POLITQUE DE CLASSIFICATION ET DE TRAITEMENT DES INFORMATIONS

1. Objet

Cette politique définit des classifications pour toutes les informations du WM (quel que soit leur format, y compris les formats électronique et papier) et les systèmes qui traitent les informations, en fonction de la sensibilité, de la valeur et de l'importance des informations et des systèmes. Cette politique décrit les instructions de traitement approprié pour chaque classification.

Cette politique soutient la politique de gestion des dossiers et des informations en garantissant l'uniformité de l'étiquetage, de l'accès et des procédures concernant toutes les informations de WM. Elle poursuit les objectifs suivants :

- assurer une compréhension et une application cohérentes des catégories et des étiquettes de classification des données ;
- fournir un aperçu des données à tous les stades de leur cycle de vie afin d'améliorer la compréhension de toutes les personnes qui travaillent avec des données et des informations de WM.

Cette politique remplace toute autre communication ou politique existante sur les sujets qu'elle aborde.

Cette politique reconnaît qu'il existe un effort continu pour améliorer les procédures relatives à la classification et au traitement des informations. WM travaille activement à la reclassification et à l'ajustement du traitement des informations anciennes conformément à la politique révisée.

2. Champ d'application

Les deux affirmations suivantes s'appliquent à toutes les données WM :

- WM ne recueille que les informations nécessaires à des fins professionnelles spécifiques ;
- les informations ne doivent être partagées qu'avec le personnel autorisé ayant besoin de les connaître à des fins professionnelles.
    - Le « besoin de connaître » signifie qu'une personne a besoin d'accéder à des données ou à des informations spécifiques dans l'exercice des fonctions qui lui sont confiées. Le besoin de connaître inclut les demandes émanant de toute procédure légale, telle que les citations à comparaître, les ordonnances judiciaires et les rapports requis par les autorités gouvernementales.
    - Lorsque des personnes déterminent si le besoin de savoir est légitime, elles doivent vérifier l'autorisation du demandeur. En cas de doute, elles doivent demander conseil à la direction, aux responsables des données concernés et/ou au service de cybersécurité.
    - Les personnes ne doivent pas répondre à des appels non sollicités, à des enquêtes par courriel ou à des demandes d'informations relatives à l'entreprise ou à des demandes d'informations de tiers provenant de connexions externes, d'adresses électroniques ou de liens vers des sites Web de collecte de données externes.

Données relevant du champ d'application

Toutes les données, les informations et les documents (sous quelque format que ce soit, y compris les formats électronique et papier) créés, collectés, utilisés, modifiés, partagés, stockés ou transmis (désignés collectivement ci-après « traités ») dans le cadre de l'emploi ou au cours d'activités avec ou pour une entreprise de WM, ainsi que les systèmes qui traitent ces informations, relèvent du champ d'application de la présente politique. Dans le cadre de la présente politique, les données et les informations sont définies ci-dessous.

- Données : faits ou chiffres bruts, généralement contenus dans une base de données ou un système.
    - Données structurées : éléments de données qui sont dans un champ fixe au sein d'un fichier ou d'un système, tels que les entrées au niveau des colonnes ou des champs.
    - Données non structurées : toutes les données qui ne sont pas structurées, telles que les données contenues dans les courriels, les textos, les applications de messagerie instantanée (comme Microsoft Teams), les vidéos, les traitements de texte, les feuilles de calcul, les fichiers PDF, les images, les fichiers issus d'un système CAO (Conception assistée par ordinateur) ou d'autres types de fichiers.
- Informations : données traitées, organisées ou agrégées d'une manière qui ajoute un contexte ou une signification aux éléments de données individuels, généralement sous forme non structurée.

Systèmes relevant du champ d'application

Cette politique s'applique à tous les systèmes de traitement ou de stockage des données et/ou à toutes les applications existantes dans le cadre de WM. Toutefois, les classifications des systèmes et des applications sont appliquées différemment des classifications des données. Les systèmes et les applications sont classés une seule fois (généralement lors des tests d'acceptation) et au niveau le plus élevé en termes de sensibilité des données, traitées (ou censé être traitées) par le système. Il incombe au propriétaire des données du domaine ou au responsable des données de classer les systèmes (définis à l'article 3).

3. Rôles et responsabilités

Cette politique s'applique à tous les employés de WM et aux tiers qui ont accès aux données de WM (désignés collectivement ci-après « le personnel de WM » ou « les personnes assujetties »). Conformément à cette politique, ces personnes sont considérées comme des parties responsables et elles sont, en tant que telles, tenues de faire preuve de prudence et d'appliquer les procédures appropriées, lorsqu'elles traitent des informations dans l'exercice de leurs fonctions.

Le non-respect de cette politique peut engager la responsabilité de l'entreprise et la responsabilité personnelle, et peut entraîner des mesures disciplinaires internes pouvant aller jusqu'à la cessation d'emploi ou à la résiliation d'un contrat ou d'un accord de service avec un tiers, et/ou des poursuites judiciaires.

