					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P13					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**

1. Objet

1.1 La présente politique définit le cadre formel de classification et d'étiquetage des actifs informationnels de l'organisation selon leur sensibilité, leur exposition au risque et les obligations réglementaires applicables.

1.2 Elle impose que toute information, qu'elle soit stockée, transmise ou traitée, soit clairement catégorisée et étiquetée de manière à indiquer le niveau de protection et les règles de traitement requis.

1.3 La présente politique impose une classification structurée, alignée sur les pratiques de gestion des risques de l'organisation, afin de soutenir les objectifs de confidentialité, d'intégrité et de disponibilité, pour les données numériques comme physiques.

1.4 Cette mesure est essentielle pour permettre le contrôle d'accès fondé sur les rôles, la préparation aux audits, le partage approprié des données et le déploiement efficace de mesures de protection techniques telles que le chiffrement, la sauvegarde et la surveillance.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les actifs informationnels de l'organisation, y compris les documents, bases de données, enregistrements et communications

2.1.2 Tous les formats de données, y compris numériques, imprimés, manuscrits ou verbaux

2.1.3 Tous les environnements : sur site, distants, mobiles et cloud

2.1.4 Tous les employés, prestataires, fournisseurs de services et sous-traitants tiers qui créent, traitent ou stockent des informations de l'organisation

2.2 Le champ d'application couvre les contenus développés en interne, les données issues de sources externes, les données à caractère personnel soumises aux obligations légales en matière de protection de la vie privée (par exemple, le RGPD), ainsi que les informations échangées avec les clients, partenaires et autorités de régulation.

2.3 Elle s'applique à tous les systèmes utilisés pour stocker ou transmettre des données, y compris les applications d'entreprise, les serveurs de fichiers, les systèmes de messagerie, les plateformes cloud et les référentiels de sauvegarde.

3. Objectifs

3.1 Établir un schéma de classification standardisé à l'échelle de l'organisation, fondé sur l'impact d'une exposition ou d'une compromission des données.

3.2 Garantir que toute information soit étiquetée de manière visible et persistante afin de refléter son niveau de classification et ses exigences de traitement.

3.3 Imposer un traitement des données et des contrôles d'accès alignés sur la classification, y compris le chiffrement, la journalisation, la protection de la transmission et la planification de la conservation.

3.4 Soutenir la conformité aux normes internationales (ISO/IEC 27001, 27002), aux cadres juridiques (RGPD, NIS2, DORA) et aux politiques internes de gestion des risques.

3.5 Garantir que tous les utilisateurs comprennent leurs responsabilités en matière de protection des données, d'application des étiquettes et de traitement correct des informations classifiées.

3.6 Maintenir la traçabilité entre le statut de classification, les contrôles associés et l'inventaire des actifs de l'organisation à des fins d'audit et de conformité.

4. Rôles et responsabilités

4.1 Responsable de la sécurité des systèmes d'information (RSSI)

4.1.1 Est responsable de la politique de classification et d'étiquetage de l'information et veille à son alignement sur les exigences réglementaires, contractuelles et opérationnelles.

4.1.2 Approuve les niveaux de classification, les standards d'étiquetage et les révisions de la politique.

4.1.3 Assure la supervision de la conformité à la politique au moyen d'audits, d'indicateurs et de revues des exceptions.

4.1.4 Assure la coordination interfonctionnelle de la gouvernance avec les équipes juridiques, de protection des données et de gestion des risques.

4.2 Propriétaires de l'information

4.2.1 Sont responsables de la classification des actifs informationnels placés sous leur responsabilité conformément au schéma de classification de l'organisation.

4.2.2 Appliquent les étiquettes de classification au moment de la création, de la mise à jour ou de la réception.

4.2.3 Revoient périodiquement la classification des actifs, notamment en cas d'évolution de la sensibilité, du périmètre réglementaire ou de la valeur métier.

4.2.4 Veillent à ce que les données sensibles soient correctement traitées et étiquetées tout au long de leur cycle de vie.

