Public

PROTÉGER BT

Norme de classification des informations et de manipulation des données applicable aux tiers

Norme : 4.0 **Propriétaire :** BT Security

Cette norme définit les contrôles de sécurité de base applicables à nos tiers amenés à accéder, stocker ou traiter des informations de BT.

Elle s'applique à tous les tiers travaillant pour BT ou au nom du groupe BT Group, y compris Openreach, EE et PlusNet. Dans un souci de simplification, nous les évoquerons en utilisant le terme générique « BT » dans le reste de ce document.

Introduction

BT classe les données et informations dans plusieurs catégories en fonction des dommages potentiellement causés par leur perte ou leur divulgation non autorisée. Lors de leur création, les données et informations sont soumises à une évaluation dont la finalité consiste à les affecter à la catégorie de classification qui convient.

Les données et informations doivent être conservées pendant une période suffisante pour satisfaire aux obligations légales et réglementaires de l'entreprise, période à la fin de laquelle elles peuvent être dûment éliminées. Tout équipement ayant servi à stocker les données doit également être éliminé à la fin de sa durée de vie utile. L'élimination des équipements doit répondre aux critères de sensibilité environnementale les plus rigoureux.

Cette norme définit les exigences relatives à la classification des informations, à l'étiquetage, à la manipulation et au traitement, à la conservation et à l'élimination des données et actifs informatiques de BT.

Définition des termes :

Terme	Explication
Doit	Ce mot, au même titre que les termes « REQUIS » ou « EST TENU DE » rappelle que la définition évoque une exigence absolue.
Ne doit pas	Cette expression, au même titre que le terme « N'EST PAS AUTORISÉ À » rappelle que la définition évoque une interdiction totale.
Peut	Ce mot, au même titre que l'adjectif « FACULTATIF » s'applique à un élément optionnel.
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 aspect 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	Cette expression, au même titre que le groupe de mots « PAS RECOMMANDÉ » indique que tous les efforts nécessaires seront fournis pour satisfaire aux exigences d'un contrôle, sachant toutefois qu'il peut 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.
BT	Ce terme désigne le groupe BT Group, y compris Openreach, EE et Plusnet. Dans un souci de simplification, nous les évoquerons en utilisant le terme générique « BT » dans le reste de ce document.

Champ d'application

Cette norme s'applique à toutes les données et informations dont dispose BT, tous formats confondus. Par conséquent, elle s'applique notamment aux documents papier, électroniques, multimédias (photos, vidéo, WebEx etc.), contenus oraux (conversations téléphoniques, messages vocaux), données et informations présents dans les systèmes, applications ou équipements capables de stocker, traiter ou transmettre des données. Le champ d'application de cette norme couvre la classification, l'étiquetage, la manipulation/le traitement, la conservation et l'élimination des informations.

Que contient ce document ?

1. Aperçu de la classification des informations

Les informations détenues ou traitées par vous dans le cadre de votre relation de tiers avec BT n'auront pas toutes la même valeur ou le même degré de sensibilité. Il incombera à BT de classer les informations en fonction du champ d'application du service dont vous vous acquitterez à leur égard, afin qu'un niveau de protection suffisant soit appliqué aux informations et à ce qu'elles soit traitées dans les meilleures conditions d'efficacité et de sécurité.

La structure de classification de BT comprend les quatre catégories d'informations suivantes :

- Public
- Internal (Interne)(Interne)
- Confidential (Confidential)
- Highly Confidential (Highly Confidential)

Si la catégorie des informations que vous devez manipuler ne vous a pas été communiquée, veuillez contacter la partie prenante de BT ou votre Approvisionneur.

2. Niveaux de classification BT

Public

Informations dont la publication générale a été spécifiquement approuvée. Ce type d'informations n'est soumis à aucune exigence de manipulation particulière.

En voici quelques exemples : les détails de nos produits et services, informations publiées sur le site Internet externe de BT, communiqués de presse, livres blancs, supports publicitaires.

Internal (Interne)

Informations dont la divulgation non autorisée, surtout en dehors de BT, serait inappropriée. La diffusion de ce genre d'informations dans le domaine public n'est pas considérée comme étant dans l'intérêt de BT. Il peut s'agir d'informations réservées spécifiquement à certaines équipes ou fonctions de l'entreprise.
Remarque : en cas d'accès ou de stockage par un tiers, les informations passent à la classe de manipulation « Confidential ».

En voici quelques exemples : les informations figurant sur l'Intranet concernant le personnel et l'entreprise, la plupart des politiques, normes, processus et procédures de BT, des documents se rapportant aux projets et des procès-verbaux de réunions.

Confidential (confidentiel)

La divulgation non autorisée de ces informations, même dans les limites de l'organisation, pourrait sérieusement nuire aux intérêts de BT. Ces informations se limitent strictement aux, et sont diffusées uniquement aux personnes autorisées à satisfaire un besoin spécifique de l'entreprise dans le cadre de leurs fonctions. Tout manquement peut entraîner des pertes financières, une baisse de rentabilité ou la perte d'opportunités, une situation embarrassante ou préjudiciable à la réputation de BT, des sanctions légales ou réglementaires à l'encontre de BT. Les informations personnelles, relatives aux cartes de paiement ou relatives à la propriété intellectuelle appartiennent à la classe d'informations « Confidential ».
Les informations Confidentialles font l'objet de conditions d'exigences de manipulation particulières, qui doivent être respectées.

