Annexe 1 Classification des informations

Introduction

Au sein de BT, un Chargé d'activités BT est propriétaire de toutes les données et les informations et il est responsable d'attribuer une classification au document ou aux données.

Les données et les informations doivent être protégées par tous les utilisateurs qui entrent en contact avec elles. En tant qu'utilisateur des informations de BT, vous avez la responsabilité de respecter les contrôles de la classification de sécurité prescrits par le présent document et les quelconques exigences spécifiques à un projet, prévues par BT. Vous ne devez utiliser le document ou les données qu'aux fins prévues et obtenir le consentement du propriétaire des données si vous voulez autoriser d'autres personnes à les consulter.

Si vous recevez des informations de BT qui n'ont pas reçu de classification, vous devez contacter l'expéditeur ou votre responsable BT, afin d'en confirmer la classification, sinon contactez la Sécurité BT conformément aux Exigences de sécurité Annexe 3.

N.B. Si vous avez accès au Réseau local Greenside de BT (BT Greenside Local Area Network ou LAN) ou que vous devez créer des documents pour BT, qui contiendront des informations de BT, vous devrez consulter la Politique relative à la sécurité 4, sinon les principes suivants s'appliqueront

Classification des informations

Il existe 4 classes d'informations :

- Document public
- Document interne
- Document confidentiel
- Document strictement confidentiel

Document public

Ces informations publiques ne nécessitent aucun contrôle ou sont destinées à être mises à la disposition du grand public.

Document interne

Les informations internes sont mises à la disposition des employés de BT et d'autres personnes qui sont autorisées à accéder au réseau d'informations, sans que cet accès présente des risques particuliers pour BT.

Document confidentiel

Les informations confidentielles sont destinées à un groupe de personnes spécifique : le principe du « besoin d'en connaître » (contrôles de l'accès) est appliqué à la lettre. La communication de documents confidentiels sans autorisation peut nuire à la réputation de BT ou aux employés.

Par exemple :

- des données personnelles sur des personnes qui peuvent être des employés de BT, des tiers ou des clients ;
- des données électroniques des systèmes ;
- des données relatives aux ventes et au marketing ;
- des plans d'affaires locaux ;
- des données sur les risques ;
- des mots de passe ;
- des informations qui sont confidentielles conformément à la loi.

Ensemble de documents confidentiels multiples

Si vous avez un ensemble de documents confidentiels en un seul lieu, il faudra éventuellement leur affecter une classification supérieure. Cela pourrait entraîner la modification de la classification de documents individuels en Documents strictement confidentiels ou nécessiter des mesures de sécurité supplémentaires pour sécuriser le lieu si :

- ensemble, ils pourraient causer de graves dommages à BT, en cas de fuite ;
- ils étaient associés à d'autres données, par exemple un nom et une adresse et/ou il existait de nombreuses coordonnées bancaires dans un système, ils pourraient constituer une cible très intéressante.

Si vous avez des inquiétudes à propos des informations en votre possession, veuillez consulter votre contact BT.

Document strictement confidentiel

Les documents et les données strictement confidentiels ont une liste de distribution définie, où le nombre de personnes est limité ; le principe du « besoin d'en connaître » est appliqué à la lettre (vous devez savoir qui possède une copie et qui peut les consulter). Une communication sans autorisation pourrait causer de graves dommages à BT. Vous devez étudier soigneusement la classification de documents dans la catégorie Strictement confidentiels, car celle-ci exige les contrôles de sécurité les plus stricts.

Contrôles de sécurité

Termes définis :

Chiffrement

Exigences minimales :

- Utiliser le chiffrement AES 256 bits.
- Les clés symétriques doivent être d'une longueur minimale de 256 bits.
- Les clés asymétriques (par ex. RSA) doivent avoir une longueur d'au moins 2048 bits.
- Utiliser uniquement des clés cryptographiques connues et fiables.
- Ne pas utiliser des certificats auto-signés.

Mot de passe ou phrase de passe (pour le chiffrement)

Ils ne doivent pas être faciles à deviner (c.-à-d. aussi aléatoire que possible, sans rapport avec l'identifiant de l'utilisateur, l'utilisateur, son identité, une date, etc.) et ils ne doivent pas être faciles à découvrir au moyen d'un dictionnaire de mots de passe couramment utilisés. Toutefois, ils doivent contenir au moins :

- 8 caractères
- Deux des caractères suivants :
  - non alphanumériques, par ex. (!, £,", $, %,^, &,*, (,), -,_, +, =, :, `, @, ~, #, ?, <, >,)
  - nombre décimal : (0... 9)
  - lettre majuscule : (A... Z)
- Les clés privées doivent être protégées par une phrase de passe, composée d'un mélange des caractères alphanumériques et des symboles définis ci-dessus.

NB : afin d'éviter toute ambiguïté, toutes les exigences contractuelles spécifiques à un client prescrites dans un contrat avec un client, qui prévoient un niveau de sécurité plus élevé, l'emporteront sur les contrôles suivants.

