SOLUMADA

POLITIQUE EN MATIÈRE D'APPAREILS MOBILES

Contrôle des versions

Propriétaire	**Version**	**Édité par**	**Date**	**Historique des modifications**
Solumada	1.0	Rudo Courtney Togara	16 janvier 2024	Création de documents et ajout de détails primaires
Solumada	1.1	Kushal Mulleea	23 janvier 2024	Révision de l'ensemble du contenu du document
Solumada	1.2	Kushal Mulleea	12 Février 2024	Ajustement du document après vérification de l'exactitude de la traduction

Classification

Confidentiel	Usage interne uniquement	Publique
		X

Pertinence par rapport à la norme

Norme	Contrôle de l'annexe A
ISO 27001:2022	–

Politique en matière d'appareils mobiles

La politique relative aux appareils mobiles décrit l'approche de Solumada en matière de gestion des risques associés à l'utilisation des appareils mobiles, qui comprennent les smartphones, les ordinateurs portables et les appareils de poche.

1.0 Objectif

L'objectif de cette politique relative aux appareils mobiles est d'établir des lignes directrices pour l'utilisation et la gestion sécurisées des appareils mobiles au sein de Solumada. Cette politique vise à protéger les informations de l'organisation, à garantir la sécurité des données et à se conformer aux exigences de la norme ISO 27001.

1.1 Champ d'application

Cette politique s'applique à tous les employés et les types d'appareils mobiles inclus dans ce champ d'application sont les tablettes PC et les ordinateurs portables fournis par l'organisation.

2.0 Utilisation des appareils mobiles

2.1 Appareils autorisés

- Les appareils mobiles délivrés et approuvés par l'organisation sont autorisés à des fins professionnelles. Ces appareils sont fournis aux employés en fonction de leur rôle et des exigences de leur poste.
- Les smartphones personnels, utilisés dans le cadre du programme BYOD, sont autorisés à des fins professionnelles uniquement pour les membres du département des projets. Cela inclut l'accès aux systèmes, données et réseaux de l'organisation et pour communiquer avec les clients sur des questions relatives aux projets.

2.2 Types d'appareils

- Ordinateurs portables
- Smartphones personnels (sous le programme BYOD)

3.0 Politique en matière de dispositifs mobiles

La politique relative aux appareils mobiles traite généralement de l'utilisation et de la sécurité des appareils mobiles fournis par l'organisation, dans le cas de Solumada, il s'agit des ordinateurs portables.

3.1 Responsabilités

3.1.1 Employés

Il est du devoir des employés de se conformer à la présente politique et d'utiliser les dispositifs mobiles fournis par l'organisation de manière sûre et responsable.

3.1.2 Service informatique

Le service informatique est responsable de la mise à disposition, de la gestion et de la sécurité des appareils mobiles fournis par l'organisation. Le département doit notamment veiller à ce que ces appareils soient configurés, contrôlés et entretenus de manière appropriée.

3.2 Mesures de sécurité

Tous les appareils mobiles utilisés à des fins professionnelles doivent respecter les politiques de Solumada en matière de sécurité de l'information, y compris, mais sans s'y limiter, celles relatives aux contrôles d'accès, aux logiciels antivirus et aux mises à jour de sécurité.

3.3 Formation et sensibilisation

Solumada fournira des programmes de formation et de sensibilisation pour éduquer les employés sur les risques associés à l'utilisation des appareils mobiles et sur l'importance d'adhérer à cette politique.

3.4 Respect et mise en œuvre

Le non-respect de la présente politique peut entraîner des mesures disciplinaires pouvant aller jusqu'à la résiliation de l'emploi ou du contrat.

3.5 Évaluation et révision

La présente politique sera ré-examinée et, si nécessaire, révisée périodiquement afin de garantir son efficacité et son alignement sur les exigences de la norme ISO 27001.

- Lors de l'utilisation d'appareils mobiles à des fins professionnelles, il est important de veiller aux points suivants :

- Les alertes de sécurité et les avertissements ne doivent jamais être ignorés. Si l'un d'eux se produit, l'utilisateur doit cesser immédiatement son activité et le signaler **au service informatique**.
- Si l'utilisateur pense que le logiciel ne fonctionne pas correctement, il doit le signaler **au service informatique** dès que possible.
- Les employés sont encouragés à se familiariser avec la procédure de signalement des incidents de sécurité de l'information, afin de pouvoir contacter les bons canaux en cas d'incident.

4.0 Coordonnées

Pour toute question, préoccupation ou information complémentaire relative à cette politique, veuillez contacter rudo@optimumsolutions.eu.

----------Fin du document----------