En voici quelques exemples : les informations personnelles concernant nos employés, tiers ou clients (notamment les paiements liés) telles que les contrats d'employés, données de performance, enquêtes CARE, identifiant de service personnel (ID de service, identifiant haut débit, identifiant PSTN). La documentation relative à certains projets d'infrastructure ou projets critiques, les diagrammes de réseau, contrats de fournisseurs tiers. Les données de journal système, les données de vente et marketing (changements de tarifs avant lancement, résultats financiers avant publication aux marchés), plans d'affaires locaux, données de risque, enregistrements des données

Highly Confidential (Hautement confidentiel)

La divulgation de ce type d'informations est susceptible de nuire aux chances de BT de concrétiser ses principaux objectifs commerciaux. Ces informations sont particulièrement sensibles et toute fuite peut causer de graves dommages à l'entreprise. L'accès aux informations Highly Confidential (Hautement confidentiel) les est limité à un très petit nombre de personnes. Leur accès doit être strictement interdit aux personnes non autorisées. Les exigences de manipulation de ces informations sont plus contraignantes que celles d'informations dites « Confidentialles ». La gravité du préjudice potentiel en fait la classe la plus contraignante. Toute personne amenée à gérer ce type d'informations

En voici quelques exemples : les mots de passe d'accès aux ordinateurs, le registre du risque de sécurité, certaines informations à caractère personnel sensibles concernant notamment les cartes de paiement, les numéros de sécurité sociale et détails de passeport. Les informations sensibles relatives aux RH susceptibles d'affecter un nombre important d'employés, les plans d'affaires stratégiques, stratégie concurrentielle, nouveaux produits stratégiques et nouvelles politiques marketing, évaluations très sensibles de concurrents, partenaires ou entrepreneurs, utilisation de l'Internet, numéros de compte des clients, rapports d'audit ou conclusions contenant des détails de lacunes et vulnérabilités considérables dans les pratiques ou processus de BT, informations susceptibles d'avoir une incidence sur le prix de nos actions notamment les procès-verbaux des réunions du conseil, informations susceptibles d'influer sur les cours, se

peut être invitée à signer un accord de confidentialité ou une liste d'initiés.

3. Exigences de manipulation et de traitement

Remarque : sauf spécification contraire, les informations assorties du niveau de classification « Public » ne sont liées à aucune exigence de manipulation particulière.

3.1 Manipulation du texte parlé et du multimédia.

Référence	Que souhaitez-vous faire de ces informations ?	Catégorie de classification	Exigences de manipulation
HSMS10	Je souhaite publier ces informations sur les médias sociaux ou sur les réseaux.	Public	Vous pouvez les publier sur n'importe quel groupe, comme Splash ou Yammer. Vous n'êtes pas autorisé à apporter des contributions aux sites ou à publier des déclarations en ligne susceptibles d'être raisonnablement considérées comme reflétant les opinions de BT.
		Internal (Interne)/Confidential (confidentiel)	Non autorisé.
		Highly Confidential (Hautement confidentiel)	Non autorisé.
HSMS20	Je veux dialoguer avec une personne ou la présenter par le biais d'une messagerie instantanée Internal, comme Microsoft Lync par exemple.	Internal (Interne)/Confidential (confidentiel)	Vous pouvez utiliser Internal (Interne)BT Live Meeting, Webex, Webjoin et Skype for Business. Assurez-vous d'avoir choisi le bon interlocuteur et de l'avoir vérifié avant d'aborder un thème spécifique, en gardant également à l'esprit que les informations suivantes ne doivent pas être partagées : · **Détails liés aux cartes de paiement, quels qu'ils soient,** · **Données à caractère personnel,** · **Coordonnées bancaires,** · **Code Confidential (PIN) ou tout autre mot de passe.**
		Highly Confidential (Hautement confidentiel)	Non autorisé.
HSM30	Je souhaite m'entretenir avec quelqu'un par messagerie instantanée externe.	Public	Les conversations doivent se limiter aux « informations à caractère public » librement disponibles sur le site Web externe de BT.

	Par exemple sur le site d'assistance d'un fournisseur comme Cisco.	Internal (Interne)/Confidential (confidentiel)	Autorisé uniquement après vérification de l'identité du ou des interlocuteurs concernés selon le principe du « besoin d'en connaître » avant de révéler une information Confidentialle quelconque sur des personnes, en gardant à l'esprit que les informations suivantes ne doivent pas être partagées : · **Détails liés aux cartes de paiement, quels qu'ils soient,** · **Données à caractère personnel,** · **Coordonnées bancaires,** · **Code Confidential (PIN) ou tout autre mot de passe.**
		Highly Confidential (Hautement confidentiel)	Non autorisé.
HSM40	Je souhaite m'entretenir avec quelqu'un en face à face ou par téléphone.	Internal (Interne)/Confidential (confidentiel)	Vous devez vérifier l'identité de votre interlocuteur selon le principe du « besoin d'en connaître » avant d'aborder des informations Confidentialles (cette règle s'applique également aux conversations dans les magasins et centres d'appel). Le cas échéant, un accord de confidentialité doit avoir été signé avant le début de la conversation. Veillez à ce que la conversation ne puisse pas être entendue par les personnes non couvertes par le principe du « besoin d'en connaître ». Ces informations ne doivent pas être laissées sur les systèmes de messagerie vocale.
		Highly Confidential (Hautement confidentiel)	Comme pour « Confidential ». Limitez les informations « Highly Confidential (Hautement confidentiel) » au strict minimum.
HSM50	Je souhaite envoyer un SMS à toutes les parties (Internals et externes).	Public	Le contenu du message doit se limiter aux « informations à caractère public » librement disponibles sur le site Web externe de BT.