	Contrôles de sécurité	Document interne	Document confidentiel	Document strictement confidentiel
1	**Loi nationale sur la protection des données - Données personnelles et**	Ces données ne doivent pas être traitées comme des documents internes. Protéger	Protéger les dossiers individuels comme des documents confidentiels.	Protéger les dossiers multiples comme des documents strictement confidentiels.

	sensibles	les dossiers individuels comme des documents confidentiels.		
2	**Contrôle de la distribution des documents commerciaux (Word, Excel, etc.) et suivi des mouvements**	Le contrôle et le suivi ne sont pas exigés. Inscrire la mention « **DOCUMENT INTERNE BT** » sur chaque page ou « **DOCUMENT INTERNE OPENREACH** » si le document ne peut être partagé que sur Openreach.	Inscrire la mention « **DOCUMENT CONFIDENTIEL** » sur chaque page du document et veiller à respecter le « **principe du besoin d'en connaître** » ; envisager d'utiliser une **liste de distribution.** Le chiffrement est exigé conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.	Inscrire la mention « DOCUMENT STRICTEMENT CONFIDENTIEL » sur chaque page du document. Inclure dans le document une **liste de distribution** des personnes concernées. Le propriétaire doit veiller au respect du « **principe d'en connaître** ». Le chiffrement au moyen d'un logiciel respectant les termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus est obligatoire avant le stockage de données sur un PC/ordinateur portable qui n'est pas fourni par BT, avec un chiffrement du disque dur, c.-à-d. support amovible. Le même principe s'applique aux messages électroniques envoyés à quiconque, employé de BT ou pas.
3	**Stockage sécurisé sur un ordinateur portable et un PC**	Le stockage sécurisé est obligatoire, par ex. PGP, WinZip 9.	Chiffrement intégral du disque dur conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.	Chiffrement intégral du disque dur conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.
4	**Stockage sécurisé sur un serveur et des bases de donnée (fixe - disque/bande)**	Stockage sécurisé pas nécessaire si conforme à toutes les exigences de sécurité physiques de stockage autrement sécurisé est nécessaire par exemple PGP,	Les informations de BT doivent être chiffrées conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.	Les informations de BT doivent être chiffrées conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.

		WinZip 9		
5	**Stockage sécurisé sur Blackberry, Windows Mobile, autres PDA, tablettes (iPad, etc.), téléphones portables et lecteurs MP3**	Il est interdit de stocker des documents internes sur ce type d'appareil, sauf s'il est fourni par BT ou qu'une concession est approuvée par le service Sécurité BT. Ces appareils ne doivent pas être configurés de sorte à permettre d'accéder aux messageries électroniques BT.com (il est autorisé d'accéder à la messagerie électronique BT.com via Webmail).	Il est interdit de stocker des documents confidentiels sur ce type d'appareil, sauf s'il est fourni par BT ou qu'une concession est approuvée par le service Sécurité BT. Ces appareils ne doivent pas être configurés de sorte à permettre d'accéder aux messageries électroniques BT.com (il est autorisé d'accéder à la messagerie électronique BT.com via Webmail).	Il est interdit de stocker ISC sur ces appareils.
6	**Stockage sécurisé sur :** **un support amovible tel qu'une clé USB, une mémoire flash, CD/DVD, des disques durs USB, des cartes numériques sécurisées, une disquette ou d'autres dispositifs semblables.**	Les informations de BT doivent être chiffrées conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus quand elles sont stockées sur de tels dispositifs.	Les informations de BT doivent être chiffrées conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus quand elles sont stockées sur de tels dispositifs.	Il est interdit de stocker ISC sur ces appareils.
7	**Stockage sur le Web/en ligne ou une quelconque installation de stockage Internet**	Interdit	Interdit	Interdit
8	**Collaboration externe sur le Web**	N'importe quelle plateforme MS Live Meeting ou Webjoin	Interdit	Interdit

