SOLUMADA

POLITIQUE RELATIVE AUX DISPOSITIFS D'EXTRÉMITÉ DE L'UTILISATEUR

Contrôle des versions

Propriétaire	**Version**	**Modifié 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	A.8.1

1.0 Introduction

Cette politique définit ce qui doit être fait pour assurer une protection adéquate des informations traitées, stockées ou accédées par l'intermédiaire des utilisateurs du périphérique. C'est important car presque toutes les informations sensibles peuvent être consultées par le biais de ces appareils. La politique est alignée sur le contrôle A.8.1 de la norme ISO 27001 - (User Endpoint Devices).

1.1 Objectif

L'objectif de cette politique relative aux terminaux utilisateurs est d'établir des lignes directrices pour la protection adéquate des informations sensibles traitées, stockées ou consultées par les terminaux utilisateurs au sein de Solumada. Cette politique vise à minimiser les risques de sécurité et à assurer la conformité aux normes internationales ISO 27001.

1.2 Champ d'application

La présente politique s'applique à tous les employés de tous les départements qui sont spécifiés dans le champ d'application du système de gestion de la sécurité de l'information (SGSI) qui utilisent les appareils terminaux de l'utilisateur pour accéder à des informations de l'entreprise, les traiter ou les stocker. Les utilisateurs disposent de périphériques d'extrémité qui incluent, mais ne sont pas limités aux ordinateurs de bureau, aux ordinateurs portables, aux téléphones mobiles, les tablettes et autres appareils portables.

2.0 Déclarations de politique générale

2.1 Sécurité des appareils des utilisateurs

- Des mots de passe forts et uniques doivent être utilisés, et l'authentification multifactorielle (MFA) est recommandée.
- Les mises à jour et les correctifs de sécurité automatiques doivent être activés pour garantir l'application des dernières corrections et améliorations en matière de sécurité.
- Un logiciel antivirus et anti-malware à jour doit être installé et actif sur tous les appareils.

2.2 L'accès à distance

- Lorsqu'ils accèdent aux ressources de l'entreprise à distance, les utilisateurs doivent utiliser des connexions VPN sécurisées, comme le prévoit **la politique de travail à distance**.

2.3 Signalement des incidents

- Les utilisateurs doivent immédiatement signaler la perte ou le vol d'un appareil au service informatique et à leur chef de service.
- Les activités suspectes, les violations de données ou les incidents de sécurité liés aux terminaux des utilisateurs doivent être signalés rapidement en suivant les procédures établies de signalement des incidents.

2.4 Conformité et monitorage

- Le respect de cette politique sera contrôlé au moyen d'audits et d'évaluations de sécurité réguliers.
- Le non-respect de cette politique peut donner lieu à des mesures disciplinaires en fonction de la gravité de la violation.

2.5 Révision et mise à jour de la politique

- La présente politique sera ré-examinée chaque année ou en fonction des besoins afin de s'assurer qu'elle reste efficace et conforme aux normes ISO 27001. Toute mise à jour sera communiquée à l'ensemble du personnel concerné.

2.6 Politiques associées

- Politique en matière de travail à distance
- Procédure de gestion des incidents de sécurité de l'information

3.0 Coordonnées

Pour toute question, préoccupation ou information complémentaire relative à la présente politique, veuillez contacter le responsable de la sécurité de l'information à cette adresse électronique: rudo@optimumsolutions.eu.

En se conformant à la présente politique relative aux dispositifs d'extrémité des utilisateurs, Solumada vise à protéger les informations sensibles, à réduire les risques de sécurité et à démontrer son engagement envers le contrôle A.8.1 de la norme ISO 27001. Tous les employés et le personnel sont responsables de la compréhension et du respect des lignes directrices décrites dans cette politique.

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