		Internal (Interne)/Confidential (confidentiel)	Le contenu du message doit se limiter au « besoin d'en connaître », en gardant à l'esprit que les informations suivantes ne doivent pas être partagées : **· Détails liés aux cartes de paiement, quels qu'ils soient,** **· Coordonnées bancaires,** **· Code Confidential (PIN) ou tout autre mot de passe,** **· Toute information à caractère personnel.**
		Highly Confidential (Hautement confidentiel)	Non autorisé.

3.2 Manipulation des documents papier.

Référence	Que souhaitez-vous faire de ces informations ?	Catégorie de classification	Exigences de manipulation
HPD10	Je souhaite stocker, copier, imprimer ou travailler au bureau sur des copies papier de ces informations.	Internal (Interne)/Confidential (confidentiel)	Les informations de BT ne doivent pas être utilisées sous forme de copies papier, à moins que cet usage ne soit inclus spécifiquement dans le champ d'application ou qu'il ait été approuvé par la partie prenante de BT, auquel cas les règles suivantes doivent être respectées : · Des mesures de protection des informations contre une divulgation accidentelle doivent avoir été prises, · Hors utilisation et après les heures de bureau, les informations doivent être rangées hors de portée, dans un lieu dont l'accès est réservé au personnel autorisé comme un casier, un tiroir verrouillé ou une salle dont l'accès est réglementé, · Utilisez une imprimante dont l'accès est contrôlé, reliée à un PC ou installée dans une pièce à accès contrôlé et vérifiez que les informations sont bien envoyées à la bonne imprimante, · Utilisez la fonction d'impression

			sécurisée pour récupérer de l'imprimante les supports imprimés, à moins que leur collecte immédiate ne soit assurée.
		Highly Confidential (Hautement confidentiel)	Non autorisé.
HPD20	Je souhaite imprimer un document depuis l'intérieur d'un bâtiment de BT.	Internal (Interne)/Confidential (confidentiel)	Veillez à ne pas vous tromper d'imprimante et à ne pas laisser les documents dans le bac d'impression. Utilisez une imprimante dont l'accès est contrôlé, reliée à un PC ou installée dans une pièce à accès contrôlé.
		Highly Confidential (Hautement confidentiel)	Comme pour « Internal (Interne)/Confidential (confidentiel) ».
HPD30	Je souhaite copier ou imprimer des informations en dehors des locaux autres que ceux de nos tiers ou de chez moi (autrement dit, dans les locaux d'un sous-traitant, à l'hôtel, etc.).	Internal (Interne)/Confidential (confidentiel)	Interdit.
		Highly Confidential (Hautement confidentiel)	Interdit.

HPD40	Je veux transporter des informations sur copie papier en dehors des bureaux de BT, des locaux d'un tiers de BT ou d'un magasin BT.	Internal (Interne)/Confidential (confidentiel)	**Les données se rapportant aux clients de BT et/ou aux paiements ne doivent pas sortir des bureaux de BT, des locaux de tiers de BT ou des magasins BT.** D'autres types d'informations sont également soumis à cette règle, à moins qu'elles soient incluses spécifiquement dans le champ d'application ou qu'elles aient été approuvées par la partie prenante de BT, auquel cas les règles suivantes doivent être respectées : · La manipulation des informations doit faire l'objet de mesures de vérification préalable, · Elles doivent être protégées contre le risque de compromission (par exemple transportées dans une chemise ou dans un sac opaque) · Elles ne doivent jamais rester sans surveillance, · En cas de perte, il vous incombe de signaler un incident de sécurité et d'avertir votre partie prenante BT le plus tôt possible.
		Highly Confidential (Hautement confidentiel)	Non autorisé.

HPD50	Je souhaite partager ou envoyer des informations sur copie papier à des parties Internals.	Internal (Interne)/Confidential (confidentiel)	Les informations sur BT ne doivent pas être utilisées sous forme de copie papier, à moins que cet usage ne soit inclus spécifiquement dans le champ d'application ou qu'il ait été approuvé par la partie prenante de BT, auquel cas les règles suivantes doivent être respectées : · Vous devez placer le document dans une enveloppe à usage Internal (Interne)ou sans fenêtre et le livrer en main propre ou par le biais de notre système de courrier Internal, · Elles ne doivent pas être envoyées aux parties Internals travaillant à domicile, · N'indiquez pas le niveau de classification à l'extérieur de l'enveloppe, · Si les informations sont couvertes par le « privilège juridique », appliquez les lignes directrices des privilèges juridiques, · En cas de perte, il vous incombe de signaler un incident de sécurité et d'avertir votre partie prenante BT le plus tôt possible.
		Highly Confidential (Hautement confidentiel)	Non autorisé.
HPD60	Je souhaite partager ou envoyer des informations sur copie papier à des parties externes.	Internal (Interne)/Confidential (confidentiel)	Interdit
		Highly Confidential (Hautement confidentiel)	Interdit
HPD70	Je souhaite envoyer un fax.	Internal (Interne)/Confidential (confidentiel)	Vous devez envoyer la page d'en-tête avec une page de test, puis contacter le destinataire pour confirmer sa réception avant de faxer le contenu. Si les informations sont couvertes par le « privilège juridique », suivez vos lignes directrices des privilèges juridiques.