9	**Envoi par message électronique**	Le chiffrement n'est pas nécessaire.	Chiffrement pour les destinataires (si la destination n'est pas une adresse électronique bt.com) selon les termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.	Le chiffrement est exigé conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.
10	**Transfert automatique des messages électroniques**	Interdit	Interdit	Interdit
11	**Transmission sur le réseau**	Le chiffrement n'est pas nécessaire.	Chiffrement pour les transmissions externes et internes conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.	Chiffrement pour les transmissions externes et internes conformément aux termes « Chiffrement » et « Mot de passe/phrase de passe » définis ci-dessus.
12	**Transfert de fichiers**	Utiliser le transfert de fichiers sécurisé, par ex. SFTP, XFB.	Utiliser le transfert de fichiers sécurisé, par ex. SFTP, XFB.	Utiliser le transfert de fichiers sécurisé, par ex. SFTP, XFB.
13	**Effacer / supprimer des données**	Utiliser les fonctions de suppression des applications ou du système d'exploitation.	Assainir les données en écrasant chaque secteur par des chaînes de données binaires aléatoires au moins une fois au moyen d'un logiciel, par ex. Blanco HMG Edition ou Blanco Version 5 pour des disques durs SSD.	Assainir les données en écrasant chaque secteur par des chaînes de données binaires aléatoires au moins une fois au moyen d'un logiciel, par ex. Blanco HMG Edition ou Blanco Version 5 pour des disques durs SSD.
14	**Mise au rebut ou réutilisation du matériel informatique (contenant des informations BT)** **Y compris, sans exclusivité toutefois :** **- la mise au rebut des pièces** **- la destruction des équipements provenant du**	Utiliser une solution logicielle vérifiable et testée pour l'effacement, produisant un certificat officiel confirmant que les données sont effacées. Si l'effacement échoue sur un matériel, celui-ci doit être détruit et un certificat officiel doit être reçu/fourni, indiquant au minimum le numéro de série du matériel, comme preuve de	Les disques (ou les autres supports de stockage, y compris mais sans exclusivité les cartes mémoires de type flash, les disques durs SSD) doivent être assainis en écrasant chaque secteur par des chaînes de données binaires aléatoires au moins une fois au moyen d'un logiciel, par ex. Blanco HMG Edition ou Blanco Version 5 pour des disques durs SSD.	Les disques (ou les autres supports de stockage, y compris mais sans exclusivité les cartes mémoires de type flash, les disques durs SSD) doivent être assainis en écrasant chaque secteur par des chaînes de données binaires aléatoires au moins une fois au moyen d'un logiciel, par ex. Blanco HMG Edition ou Blanco Version 5 pour des disques durs SSD.

	fournisseur **- les exigences de destruction pour les sauvegardes** **- les pièces de serveur qui sont renvoyées au fabricant pour réparation**	sa mise au rebut. La solution suscitée ne peut pas être utilisée sur un disque dur SSD, qui doit être détruit et pour lequel il faut recevoir/fournir un certificat officiel. Consulter la norme BS EN 17513 pour un complément d'information.	Si l'assainissement n'est pas réalisable ou n'est pas approprié, le disque (ou les autres supports de stockage, y compris mais sans exclusivité les cartes mémoires de type flash, les disques durs SSD) doit être détruit au moyen d'une méthode de destruction des disques. Un certificat officiel doit être produit pour vérifier que les données ont été effacées ou que le support a été détruit.	Si l'assainissement n'est pas réalisable ou n'est pas approprié, le disque (ou les autres supports de stockage, y compris mais sans exclusivité les cartes mémoires de type flash, les disques durs SSD) doit être détruit au moyen d'une méthode de destruction des disques. Un certificat officiel doit être produit pour vérifier que les données ont été effacées ou que le support a été détruit.
15	**Impression**	Il faut utiliser une imprimante branchée sur le PC ou être présent à l'imprimante en réseau au moment de l'impression.	Utiliser une imprimante contrôlée par un code PIN, une imprimante branchée sur le PC ou une imprimante se trouvant dans une salle sécurisée avec contrôle d'accès. Vérifier soigneusement vers quelle imprimante l'impression est dirigée et ne jamais laisser les documents dans le bac d'impression.	Utiliser une imprimante contrôlée par un code PIN, une imprimante branchée sur le PC ou une imprimante se trouvant dans une salle sécurisée avec contrôle d'accès. Prêter attention lors de l'impression. Vérifier soigneusement vers quelle imprimante l'impression est dirigée et ne jamais laisser les documents dans le bac d'impression.
16	**Services postaux/de messagerie entre BT et le fournisseur**	Enveloppe simple.	Utiliser deux enveloppes et envoyer en recommandé uniquement au destinataire. Ne pas indiquer la mention « Document confidentiel » sur la 1ère enveloppe.	Utiliser deux enveloppes et envoyer en recommandé uniquement au destinataire. Ne pas indiquer la mention « Document strictement confidentiel » sur la 1ère enveloppe.
17	**Divulgation à l'extérieur**	Demander l'autorisation du Contact Sécurité BT. Cf. l'annexe 3.	Demander l'autorisation du Contact Sécurité BT. Cf. l'annexe 3.	Demander l'autorisation du Contact Sécurité BT. Cf. l'annexe 3.

18	**Document utilisé dans le cadre d'une formation, d'un développement ou de tests**	Il doit être rendu anonyme par BT et être conforme au guide des bonnes pratiques d'Anonymisation des données de BT BP001.	Il doit être rendu anonyme par BT et être conforme au guide des bonnes pratiques d'Anonymisation des données de BT BP001.	Interdit
19	**Destruction des documents sous format papier**	Déchiquetés au moyen d'un déchiqueteur à coupe croisée.	Déchiquetés au moyen d'un déchiqueteur à coupe croisée.	Déchiquetés au moyen d'un déchiqueteur à coupe croisée à une dimension de 4 x 15 mm.
20	**Lieux publics**	Ne jamais parler en public des informations internes.	Ne jamais parler en public des informations confidentielles. Ne jamais travailler sur des documents dans des lieux publics où d'autres personnes pourraient les voir.	Ne jamais parler en public des informations strictement confidentielles. Ne jamais travailler sur des documents dans des lieux publics.