POLITIQUE BRING YOUR OWN DEVICE (BYOD)

<table>
<thead>
<tr>
<th>Code:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
</tr>
<tr>
<td>Date de la version:</td>
</tr>
<tr>
<td>Créé par:</td>
</tr>
<tr>
<td>Approuvée par:</td>
</tr>
<tr>
<td>Niveau de confidentialité:</td>
</tr>
</tbody>
</table>

Comment [DK1]: Tous les champs dans ce document marqués avec des crochets [ ] doivent être remplis.

Comment [DK2]: Le système de codage des documents devraient être aligné avec le système existant de l'organisation pour la codification des documents; au cas où un tel système n'est pas en place, cette ligne peut être supprimée.
Historique des modifications

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Créé par</th>
<th>Description de la modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>JJ-MM-AAAA 0.1</td>
<td>Dejan Kosutic</td>
<td>Structure documentaire de base</td>
<td></td>
</tr>
</tbody>
</table>

Table des matières

1. BUT, DOMAINE D’APPLICATION ET AUDIENCE ................................................................. 3

2. DOCUMENTS REFERENCES ........................................................................................................ 3

3. REGLES DE SECURITE POUR L’UTILISATION DE BYOD ....................................................... 3
   3.1. POLITIQUE DE LA COMPAGNIE ....................................................................................... 3
   3.2. QUI EST AUTORISE A UTILISER DES BYOD ET POUR QUOI ........................................ 3
   3.3. QUELS APPAREILS SONT AUTORISES ............................................................................. 3
   3.4. UTILISATION ACCEPTABLE ............................................................................................. 3
   3.5. DROITS SPECIAUX ........................................................................................................... 4
   3.6. REMBOURSEMENT ........................................................................................................... 4
   3.7. FAILLES DE SECURITE ................................................................................................... 5
   3.8. FORMATION ET SENSIBILISATION .................................................................................. 5

4. GESTION DES ENREGISTREMENTS CONSERVES SUR LA BASE DE CE DOCUMENT ......... 5

5. VALIDITE ET GESTION DOCUMENTAIRE ............................................................................. 5
1. **But, domaine d'application et audience**

Le but de ce document est de définir comment [nom de l'organisation] conservera le contrôle sur ses informations alors que ces informations sont accessibles par des dispositifs qui ne sont pas détenus par l'organisation.

Ce document est appliqué à tous les appareils appartenant à des particuliers qui ont la capacité de stocker, transférer ou traiter des informations sensibles du domaine d'application du Système de Management de la Sécurité de l'Information (SMSI). Ces dispositifs comprennent les ordinateurs portables, les smart phones, les tablettes, les clés de mémoire USB, les appareils photo numériques, etc. Ces dispositifs seront appelés BYOD dans cette politique.

L’audience de ce document est l’ensemble des employés de [nom de l’organisation].

2. **Documents référencés**

- Norme ISO/IEC 27001, clauses A.6.2.1, A.6.2.2, A.13.2.1

3. **Règles de sécurité pour l'utilisation de BYOD**

pour un usage privé, ou qu’ils soient utilisés à l’intérieur ou à l’extérieur des locaux de l’organisation.

3.1. **Politique de la compagnie**

[nom de l’organisation] prend en charge l’utilisation généralisée de BYOD dans le travail - par

Les données de l’entreprise stockées, transférées ou traitées par des BYOD restent sous la propriété propriétaire de l’appareil.

3.2. **Qui est autorisé à utiliser des BYOD et pour quoi**

[titre du poste] créera une liste de postes et/ou de personnes autorisés à utiliser des BYOD, ainsi que

[titre du poste] créera une liste d’applications BYOD prohibées.

3.3. **Quels appareils sont autorisés**

ainsi que les **paramètres obligatoires** pour chaque appareil.

3.4. **Utilisation acceptable**

- [décrire comment la sauvegarde des informations de l’entreprise doit être faite]

Comment [DK3]: Alternativement, il est mesure d'effectuer le travail autrement.