		Highly Confidential (Hautement confidentiel)	Interdit
HPD80	Je souhaite me débarrasser d'informations sur copie papier.	Internal (Interne)/Confidential (confidentiel)	Vous devez vous assurer que les informations ne doivent pas être conservées pour des motifs légaux ou réglementaires. Les documents doivent être déchiquetés, au minimum, conformément à la norme DIN66399 niveau P-4, à l'aide d'une déchiqueteuse à coupe croisée (cette règle s'applique également aux détails des cartes de paiement). Ne les placez jamais dans une corbeille à papier ordinaire.
		Highly Confidential (Hautement confidentiel)	Vous ne devriez pas être en possession d'informations de cette classe sur copie papier. Si c'est le cas, les règles suivantes s'imposent : Vous devez vous assurer que les informations ne doivent pas être conservées pour des motifs légaux ou réglementaires. Les documents doivent être déchiquetés, au minimum, conformément à la norme DIN66399 niveau P-4, à l'aide d'une déchiqueteuse à coupe croisée (cette règle s'applique également aux détails des cartes de paiement) ou peuvent être incinérés conformément à la norme BS EN15713/2009. Ne les placez jamais dans une corbeille à papier ordinaire. **Remarque : Certaines informations peuvent nécessiter un déchiquetage des documents sur site, par un tiers externe certifié. Si c'est le cas, vous devrez obtenir un certificat de destruction auprès du tiers concerné.**

3.3 Manipulation des documents électroniques.

Référence	Que souhaitez-vous faire de ces informations ?	Catégorie de classification	Exigences de manipulation
HED10	Je souhaite stocker des informations électroniques sur mon ordinateur portable ou mon PC professionnels.	Toutes les données de BT	Les copies de travail peuvent être conservées sur votre ordinateur portable professionnel uniquement s'il est doté d'un système de chiffrement intégral des données stockées sur le disque de votre ordinateur, comme Bitlocker. Ce système convertit les informations en codes illisibles, difficiles à déchiffrer par une personne non autorisée. Les documents terminés doivent être stockés en toute sécurité et toute copie de travail doit être retirée de l'ordinateur portable.
HED20	Je souhaite stocker mes documents sur un système de gestion des documents comme SharePoint ou sur un lecteur réseau.	Internal (Interne)/Confidential (confidentiel)	Limitez l'accès du site et des documents à des fins de modification aux personnes disposant de l'approbation nécessaire. Le propriétaire ou l'administrateur du système de gestion des documents/du lecteur réseau doivent : - utiliser les niveaux et groupes de permission pour configurer le contrôle d'accès en fonctions des postes. Ils ne doivent pas être configurés au-delà du niveau minimum requis pour que la personne puisse travailler ; · revoir les contrôles d'accès chaque année ; · documenter le processus d'affectation des personnes aux postes. · Les postes et personnes affectés doivent être revus à intervalles réguliers et de préférence une fois par trimestre. **REMARQUE : les systèmes de gestion**

			des documents ou lecteurs réseau ne doivent pas servir à stocker des informations relatives aux cartes de paiement.
		Highly Confidential (Hautement confidentiel)	Comme pour « Internal (Interne)/Confidential (confidentiel) » et : Les documents doivent être chiffrés avant d'être chargés sur le système de gestion des documents. Vous devez également fixer la date de révocation de l'accès à votre document. **REMARQUE : les systèmes de gestion des documents ou lecteurs réseau ne doivent pas servir à stocker des informations relatives aux cartes de paiement.**
HED30	Je souhaite stocker des informations électroniques sur le Cloud ou à l'aide de services sur Internalt (cas de figure où il n'existe aucun contrat commercial d'hébergement d'informations de BT) comme Google docs,	Toutes les données de BT	Non autorisé.

	Github, Drop Box, Pastebin, Facebook, etc.		
HED40	Je souhaite stocker des informations électroniques sur un support amovible, comme une clé USB.	Toutes les données de BT	Autorisé seulement si un besoin commercial autorisé vous oblige à transporter des informations en dehors des bureaux de BT, en gardant à l'esprit que les dispositifs ou informations doivent être chiffrés. En cas de perte, il vous incombe de signaler un incident de sécurité et d'avertir votre partie prenante BT le plus tôt possible. **REMARQUE : les supports amovibles ne doivent pas servir à stocker des informations relatives aux cartes de paiement.**
HED50	Je souhaite stocker des documents ou informations électroniques sur mon ordinateur portable ou sur un terminal personnel.	Toutes les données de BT	Non autorisé.
HED60	Je souhaite envoyer des documents électroniques à mon adresse de messagerie électronique personnelle.	Toutes les données de BT	Non autorisé.
HED70	Je souhaite appliquer le transfert automatique d'e-mails vers une adresse de messagerie électronique externe.	Toutes les données de BT	Non autorisé.

