[Logo de l'organisation]

Commented [AES1]: Remplissez tous les champs entre crochets [ ] dans ce document.

[Nom de l'organisation]

POLITIQUE BRING YOUR OWN DEVICE (BYOD)

Commented [AES2]: Pour en savoir plus sur ce sujet, consultez cet article :

What is a BYOD policy, and how can you easily write one using ISO 27001 controls?
https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/

Code :	
Version :	
Date de la version :	
Créé par :	
Approuvée par :	
Niveau de confidentialité :	

Commented [AES3]: Le système de codage des documents doit 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

Date	**Version**	**Crée par**	**Description de la modification**
	0.1	Advisera	Structure documentaire de base

Table des matières

1. But, domaine d'application et utilisateurs

Ce document a pour but de définir comment [nom de l'organisation] conservera le contrôle sur ses informations, alors que ces informations sont accessibles par l'intermédiaire d'équipements qui n'appartiennent pas à l'organisation.

Commented [AES4]: Indiquez le nom de votre organisation.

Ce document s'applique à tous les équipements personnels des employés qui permettent de stocker, transférer ou traiter des informations sensibles du domaine d'application du Système de management de la sécurité de l'information (SMSI). Ces équipements comprennent les ordinateurs portables, les smartphones, les tablettes, les clés de mémoire USB, les appareils photo numériques, etc. Ces équipements seront dénommés BYOD dans la présente Politique.

Les utilisateurs de ce document sont l'ensemble des employés de [nom de l'organisation].

Commented [AES5]: Indiquez le nom de votre organisation.

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.14, A.6.7 et A.8.1

3. Règles de sécurité pour l'utilisation de BYOD

Les règles de la présente Politique s'appliquent à tous les BYOD, qu'ils soient utilisés à des fins professionnelles ou personnelles, ou qu'ils soient utilisés à l'intérieur ou à l'extérieur des locaux de l'organisation.

3.1. Politique de l'entreprise

[Nom de l'organisation] prend en charge l'utilisation généralisée de BYOD à des fins professionnelles – c'est-à-dire en utilisant de tels équipements dans le but de réaliser un travail pour l'organisation.

Commented [AES6]: Indiquez le nom de votre organisation.

Commented [AES7]: Autrement, vous pouvez indiquer : [redacted]

[redacted]

3.2. Qui est autorisé à utiliser des BYOD et dans quel but

[Titre du poste] créera une Liste de titres de poste et / ou de personnes autorisées à utiliser des BYOD, ainsi que les applications et les bases de données auxquelles ils ont le droit d'accéder avec leurs équipements personnels.

[redacted]

3.3. Quels équipements sont autorisés

[Titre du poste] créera une Liste des équipements autorisés et pouvant servir de BYOD, ainsi que des paramètres obligatoires pour chaque équipement.

Commented [AES8]: Par ex. pare-feu, sauvegarde, verrouillage d'écran, etc.

3.4. Utilisation acceptable

Pour chaque BYOD, les points suivants sont obligatoires :

- [décrire comment la sauvegarde des informations de l'organisation doit être réalisée]
- [décrire quels logiciels de sécurité doivent être installés - par exemple logiciel anti-virus, prévention d'intrusion, logiciel de gestion des appareils mobiles, etc.]
- [décrire le procédé de cryptage qui doit être utilisé et dans quel but]
- [décrire la méthode d'authentification qui doit être utilisée]
- [décrire la méthode de connexion sécurisée au réseau de l'organisation]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Commented [AES9]: Par ex. mots de passe, codes d'accès, [illegible]

Commented [AES10]: Par ex. VPN.

Commented [AES11]: Doit être supprimé si cette Politique n'existe pas.

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

- permettre l'accès à toute personne autre que l'employé propriétaire de l'équipement
- installer des applications énumérées dans la Liste d'applications interdites aux BYOD
- conserver du contenu illégal sur l'équipement
- installer des logiciels sans licences d'utilisation
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

3.5. Droits spéciaux

[Nom de l'organisation] dispose du droit de consulter, modifier et supprimer toutes les données de l'organisation qui sont stockées, transférées ou traitées sur des BYOD.

Commented [AES12]: Indiquez le nom de votre organisation.

[Titre du poste] est autorisé à configurer tous les BYOD conformément à la présente Politique et à contrôler leur utilisation via [indiquer le nom du logiciel de gestion des appareils mobiles].

Commented [AES13]: Supprimez cet élément si vous n'utilisez [illegible]

[illegible]

Commented [AES14]: Indiquez le nom de votre organisation.

3.6. Remboursement

[Nom de l'organisation] ne paiera aucun frais à ses employés (les propriétaires de BYOD) pour l'utilisation des équipements à des fins professionnelles.

[Nom de l'organisation] paiera pour ce qui suit :

- [illegible]
- [illegible]

3.7. Failles de sécurité

Toutes les failles de sécurité liées à des BYOD doivent être immédiatement signalées à [titre du poste]. [illegible]

3.8. Formation et sensibilisation

[Titre du poste] est en charge de la formation des nouveaux employés, et de ceux déjà en poste, sur l'utilisation appropriée des BYOD, ainsi que de la sensibilisation aux menaces les plus courantes.

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

[illegible]	*Lieu de conservation*	*Personne responsable de la conservation*	[illegible]	[illegible]
[illegible]	[intranet de l'organisation]	[titre du poste]	[illegible]	[illegible]
[illegible]	[intranet de l'organisation]	[titre du poste]	[illegible]	[illegible]
[illegible]	[intranet de l'organisation]	[titre du poste]	[illegible]	[illegible]

Commented [AES15]: Indiquez le nom de votre organisation.

Commented [AES16]: Autrement, vous pouvez définir un [illegible]

Commented [AES17]: Indiquez le nom de votre organisation.

Commented [AES18]: Adapter aux pratiques en vigueur dans l'organisation.

Commented [AES19]: Il s'agit généralement du Responsable [illegible]

Commented [AES20]: Cette formation vous aidera à sensibiliser vos employés à la sécurité et à évaluer leurs connaissances : [illegible]

Commented [AES21]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation. [illegible]

Commented [AES22]: Ajuster si nécessaire.

Commented [AES23]: Ajuster si nécessaire.

Commented [AES24]: Ajuster si nécessaire.

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

Le propriétaire de ce document est [titre du poste], qui doit vérifier et, si nécessaire, mettre à jour le document au moins une fois par an. [redacted]

Commented [AES25]: Il ne s'agit que d'une recommandation ; [redacted]

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre d'incidents liés à l'utilisation de BYOD
- [redacted]

[titre du poste]
[nom]

[signature]

Commented [AES26]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.