informations d'identification d'une part et de l'autre, les ressources auxquelles il souhaite accéder.
tiers	Qualifie les personnes qui travaillent pour nous, mais ne font pas partie du personnel de BT.
AES	La norme de chiffrement Advanced Encryption Standard (AES) est une spécification de chiffrement des données électroniques, établie par le National Institute of Standards and Technology (NIST - Institut national des normes et technologies) américain en 2001.
ASG	Application Support Group
BT Group	BT Group regroupe les CFU (Unités en contact direct avec la clientèle) et CU (Corporate units) de BT Group dont notamment, mais pas exclusivement, Openreach, EE et Plusnet - sauf indication contraire, ces entités sont évoquées par l'utilisation du terme générique « BT » pour les besoins de ce document.
BT Stakeholder (Partie prenante)	Employé de BT responsable du travail confié au tiers.
CCTV	ou vidéosurveillance.
DBA	Administrateur de base de données
DC	Centre de données
Défense en profondeur	Méthode de cybersécurité par laquelle une série de mécanismes défensifs s'intercalent en couches, afin de protéger des données et informations précieuses. Si un des mécanismes échoue en cas d'attaque, un autre mécanisme le remplace immédiatement pour la déjouer.
DR	Disaster Recovery (Reprise d'activité ou rétablissement après sinistre)
GCM	Galois/Counter Mode, mode d'opération de chiffrement par bloc en cryptographie symétrique, très répandu en raison de son efficacité.
HDD	Hard Disc Drive (Lecteur de disque dur)
HMG	Her Majesty's Government (Gouvernement de Sa Majesté) - ce sigle couvre les organismes du gouvernement britannique.
ISMS	Information Security Management System (Système de gestion de la sécurité de l'information). Cadre de politiques et procédures regroupant les contrôles légaux, physiques et techniques se rapportant aux processus de gestion des risques liés à la sécurité de l'information d'une organisation.
ISO 27001	Norme industrielle relative aux systèmes de gestion de la sécurité de l'information (ISMS).
ISO 27017	Code de pratique des contrôles de sécurité de l'information basé sur la norme ISO/IEC 27002 pour les services dans le Cloud.
ISO 7816	Norme internationale se rapportant aux cartes d'identification électronique à contact et en particulier, aux cartes à puce, gérée conjointement par International Organization for Standardisation (ISO - Organisation internationale de normalisation) et la Commission électrotechnique internationale (CEI).
NAS	Serveur de stockage en réseau de fichiers de données.
NIST	Le National Institute of Standards and Technology (Institut national des normes et technologies) est à la fois un laboratoire de sciences physiques et une agence non réglementée du Ministère du Commerce américain.

PCI DSS	Payment Card Industry Data Security Standard (PCI DSS - Norme de sécurité des données applicables à l'industrie des cartes de paiement) est une norme de sécurité de l'information développée pour les organismes traitant les cartes de crédit des grands systèmes de cartes.
Comptes privilégiés	Est qualifié de « privilégié » l'utilisateur bénéficiant d'un accès aux systèmes critiques à des fins d'administration.
RSA	(Rivest–Shamir–Adleman) est l'un des premiers systèmes de chiffrement à clé publique, largement utilisé pour la transmission de données sécurisée.
SAN	Réseau de stockage local composé de plusieurs périphériques, basé sur des blocs.
SSD	Solid State Drive (Disque semi-conducteur)

28.Historique des modifications

N° de version	Date	Modification apportée par	Brefs détails de la modification
0.1	30/10/2017	Mark Tilston	Version initiale de mappage et mise à jour de contenu.
0.2	10/04/2019	Tim Hunt	Transfert au nouveau format.
1.0	01/05/2019	Ian Morton	Passage à Bon pour publication.
1.1	01/10/2019	Karen Tanner	Contrôles supplémentaires ajoutés dans le cadre de l'ajustement des exigences de sécurité de BT.

29.Validation du document

Fonction	Date
Mark Tilston	06/11/2019

30.Conformité

La plupart des employés de BT se comporte avec professionnalisme et respecte les valeurs de l'entreprise. Sachez toutefois que tout comportement non conforme à cette norme vous exposerait au risque de mesures disciplinaires, en adéquation avec la législation et la réglementation locales.

Pour toute autre personne, tout comportement non conforme à cette norme compromettrait sérieusement la continuité de nos arrangements mutuels vis-à-vis de vos services.

31.Liens et informations utiles

À l'intention du personnel de BT :

Suivez ce lien pour consulter les Politiques et normes de BT.

Nos politiques et normes font l'objet, au minimum, d'une révision annuelle. Pour consulter notre programme de révision, veuillez cliquer ici.

Pour signaler un « incident de sécurité », écrivez au : Security Control Centre (Centre de contrôle de sécurité).

Pour de plus amples détails ou des conseils sur cette norme, une autre politique de sécurité ou d'autres normes, contactez security.policy@bt.com

À l'intention des tiers :

Le lien suivant vous permettra de consulter les normes et autres conditions de sécurité pertinentes.

32. Propriété et confidentialité

Ce document ne doit pas être partagé avec un autre tiers, quel qu'il soit, sans le consentement écrit de BT. BT reste propriétaire de cette norme et de toute documentation connexe, qui doivent lui être retournées sur simple demande.

Ce document classé dans la catégorie « Internal » (Interne) doit être traité comme un document « Confidential » (Confidentiel) en cas de téléchargement par un tiers.