HED80	Je souhaite partager ou envoyer des documents électroniques à des parties Internals.	Internal (Interne)/Confidential (confidentiel)	Les informations Internals/Confidential (confidentiel)les de BT peuvent être partagée uniquement avec les parties Internals qui doivent en disposer pour pouvoir exécuter leurs tâches, auquel cas : · le fait que l'e-mail contient des informations Internals/Confidential (confidentiel)les doit être clairement indiqué, · vous devez utiliser les paramètres de sensibilité pour indiquer qu'il s'agit d'un courriel « Confidential », · vous devez paramétrer les autorisations sur « Ne pas transférer ». **REMARQUE : les détails relatifs aux cartes de paiement ne doivent jamais être détenus sur un PC, mais s'ils doivent l'être ou s'ils doivent être envoyés par email, ils doivent être chiffrés en permanence.**
		Highly Confidential (Hautement confidentiel)	Les informations Highly Confidential (Hautement confidentiel)les de BT peuvent être partagé uniquement avec les parties Internals qui doivent en disposer pour pouvoir exécuter leurs tâches, auquel cas : · le fait que l'e-mail contient des informations Highly Confidential (Hautement confidentiel)les doit être clairement indiqué ; · vous devez utiliser les paramètres de sensibilité pour indiquer qu'il s'agit d'un courriel « Highly Confidential (Hautement confidentiel) » ; · vous devez, de préférence, paramétrer les autorisations sur « Ne pas transférer » ; · vous devez les envoyer par messagerie électronique sécurisée (si ce type de messagerie n'est pas disponible, les informations doivent être chiffrées).

			REMARQUE : les détails relatifs aux cartes de paiement ne doivent jamais être détenus sur un PC, mais s'ils doivent l'être ou s'ils doivent être envoyés par email, ils doivent être chiffrés en permanence.
HED90	Je souhaite partager ou envoyer des documents électroniques à une partie externe.	Toutes les données de BT	Les données peuvent être partagées ou envoyées à une partie externe uniquement si un besoin commercial approuvé ou un autre motif, comme un accord de confidentialité, justifient une telle démarche. · La diffusion ou l'envoi des données à une partie externe dépend strictement du besoin d'en connaître en cas de besoin commercial, contractuel ou légal approuvé et avec l'approbation de la partie prenante de BT. · Assurez-vous que le niveau de classification des données figure sur le document et les e-mails, quels qu'ils soient. · Vous devez veiller à ce que les parties externes soient informées du niveau de classification du document et conscientes des exigences liées à sa protection. · Les informations doivent être chiffrées. · Vous devez être sûr que le document aboutira à l'adresse de messagerie électronique à laquelle vous le destinez. · Quoi qu'il en soit, vous devrez toujours suivre les lignes directrices des privilèges juridiques, s'il y a lieu.
HED91	Je souhaite envoyer un e-mail à un large groupe d'employés de BT (100 ou plus) par exemple à des fins d'enquête auprès du personnel, de formation ou à propos d'avantages sociaux.	Internal (Interne)/Confidential (confidentiel)	Vous devez suivre notre guide destiné aux tiers sur les consignes de messagerie électronique.
		Highly Confidential (Hautement confidentiel)	Non autorisé.

HED100	Je souhaite transférer un document de BT ou des informations de BT, en Internal, sans recourir à la messagerie électronique, à Skype/Lync for Business ou à un support amovible (par exemple parce que le fichier est trop volumineux).	Toutes les données de BT	Vous pouvez recourir à un système de transfert électronique de fichiers dont l'utilisation a été approuvée par notre propre Politique de sécurité. Le document doit être chiffré à la source avant d'être transféré.
HED110	Je souhaite transférer un document de BT ou des informations de BT, en externe, sans recourir à la messagerie électronique, à Skype/Lync for Business ou à un support amovible (par exemple parce que le fichier est trop volumineux).	Internal (Interne)/Confidential (confidentiel)	Les données peuvent être diffusées ou envoyées à une partie externe uniquement si un besoin commercial approuvé ou un autre motif, comme un accord de confidentialité approuvé par une partie prenante de BT, justifient une telle démarche. · La diffusion ou l'envoi des données à une partie externe dépend strictement du besoin d'en connaître en cas de besoin commercial, contractuel ou légal approuvé et avec l'approbation de l'expéditeur ou du propriétaire du document. · Les données doivent être sécurisées dans l'environnement externe pour éviter toute perte de confidentialité, d'intégrité ou de disponibilité. · Les informations doivent être chiffrées avant d'être envoyées ou en cours de cheminement entre votre environnement et l'environnement externe. · Veillez à ce que le niveau de classification des données figure sur le document, quel qu'il soit. · Vérifiez que le document est envoyé au bon destinataire. · Recourez à un protocole de transfert standard, comme FTP.

		Highly Confidential (Hautement confidentiel)	Les données peuvent être diffusées ou envoyées à une partie externe uniquement si un besoin commercial approuvé ou un autre motif, comme un accord de confidentialité, justifient une telle démarche. · La diffusion ou l'envoi des données à une partie externe dépend strictement du besoin d'en connaître en cas de besoin commercial, contractuel ou légal approuvé et avec l'approbation de la partie prenante de BT. · Vous devez recourir au chiffrement total de bout en bout pour protéger les données de la source (votre système) à leur destination (le système externe) et au repos, lorsqu'elles sont arrivées sur le système tiers, conformément aux exigences de la norme applicable aux tiers Section 11. · Veillez à ce que le niveau de classification des données figure sur le document, quel qu'il soit. · Vérifiez que le document est envoyé au bon destinataire. · Recourez à un protocole de transfert standard, comme FTP.
HED120	Je souhaite faire une copie de sauvegarde de mes documents électroniques.	Toutes les données de BT	· Les documents de BT doivent être stockés uniquement sur des emplacements approuvés à cette fin par notre propre équipe INFOSEC, comme les lecteurs réseau ou systèmes de gestion de documents. (Si la seule solution consiste à utiliser un support amovible, le dispositif doit être chiffré). · Tous les contenus doivent être chiffrés ou protégés par mot de passe.