[... 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 au moins annuelle afin de garantir son alignement avec :

9.1.1 Les évolutions des exigences réglementaires (par exemple, RGPD, NIS2, DORA)

9.1.2 Les mises à jour des lignes directrices de classification ISO/IEC 27001 ou 27002

9.1.3 Les changements organisationnels ayant un impact sur la sensibilité des données ou leur propriété

9.1.4 Les évolutions technologiques, y compris les nouvelles plateformes de gestion documentaire ou de gestion des données

9.2 Le responsable de la sécurité des systèmes d'information (RSSI) doit initier la revue en collaboration avec le Comité de sécurité de l'information, le service juridique et les unités métier concernées.

9.3 Les revues doivent inclure :

9.3.1 L'efficacité de la mise en œuvre de la classification et le respect des exigences par les utilisateurs

9.3.2 L'analyse des incidents ou des exceptions liés à une mauvaise classification

9.3.3 Le retour d'expérience des utilisateurs sur les outils d'étiquetage ou les supports d'orientation

9.3.4 Une analyse comparative avec les standards de classification du secteur

9.4 Les mises à jour de la politique doivent faire l'objet d'une gestion des versions, être documentées dans le référentiel du SMSI et être communiquées à l'ensemble du personnel concerné en mettant l'accent sur les nouvelles responsabilités ou les évolutions d'outillage.

9.5 Les nouvelles recrues doivent être sensibilisées à la version en vigueur de la politique lors du processus d'intégration. Tous les employés doivent suivre une formation de rappel à la suite de changements significatifs de la politique.

10. Politiques associées et articulations

10.1 La présente politique est directement soutenue par les politiques associées suivantes et met en œuvre les contrôles qui y sont décrits :

10.1.1 P4 - Politique de contrôle d'accès : l'accès à l'information est régi par les niveaux de classification ; les données les plus sensibles exigent des mécanismes de contrôle d'accès et d'autorisation plus stricts.

10.1.2 P11 - Politique de gestion des comptes utilisateurs et des privilèges : renforce l'attribution des privilèges selon le besoin d'en connaître, déterminé notamment par les niveaux de classification.

10.1.3 P12 - Politique de gestion des actifs : garantit que chaque actif de l'inventaire comporte sa classification et son étiquette, afin de soutenir la traçabilité et la responsabilité.

10.1.4 P14 - Politique de conservation et d'élimination des données : les règles de conservation et d'élimination sont déterminées par le niveau de classification des données et les obligations réglementaires de conservation.

10.1.5 P18 - Politique des contrôles cryptographiques : applique des standards de chiffrement appropriés selon la classification de l'actif informationnel.

10.1.6 P22 - Politique de journalisation et de surveillance : permet la surveillance de l'accès aux informations classifiées et de leur circulation, afin d'assurer l'auditabilité et la détection des erreurs d'étiquetage ou des usages inappropriés.

10.2 Chaque articulation garantit une protection cohérente de l'information tout au long de son cycle de vie, depuis sa création et sa classification jusqu'à son traitement sécurisé, son stockage, sa transmission et sa destruction finale.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des normes et cadres réglementaires internationalement reconnus régissant la classification et l'étiquetage des informations sensibles.

11.2 ISO/IEC 27001

11.2.1 Clause 4.2 - Compréhension des besoins et attentes des parties intéressées. Les exigences de classification découlent souvent d'obligations légales, réglementaires ou contractuelles imposées par les parties intéressées (par exemple, le RGPD, les accords de non-divulgation des clients) et doivent être prises en compte dans la politique.

11.2.2 Clause 6.1.3 - Traitement des risques liés à la sécurité de l'information. La classification a une incidence directe sur la sélection des mesures de traitement des risques, y compris le contrôle d'accès, le chiffrement et la conservation, selon la sensibilité des données.

11.2.3 Clause 7.2 - Compétence. La politique impose que le personnel responsable de la classification et de l'étiquetage soit formé, ce qui relève des exigences de compétence.

11.2.4 Clause 7.3 - Sensibilisation. La politique impose que tous les utilisateurs connaissent les niveaux de classification et leurs responsabilités dans le traitement de l'information, conformément aux obligations de sensibilisation.

11.2.5 Clause 7.5 - Informations documentées. La politique de classification elle-même est un document contrôlé, et les procédures, les enregistrements de formation et les étiquettes de classification font partie des informations documentées.

11.2.6 Clause 8.1 - Planification et maîtrise opérationnelles. La classification et l'étiquetage sont des processus opérationnels intégrés à la gestion du cycle de vie des données, et cette clause exige que ces activités soient planifiées, mises en œuvre et maîtrisées.

