					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P13S					Titre du document : **Politique de classification et d'étiquetage des données**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clauses 5.3, 8	
ISO/IEC 27002:2022	Mesures 5.12, 5.13	
NIST SP 800-53 Rév. 5	AC-16, MP-3, MP-5	
NIS2 (UE)	Article 21(2)(a)	
DORA (UE)	Article 5(8)	
COBIT 2019	BAI03.05, DSS05	
RGPD (UE)	Articles 5, 32	

1. Objet

1.1 La présente politique définit la manière dont l'ensemble des informations traitées par l'organisation doivent être classifiées et étiquetées afin de préserver leur confidentialité, leur intégrité et leur disponibilité tout au long de leur cycle de vie.

1.2 Elle vise à assurer un traitement cohérent des données en attribuant aux informations des niveaux de protection appropriés selon leur sensibilité, leur impact sur l'activité ou les obligations légales applicables.

1.3 La classification et l'étiquetage contribuent à réduire le risque de divulgation accidentelle, d'accès non autorisé ou de traitement inapproprié des données sensibles, en particulier dans les PME pouvant s'appuyer sur des systèmes plus simples et sur des contrôles documentés moins formalisés.

1.4 La présente politique est essentielle à la certification ISO/IEC 27001 et à la conformité réglementaire, notamment au regard des textes relatifs à la protection des données tels que le RGPD et des référentiels de cybersécurité tels que NIS2 et DORA.

2. Champ d’application

2.1 La présente politique s'applique à toutes les données de l'organisation, quel qu'en soit le format ou l'emplacement, y compris :

2.1.1 les documents électroniques, feuilles de calcul, courriels, formulaires, images et fichiers numérisés ;

2.1.2 les documents physiques tels que les enregistrements imprimés, rapports, factures et notes ;

2.1.3 les données stockées ou traitées dans des services cloud, sur des serveurs locaux, des supports amovibles ou des équipements personnels utilisés à des fins professionnelles ;

2.1.4 les données temporaires ou transitoires générées dans le cadre des activités de l'entreprise (par exemple, journaux, fichiers cache, courriels).

2.2 L'ensemble du personnel, les prestataires, les intérimaires et les tiers disposant d'un accès aux données de l'organisation sont tenus de se conformer à la présente politique.

2.3 Elle s'applique à l'ensemble du cycle de vie des données, depuis leur création et leur stockage jusqu'à leur archivage ou leur suppression, y compris leur accès et leur transfert.

3. Objectifs

3.1 Définir un schéma de classification simple et opposable, compréhensible et applicable dans l'ensemble de l'organisation.

3.2 Exiger que chaque actif de données soit classifié selon son niveau de sensibilité et étiqueté en conséquence afin d'orienter son traitement, son stockage et les modalités d'accès appropriées.

3.3 Veiller à ce que les pratiques d'étiquetage des données soient intégrées aux processus métiers, notamment lors de l'intégration, du lancement de projet et de la mise en service des systèmes.

3.4 Réduire le risque de violation de données par l'application de contrôles de sécurité adaptés au niveau de classification (par exemple, chiffrement, restriction d'accès).

3.5 Garantir la conformité aux exigences relatives à la protection de la vie privée et à la sécurité de l'information en démontrant que les données sensibles (par exemple, données à caractère personnel, données financières ou informations propriétaires) sont correctement étiquetées et gérées.

3.6 Établir la responsabilité des décisions de classification et garantir des revues et mises à jour périodiques en fonction de l'évolution des besoins métiers et des exigences juridiques.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Est responsable de la présente politique et approuve le schéma de classification.

4.1.2 Assure la supervision afin que les responsabilités en matière de classification soient dûment déléguées et effectivement mises en œuvre.

4.1.3 Revoit et autorise toute dérogation à la politique relative aux exigences de classification ou d'étiquetage.

4.1.4 Veille à ce que les pratiques de traitement des données satisfassent aux exigences de conformité prévues par des textes tels que le RGPD et DORA.

4.2 Propriétaire de l'information / gestionnaire de données

4.2.1 Attribue une classification initiale à chaque nouvel ensemble de données ou actif informationnel lors de sa création ou de son acquisition.

4.2.2 Veille à ce que des étiquettes visibles (par exemple, en-têtes, pieds de page, filigranes, noms de dossiers) soient appliquées lorsque cela est pertinent.

4.2.3 Revoit périodiquement les classifications afin d'en vérifier la pertinence et l'exactitude et d'identifier les modifications nécessaires (par exemple, après déclassification ou publication).

4.2.4 Travaille avec le responsable informatique pour mettre en œuvre les protections techniques fondées sur la classification (par exemple, droits d'accès, chiffrement).

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exigences de revue et de mise à jour

9.1 La présente politique doit faire l'objet d'une revue annuelle par le DG et le gestionnaire de données afin de garantir qu'elle reflète :

9.1.1 les évolutions des activités de l'entreprise ou des types de données ;

9.1.2 les nouvelles exigences réglementaires (par exemple, en matière de vie privée ou de supervision financière) ;

9.1.3 les évolutions technologiques affectant les capacités d'étiquetage ou de classification.

9.2 La revue doit inclure les mises à jour des catégories de classification, des outils ou pratiques d'étiquetage, ainsi que du contenu de sensibilisation et de formation.

9.3 Les révisions de la politique doivent être approuvées par le DG et communiquées à l'ensemble du personnel. Un historique des versions doit être conservé à des fins d'audit.

10. Politiques associées et articulations

10.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : attribue la responsabilité de la propriété de la politique et de sa mise en œuvre.

10.2 P4S – Politique de contrôle d'accès : aligne les accès aux systèmes sur les niveaux de classification des données.

10.3 P12S – Politique de gestion des actifs : assure le suivi des actifs physiques et numériques stockant des données classifiées.

10.4 P17S – Politique de protection des données et de la vie privée : encadre la protection des données à caractère personnel, dont une grande partie est classifiée « Confidentiel ».

10.5 P30S – Politique de réponse aux incidents : définit les circuits d'escalade et les procédures de réponse en cas de manquement à la classification ou d'exposition de données.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 5.3 : exige une définition claire des responsabilités relatives au traitement et à la protection des données.

11.1.2 Clause 8.1 : impose une planification opérationnelle et des contrôles, y compris ceux liés à la catégorisation des données.

11.2 ISO/IEC 27002

11.2.1 Mesure 5.12 : fournit des orientations sur la classification de l'information fondée sur les risques et les exigences réglementaires.

11.2.2 Mesure 5.13 : décrit les mécanismes pratiques d'étiquetage et les règles de traitement associées.

11.3 NIST SP 800-53 Rév. 5

11.3.1 AC-16 : impose le marquage des informations afin d'assurer que les mesures de protection sont alignées sur la classification.

11.3.2 MP-3 / MP-5 : fournissent des orientations sur l'étiquetage et le contrôle des supports et des sorties.

11.4 RGPD (UE)

11.4.1 Articles 5 et 32 : imposent la minimisation des données et l'intégrité au moyen de mesures de classification et de traitement appropriées.

11.5 NIS2 (UE)

11.5.1 Article 21(2)(a) : impose des contrôles techniques et organisationnels pour une protection des données fondée sur les risques.

11.6 DORA (UE)

11.6.1 Article 5(8) : exige que les entreprises classifient les actifs de données dans le cadre de leur programme de gestion des risques liés aux TIC.

11.7 COBIT 2019

11.7.1 BAI03.05 : exige la classification de l'information et une protection ajustée au risque.

11.7.2 DSS05.02 : traite de la mise en œuvre des contrôles fondés sur la classification et de la surveillance.