HED130	Je souhaite supprimer des documents électroniques.	Toutes les données de BT	Les documents détenus sur SharePoint et lecteurs réseau doivent être supprimés en utilisant la fonction de suppression standard de Windows. Les corbeilles doivent être vidées au moins une fois par semaine (cette consigne ne s'applique pas aux environnements Citrix par exemple arrière-guichet de vente au détail et centres d'appel offshore, dans la mesure où ils sont gérés automatiquement). Les e-mails qui ne sont plus nécessaire doivent être supprimés.
HED140	Je souhaite supprimer ou réutiliser un équipement informatique qui contenait des informations Confidentialles ou Highly Confidential (Hautement confidentiel)les de BT, par exemple des pièces, équipements tiers, sauvegardes, pièces de serveurs renvoyées à des fins de réparation.	Toutes les données de BT	Les services de déchiquetage peuvent être utilisés pour toutes sortes de médias et matériels, notamment pour les disques durs, bandes magnétiques, microfiches, CD/DVD, circuits imprimés, téléphonie mobile. Vous devez garder une trace des équipements détruits. Les services de suppression des données peuvent être utilisés pour les équipements destinés à être réutilisés. Vous devez garder une trace des équipements dont les données ont été supprimées et demander un certificat de suppression des données. S'agissant des équipements ayant contenu des données du gouvernement britannique, le Blanco **DOIT** être utilisé, dans la mesure où il s'agit du seul produit certifié.

HED150	Je souhaite supprimer des données système et d'application.	Toutes les données de BT	Les données doivent être effacées à un point rendant leur récupération impossible. En recourant de préférence à une méthode logicielle d'effacement de données (data erasure, data clearing, data wiping ou data destruction en anglais) pour écraser les données. Les copies de sauvegarde à conserver pour des raisons légales et réglementaires doivent être au-delà d'une utilisation quotidienne.

3.4 Manipulation des données systèmes et d'application (données électroniques)

Sont comprises dans les données électroniques, toutes les données et informations détenues dans les applications ou sur les systèmes gérés par le service Technologie ou individuellement par une unité d'entreprise, comme l'entrepôt de données ou un système de facturation, par exemple.
Les extraits de données reçus d'une application ou d'un système doivent être traités comme des documents électroniques (voir Section 6.3).

Référence	Que souhaitez-vous faire de ces données et informations ?	Catégorie de classification	Exigences de manipulation
HSADE	Je souhaite stocker et traiter des données et informations électroniques de BT dans un centre de données (tiers et Cloud inclus).	Toutes les informations de BT	Vous devez suivre les contrôles de la norme applicable aux tiers. Les données qui contiennent des informations se rapportant aux cartes bancaires doivent être détenues conformément aux exigences de la norme PCI DSS. Parce qu'elles sont particulièrement sensibles, les données parmi lesquelles figurent des données relatives aux comptes bancaires sont également soumises aux contrôles suivants : 1. Les comptes bancaires doivent être tokenisés pour les personnes (comptes en banque personnels des clients et employés). 2. Si les coordonnées bancaires doivent être montrées à un agent dans le cadre d'un processus d'entreprise (par exemple pour vérifier que les détails

			correspondent bien au compte sur lequel doit porter la facturation ou dans le cadre d'un échange de communications avec un client, notamment par e-mail ou sur une facture), seuls les quatre derniers chiffres du compte en banque doivent être visibles (coordonnées bancaires partiellement masquées). 3. Dans les cas où l'opération oblige à accéder à l'intégralité du compte bancaire (par exemple pour valider la requête de crédit ou de débit d'une banque), les coordonnées bancaires doivent être tokenisées ou déchiffrées puis communiquées à la banque par le biais d'un mécanisme de transport chiffré. Les coordonnées bancaires déchiffrées ou tokenisées doivent être supprimées immédiatement après avoir été utilisées.
HSAD1	Je souhaite stocker et traiter des données et informations de BT dans une application ou sur le système d'un tiers.	Toutes les données	· Les informations Confidentialles, Highly Confidential (Hautement confidentiel)les et à caractère personnel doivent être chiffrées. · Les informations relatives aux cartes de paiement doivent être chiffrées conformément aux exigences de la norme PCI DSS.
HSAD2	Je souhaite envoyer des données et informations de BT sur un réseau tiers ou par un autre canal externe.	Toutes les données de BT	Les informations doivent être couvertes par l'approbation d'une partie prenante de BT avant d'être envoyées. Le tiers concerné doit disposer d'un accord de confidentialité ou d'un contrat approprié. Le transfert de données doit être chiffré. Si des informations Confidentialles ou Highly Confidential (Hautement confidentiel)les, y compris des données à caractère personnel, doivent être envoyées au-delà des limites de votre réseau à un tiers, un accord de traitement des données doit être mis en place.

4. Conservation des données

Les tiers doivent avoir mis en place une politique de conservation des données, assortie d'un « Plan de conservation des données » spécifique définissant les périodes de conservation afférentes aux informations détenues par BT (la période de conservation doit être suffisamment longue pour permettre l'exécution du contrat, après quoi les données ne devraient pas être conservées plus de deux ans, 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).

Informations de BT : toutes formes d'enregistrement et de non-enregistrement papier ou numérique telles que les copies de travail, versions provisoires, notes informelles, courriers indésirables ou autres formes de stockage (telles que microfiches/microfilms, pellicules, cassettes audio ou vidéo).

