SOLUMADA

Politique de classification des informations

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	A.5.12

1. Introduction

Cette politique définit les principes et les procédures de classification des informations au sein de Solumada conformément au contrôle A.5.12 de la norme ISO 27001.

2. Objectif

L'objectif de cette politique est d'établir un cadre structuré pour classer les informations en fonction de leur sensibilité, assurer leur protection adéquate et faciliter la mise en œuvre des contrôles de sécurité.

3. Champ d'application

Cette politique s'applique à tous les employés de tous les départements spécifiés dans le champ d'application du système de gestion de la sécurité de l'information (SGSI) et à tout autre personnel ayant accès aux actifs informationnels de Solumada.

4. Classification des informations

4.1. Les informations sont classées en trois catégories en fonction de leur sensibilité:

4.1.1. Information du public (faible sensibilité):

Les informations publiques sont des informations qui n'ont pas d'exigences particulières en matière de sensibilité ou de confidentialité et qui peuvent être librement partagées avec le public. Il peut s'agir, par exemple, de documents de marketing, d'annonces publiques et d'informations générales sur les contacts.

4.1.2. Usage interne uniquement (sensibilité modérée):

Les informations à usage interne sont destinées à être utilisées au sein de l'organisation et ne doivent pas être divulguées à des parties externes sans autorisation appropriée. Cette catégorie peut inclure les manuels des employés, les communications internes et les données commerciales non confidentielles.

4.1.3. Informations confidentielles (haute sensibilité):

Les informations confidentielles sont très sensibles et doivent être protégées contre tout accès ou toute divulgation non autorisés. Elles comprennent les informations personnelles identifiables (IPI), les données financières et les données sensibles des clients.

5. Responsabilités

- Tout le personnel est responsable de la classification correcte des informations et de leur utilisation conformément à leur classification.
- Le propriétaire de l'information est responsable de définir la classification des informations sous son contrôle et assure que les mesures de sécurité appropriées sont en place pour les protéger.
- Le responsable de la sécurité de l'information (ISO) est chargé de superviser la mise en œuvre et le respect de cette politique et de fournir des conseils sur la classification des informations.

6. Traitement des informations classifiées

6.1. Information du public:

- Aucune particularité de traitement s'applique, mais toutes les précautions doivent être prises pour garantir la sécurité des données.

6.2. Informations à usage interne uniquement:

- L'accès à ces informations doit être limité au personnel autorisé.
- Les informations ne doivent pas être communiquées à l'extérieur de l'organisation sans autorisation appropriée.

6.3. Informations confidentielles:

- L'accès aux informations confidentielles doit être limité aux personnes ayant un besoin légitime de les connaître.

- Les informations doivent être stockées, transmises et éliminées en toute sécurité, conformément aux contrôles de sécurité établis.

7. Étiquetage et Marquage

Les informations doivent être étiquetées ou marquées de manière appropriée pour illustrer leur classification. Cet étiquetage doit être clairement visible et cohérent avec les catégories de classification. Vous pouvez contacter le responsable de la sécurité de l'information si vous ne savez pas comment étiqueter les documents et les actifs informationnels.

8. Revue et révision

La présente politique sera ré-examinée et mise à jour si nécessaire afin de garantir son efficacité et sa pertinence.

9. Informations sur les contacts

Pour toute question ou préoccupation relative à la classification des informations, contactez le responsable de la sécurité de l'information (ISO) à cette adresse électronique: rudo@optimumsolutions.eu

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