11.2.7 Clause 9.1 - Surveillance, mesure, analyse et évaluation. La politique prévoit des dispositions relatives à la surveillance de la conformité de la classification, aux tendances d'incident et à l'efficacité du schéma d'étiquetage.

11.2.8 Clause 10.1 - Non-conformité et action corrective. La politique définit les réponses à une mauvaise classification, y compris les actions correctives telles que la nouvelle formation, les mises à jour et la gestion des exceptions.

11.3 ISO/IEC 27002:2022

11.3.1 Mesure 5.12 - Classification de l'information. Cette mesure garantit que l'information est classifiée selon sa sensibilité, sa valeur et sa criticité, ce que la présente politique formalise précisément.

11.3.2 Mesure 5.13 - Étiquetage de l'information. Cette mesure impose un étiquetage approprié de l'information conformément à son niveau de classification, ce que la présente politique couvre intégralement.

11.3.3 Mesure 5.10 - Utilisation acceptable de l'information et des autres actifs associés. La politique encadre la manière dont les utilisateurs doivent traiter les données classifiées, soutenant directement l'utilisation acceptable et prévenant les usages inappropriés.

11.3.4 Mesure 5.11 - Restitution des actifs. La classification contribue à garantir que les données sensibles sont identifiées, restituées de manière sécurisée ou assainies lorsqu'un employé ou un fournisseur quitte l'organisation.

11.3.5 Mesure 5.9 - Inventaire de l'information et des autres actifs associés. La classification est souvent liée à l'inventaire des actifs, qui doit refléter le niveau de classification de chaque élément afin de soutenir l'attribution appropriée des contrôles.

11.3.6 Mesure 5.14 - Transfert d'information. Les niveaux de classification influencent les contrôles applicables aux transferts internes et externes de données (par exemple, chiffrement, approbation, restrictions d'accès).

11.3.7 Mesure 8.12 - Prévention de la fuite de données. L'application de la classification et de l'étiquetage contribue à prévenir les divulgations non autorisées et les pertes de données.

11.3.8 Mesure 8.11 - Masquage des données. Certains niveaux de classification (par exemple, Confidentiel, Restreint) peuvent imposer le masquage lorsque les données sont utilisées dans des environnements de test/développement ou à des fins analytiques.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Politique et procédures de protection des systèmes et des communications : soutient les politiques de classification dans le cadre global de la protection des données.

11.4.2 AC-16 - Attributs de sécurité : met en œuvre l'application des accès sur la base des métadonnées de classification et des autorisations des utilisateurs.

11.4.3 MP-3 / MP-5 - Marquage des supports et protection pendant le transport : impose l'étiquetage et la protection des données au repos et en transit selon leur classification.

11.5 RGPD de l'UE (2016/679)

11.5.1 Article 5 - Principes relatifs à la protection des données : impose que les données à caractère personnel soient traitées de manière sécurisée, proportionnée à leur sensibilité.

11.5.2 Article 32 - Sécurité du traitement : renforce la classification en tant que mécanisme de protection des données fondé sur les risques et de mise en œuvre de mesures techniques appropriées.

11.6 Directive NIS2 de l'UE (2022/2555)

11.6.1 Article 21(2)(a) : impose des politiques de gestion des risques liés à la sécurité de l'information, y compris des contrôles de classification des actifs et des données.

11.6.2 Article 21(3) : encourage l'adoption de mesures permettant d'imposer un traitement approprié des données, soutenu par un étiquetage fondé sur la classification.

11.7 DORA de l'UE (2022/2554)

11.7.1 Article 5 - Gouvernance et contrôle : impose des cadres de gouvernance qui classifient les actifs de données aux fins de maîtrise des risques liés aux TIC.

11.7.2 Article 9 - Gestion des risques liés aux TIC : impose des mesures techniques et organisationnelles pour les actifs TIC critiques, y compris la classification et l'étiquetage.

11.8 COBIT 2019

11.8.1 DSS05.02 - Gestion des services de sécurité : impose des classifications de sécurité de l'information afin de garantir la protection des données de l'entreprise.

11.8.2 MEA03 - Surveiller, évaluer et apprécier la conformité : soutient l'audit et la revue réguliers des pratiques de classification afin d'assurer le respect de la politique et la maturité.