5. Élimination des équipements

Tout équipement pouvant servir au stockage de données, composants d'ordinateurs inclus, doit être traité comme actif informatique. Le Glossaire ci-dessous fournit des exemples d'« actifs informatiques ».
Tout équipement arrivé à la fin de sa durée de vie utile doit être éliminé. Exemples de fin de vie des équipements :

- L'équipement est défectueux.
- L'équipement a été mis hors service (équipement retiré du service ou obsolète).
- L'équipement a servi dans le cadre d'un essai ou d'une preuve de concept.

5.1 Exigences des tiers en matière d'élimination.

Ces exigences s'appliquent :

- À tout tiers ou agence en sous-traitance.
- À tout tiers chargé d'exécuter des services de maintenance sur un équipement de BT dans le cadre desquels des actifs informatiques sont susceptibles d'être retirés et remplacés.
- À tout tiers s'acquittant de services externalisés auprès de BT et dans le cadre desquels des données de BT résident dans un équipement ou dans les archives du tiers.
- À toute agence d'élimination des déchets se chargeant de l'élimination des équipements de BT.

Référence	Que souhaitez-vous faire de ces données et informations ?	Catégorie de classification	Exigences de manipulation

EDR10	Je souhaite éliminer des équipements contenant des données de BT.	Toutes les données de BT	Disques durs (HDD) : effacement multi-passes successives, désintégration ou incinération.
			Disques SSD : effacement multi-passes successives, désintégration.
			CD-R / DVD-R, CD-RW / DVD-RW, BD-R, BD-RE, BD-RE : abrasion, désintégration, incinération.
			Bande magnétique : démagnétisation, désintégration, incinération.
			Mémoires flash et clés USB : effacement multi-passes successives, démagnétisation, désintégration.
			SIMS : découpage en plusieurs morceaux (notamment à travers le contact métallique) pour les rendre illisibles.

6. Exigences d'audit

6.1 Exigences d'audit relatives à l'élimination des données et informations

La conservation des données et leur élimination doivent faire l'objet d'un enregistrement détaillé qui servira de piste d'audit, de preuve et de moyen de suivi. Elle doit notamment inclure :

- Une preuve de destruction et/ou d'élimination (y compris la date d'exécution et 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).

6.2 Exigences d'audit relatives à l'élimination des équipements

Une piste d'audit doit être fournie pour les types d'équipements suivants :

- Supports amovibles ;
- Lecteurs de disque ;
- Bandes de sauvegarde ;
- Composant d'ordinateur (cf. glossaire).

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 la destruction et/ou de l'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.

7. Glossaire

Terme	Explication
Tiers	Toute entreprises amenées à traiter des données/informations de BT et à manipuler les équipements de BT doivent se conformer à cette norme. Cela comprend notamment : · Tous les tiers ou agence en sous-traitance, · Tout tiers chargé d'exécuter des services de maintenance sur un équipement de BT dans le cadre desquels des actifs informatiques sont susceptibles d'être retirés et remplacés, · Tout tiers s'acquittant de services externalisés auprès de BT et dans le cadre desquels des données de BT résident dans un équipement ou dans les archives du tiers, · Toute agence d'élimination des déchets se chargeant de l'élimination des équipements de BT.
AES	Norme de chiffrement avancé (Advanced Encryption Standard)
Clés asymétriques	Également appelé chiffrement à clé publique, le chiffrement asymétrique chiffre et déchiffre les données en utilisant des clés publiques et privées. Les clés sont de grands numéros appairés, mais non identiques (asymétriques). Une clé de la paire, la clé publique, peut être partagée.
Données de BT	Toutes données appartenant à BT ou détenues sous licence par BT dans le cadre d'une exploitation de type société à responsabilité limitée au R.-U. ou dans l'une de ses filiales internationales.
CDP	Point de distribution de liste de révocation de certificats (Certificate Revocation List Distribution Point).
CESG	Groupe de sécurité des communications électroniques du gouvernement britannique.

Composant d'ordinateur	Contrôleurs de disque dur, contrôleurs de lecteur CD-ROM, contrôleurs lecteur DVD, cartes d'interface Ethernet, contrôleurs d'écran d'ordinateur et imprimantes réseau.
CRL	Liste de révocation de certificats (Certificate Revocation List)
Client	Personne ou organisation obtenant, ayant obtenu ou considérées par BT ou ses marques comme étant susceptible d'obtenir des produits, de recevoir des offres de produits et services.
Données de clients	Toute donnée se rapportant aux clients des marques exploitées par BT.
Données	Mots, nombres, dates, images, sons, etc. sans contexte.
Élimination des données	L'élimination des données concerne la destruction des données et informations non classées parmi les enregistrements permanents.
Cycle de vie des données	Le cycle de vie des données couvre les méthodes de collecte, de stockage, de manipulation, de traitement, de transmission et de destruction des données.
Période de conservation des données	Il s'agit de la période (qui peut être permanente) pendant laquelle un type de données ou d'informations est détenu/stocké avant de pouvoir être détruit ou éliminé. Pendant cette période les données peuvent être archivées du moment qu'elles restent accessibles jusqu'à l'expiration de la période de conservation des données.
DEK	Clé de chiffrement de données
Données électroniques	Désigne toutes les données et informations détenues dans les applications ou sur les systèmes gérés par le service Technologie ou par une unité d'entreprise individuelle, par exemple un entrepôt de données ou un système de facturation.
Clés à courbe elliptique	Cryptographie sur les courbes elliptiques. La cryptographie sur les courbes elliptiques (Elliptic Curve Cryptography ou ECC) est une approche basée sur la structure algébrique des courbes elliptiques sur champs finis. L'ECC se contente de clés moins longues par rapport à la cryptographie non-EC (basée sur des corps de Galois) pour une sécurité équivalente.
Chiffrement	Conversion de données en codes secrets ne pouvant pas être lus par les personnes non autorisées.
Entropie	Mesure du caractère aléatoire des données ; une clé de 128 bits peut avoir jusqu'à 128 bits d'entropie ou un seul.
GCM	Messagerie Cloud Google.
HSM	Modules de sécurité du matériel.
Enregistrement inactif	Un enregistrement peut être à l'état actif ou inactif. Lorsqu'un enregistrement a expiré ou n'est plus nécessaire, par exemple si un client quitte BT, son enregistrement devient inactif. De même, si un employé quitte BT, son enregistrement auprès du service des RH devient inactif.
Informations	Groupe de mots, chiffres, nombres, dates, images, sons, etc. contextualisés (par exemple pour leur donner du sens).