Comment [DK4]: Par exemple, pare-feu, sauvegarde, verrouillage d'écran, etc.
Éviter toute logistique de mise à disposition, e.g. conserver logiciel non-utilisé, prévention d'intrusion, logiciel de gestion des appareils mobiles, etc.

[drug] méthode de connexion sécurisée [au réseau de l'entreprise]

être laissés sans surveillance, et de préférence être physiquement enfermés

des correctifs et des mises à jour doivent être installés régulièrement

[Politique de classification des informations]

BYOD soient mis au rebut, vendus, ou remis à un tiers pour entretien

Il est interdit de faire ce qui suit avec un BYOD:

permettre l'accès à quiconque, excepté à l'employé propriétaire de l'appareil

installer des logiciels sans licences d'utilisation

stocker localement des mots de passe, sauf lorsque vous utilisez les applications suivantes:

transférer les données de l'entreprise à d'autres appareils qui ne sont pas autorisés

3.5. Droits spéciaux

[nom de l'organisation] a le droit de voir, modifier et supprimer toutes les données de l'entreprise qui sont stockées, transférées ou utilisées sur les BYOD. Politique et à surveiller son utilisation via [spéfier le nom du logiciel de gestion des appareils mobiles].

[nom de l'organisation] a le droit de procéder à une suppression de l'ensemble des données sur les BYOD. Le logiciel ne payera aucun frais à ses employés (les propriétaires de BYOD) pour l'utilisation des logiciels à des fins de travail.

[nom de l'organisation] paiera pour les points suivants:

• Tout nouveau logiciel qui doit être installé pour les besoins de l'entreprise.
3.7. Failles de sécurité

Toutes les failles de sécurité liées à des BYOD doivent être immédiatement signalées à [titre du poste]. En outre, toutes les failles qui ne sont pas un exemple d’une variété de incidents, doivent être signalées par les mêmes canaux dans un jour ouvrable.

3.8. Formation et sensibilisation

[titre du poste] est en charge de la formation des employés nouveaux et existants sur l’utilisation appropriée des BYOD, ainsi que de la sensibilisation sur les menaces les plus courantes.

4. Gestion des enregistrements conservés sur la base de ce document

<table>
<thead>
<tr>
<th>Nom de l’enregistrement</th>
<th>Lieu de conservation</th>
<th>Personne responsable de la conservation</th>
<th>Mesures pour la protection des enregistrements</th>
<th>Temps de rétention</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Liste des postes et/ou de personnes autorisés de BYOD et ce à quoi ils peuvent accéder]</td>
<td>[intranet de l’entreprise]</td>
<td>[titre du poste]</td>
<td>Seul [titre du poste] peut modifier et publier une nouvelle version de la Liste</td>
<td>Une liste qui n’est plus valide doit être archivée pendant 3 ans</td>
</tr>
<tr>
<td>[Liste des dispositifs BYOD acceptables et de leurs paramètres]</td>
<td>[intranet de l’entreprise]</td>
<td>[titre du poste]</td>
<td>Seul [titre du poste] peut modifier et publier une nouvelle version de la Liste</td>
<td>Une liste qui n’est plus valide doit être archivée pendant 3 ans</td>
</tr>
<tr>
<td>[Liste d’applications BYOD prohibées]</td>
<td>[intranet de l’entreprise]</td>
<td>[titre du poste]</td>
<td>Seul [titre du poste] peut modifier et publier une nouvelle version de la Liste</td>
<td>Une liste qui n’est plus valide doit être archivée pendant 3 ans</td>
</tr>
</tbody>
</table>

5. Validité et gestion documentaire

Ce document est valide dès le [date].

Le propriétaire de ce document sur [titre du poste], qui doit veiller à ce nécessaire mettre à jour le document au moins une fois par an. [titre du poste] examinera la Liste des postes et/ou de personnes autorisés, la Liste des dispositifs acceptables, et la Liste des applications prohibées tous les 3 mois.
Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés:

- ...
- le nombre d'employés utilisant un BYOD sans autorisation

[titre du poste]
[nom]

[signature]

Comment [DK14]: Nécessaire uniquement si la procédure de contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.