Commented [MD1]: "Bit" is masculine.

Actifs informatiques	Tout équipement pouvant servir au stockage de données constitue un « actif informatique ». Les éléments suivants en font partie : les lecteurs de disque (SSD et magnétiques), supports amovibles (par exemple les disquettes, clés USB, DVD, CD, cartes mémoire Internals, mémoires flash et cartes SD), bandes de sauvegarde, cartes SIM de téléphones portables. Les composants d'ordinateur tels que les contrôleurs de disque dur, contrôleurs de lecteur CD-ROM, contrôleurs lecteur DVD, cartes d'interface Ethernet, contrôleurs d'écran d'ordinateur et imprimantes réseau.
Systèmes d'information	Ensemble de matériels, logiciels, données, personnes et procédures œuvrant de concert pour produire des informations de qualité.
KEK	Clé de chiffrement de clé.
NDA	Accord de confidentialité (Non-Disclosure Agreement).
NIST	Institut national des normes et technologies
Nonce	Valeur unique générée aléatoirement et utilisée une seule fois au cours d'un échange cryptographique, souvent à des fins d'authentification.
Non-enregistrements	Duplicatas d'originaux et de copies de travail. Documents Internals se rapportant à des questions non-commerciales. Ébauches de lettres, rapports, feuilles de travail et notes informelles. Livres, manuels et autres supports imprimés provenant de sources externes à BT et servant de documentation de référence. Spam et courrier indésirable.
OCSP	Protocole de vérification de certificat en ligne (Online Certificate Status Protocol)
Bureau	Désigne tout local de BT et notamment ses magasins, centres d'appel, son siège social et site d'échange.
Détails relatifs aux cartes de paiement	Désigne les informations se rapportant au compte utilisé par le titulaire d'une carte pour payer un fournisseur. Il s'agit notamment du numéro de paiement du compte (PAN), de la date d'expiration, du code de vérification (CVV). Elles sont régies par la réglementation afférente à la norme PCI/DSS.
Données à caractère personnel	Informations se rapportant à toute personne physique, notamment les noms et prénoms, dates de naissance, adresses, numéros de téléphone y compris de clients et de toute personne travaillant pour BT.
PRNG	Générateurs de nombres pseudo-aléatoires (Pseudo-random number generators)
Enregistrements	Documents conservés comme preuves des transactions, décisions, activités, e-mails de BT ou pour satisfaire à des obligations légales. Cela comprend également les données et informations détenues dans les systèmes et applications, dans la mesure où elles attestent aussi des transactions commerciales, produits et services EE.
RSA	Technologie de chiffrement à clé publique développée par RSA Data Security, Inc. L'acronyme est constitué des initiales de ses trois inventeurs, nommément Rivest, Shamir et Adelman.

Hash salés	En cryptographie, le sel est une donnée aléatoire ajoutée à une fonction unidirectionnelle pour hacher un mot de passe ou une phrase de chiffrement secrète. Consulter l'annexe C pour de plus amples informations.
Clés symétriques	Les algorithmes à clés symétriques sont des algorithmes de cryptographie utilisant les mêmes clés de chiffrement pour le chiffrement de texte en clair et le déchiffrement de texte chiffré.
Politique de conservation niveau système	Une politique niveau système indique combien de temps le système doit conserver les données pour respecter les plans de conservation des données de l'entreprise.
TPM	Module de plateforme sécurisée (Trusted Platform Module)

8. Historique des modifications

N° de version	Date	Modification apportée par	Brefs détails de la modification
Avant-projet 4.0	05/08/2018	Karen Tanner	Avant-projet de remplacement de la version 3 actuelle
4.0 publié	07/11/2019	Karen Tanner	Révisé et validé

9. Validation du document

Nom	Fonction	Date
Ian Morton	Propriétaire de la version du document BT	07/11/2019

10. Conformité

La plupart des tiers se comportent de manière professionnelle et en adéquation avec les valeurs de BT. Si toutefois vous vous comportiez d'une manière non conforme à cette norme, à d'autres politiques ou normes, BT pourrait se voir contraint de ne plus faire appel à vos services.

11. Propriété et confidentialité

Ce document ne doit pas être partagé avec tout autre tiers sans le consentement écrit de BT. BT reste propriétaire de cette norme et de toute documentation connexe, qui doivent lui être restituées sur simple demande.