Des responsabilités supplémentaires incombent aux personnes suivantes :

- le propriétaire des données du domaine et le responsable des données dont les responsabilités sont énumérées dans le modèle de gestion des données de l'entreprise WM (cliquer ici) ;
- le directeur principal de la cybersécurité (DPC) qui effectue des contrôles de protection des données selon le cadre de cybersécurité défini par l'institut américain NIST (National Institute of Standards and Technology) ;
- le directeur principal de la gestion des données (DPGD), dans le cadre de la gouvernance des données d'entreprise ;
- l'équipe de gouvernance en matière de cybersécurité qui examine les courriels de la boite courriel InfoSec@wm.com, répond aux questions sur la politique et sollicite, si nécessaire, la participation du DPC, du DPGD et des responsables de la gestion des données.

4. Autorité de classification

Il existe deux types d'autorité de classification : l'autorité de classification initiale (ACI) et l'autorité de classification de dérivés. Les personnes qui ne sont pas officiellement désignées pour exercer l'ACI sont, par définition, des classificateurs des dérivés.

- Autorité de classification initiale

La classification initiale désigne la détermination initiale du *niveau de risque* de l'information, c'est-à-dire le niveau d'atteinte à la réputation ou aux opérations de WM, ou le niveau de répercussions légales ou réglementaires que la divulgation de ladite information pourrait raisonnablement entraîner. L'autorité de classification des informations initiales ne peut être exercée que par les personnes suivantes, telles que définies dans le modèle de gestion des données de l'entreprise WM :

- les propriétaires exécutifs des données ;
- les propriétaires de données du domaine ;
- les responsables des données ;
- d'autres experts en la matière, à qui cette autorité a été déléguée par écrit.

Les personnes disposant de cette autorité peuvent autoriser des équipes spécifiques à les aider à gérer ces responsabilités.

- Autorité de classification des dérivés

La classification des dérivés consiste à paraphraser, à reformuler ou à générer sous une nouvelle forme des données ou des informations déjà classées. Ces actions comprennent généralement le marquage ou l'étiquetage de l'information nouvellement dérivée conformément aux marquages de classification de la source de l'information (p. ex., cette politique). Toutes les personnes qui accèdent aux données et aux informations et qui les enregistrent, les transmettent, les partagent ou les gèrent d'une autre manière sont des classificateurs des dérivés.

Les classificateurs des dérivés :

- ont des connaissances sur les données ou les informations ;
- ont une conscience générale du risque au niveau juridique, réglementaire, financier ou de la réputation, que présentent les données ou les informations
- reçoivent une formation initiale ou de remise à niveau, selon les recommandations du service de la cybersécurité ;
- évitent la classification excessive.

Comme les données et les informations peuvent parfois changer ou évoluer au cours de leur cycle de vie, les classificateurs des dérivés doivent être habilités à prendre ces décisions de classification et à solliciter les personnes disposant de l'ACI en cas de risques difficiles à déterminer en raison de contradictions ou de manque de clarté. Bien que les catégories de classification soient définies à l'article 5 ci-dessous, les exemples de catégories de classification qui changent sont les suivants :

- les résultats financiers trimestriels peuvent relever de la catégorie « restreinte » lorsqu'ils sont à l'état de projet, et « publique » après leur publication ;
- les informations contractuelles peuvent être « restreintes » pendant les négociations, puis considérées « internes » après l'exécution du contrat ;
- une note initialement classée « interne » peut devoir être reclassée « restreinte » si elle est en lien avec un litige ou une affaire juridique ;
- un rapport qui combine l'adresse de service avec d'autres informations sur le client (p. ex., le nom) peut devoir être reclassé en catégorie « restreinte ».

5. Catégories de classification des informations

Les données et les informations de WM sont classées en fonction du niveau d'impact sur WM, auquel on peut raisonnablement s'attendre en cas d'accès, d'acquisition, de divulgation, d'altération, de perte ou de destruction de ces informations sans autorisation appropriée. Les normes de classification permettent à WM d'identifier et de protéger les informations et d'établir et de maintenir le niveau de sécurité approprié pour les données et les informations.
Les documents et les systèmes sont classés selon le niveau de l'élément ou du contenu le plus restrictif qu'ils contiennent. Par exemple, si un système traite des numéros d'assurance sociale (« NAS »), il sera classé dans la catégorie « fortement restreint », quel que soit le nombre de NAS traités ou, le cas échéant, la proportion d'autres informations moins sensibles, susceptibles d'être également traitées par ce système.

La **procédure de classification et de traitement des informations** donne des exemples de catégories de données et d'informations, ainsi que les actions et les instructions de traitement afférentes.

Définitions des catégories de classification :

Catégorie	**Fortement restreinte**
Étiquette	Fortement restreinte (RH)
Définition	Cette classification concerne les informations considérées comme présentant le **niveau de risque le plus élevé** et nécessitant les contrôles de sécurité les plus stricts. La divulgation, l'altération, la compromission ou la destruction non autorisées d'informations très confidentielles risqueraient de causer de graves préjudices à WM ou aux personnes dont les informations ont été compromises. Les informations fortement restreintes comprennent également les informations dont on peut raisonnablement s'attendre à ce qu'elles exposent WM à un risque financier important, qu'elles suscitent une enquête, qu'elles engagent la responsabilité civile, qu'elles entrainent un désavantage concurrentiel et/ou à une non-conformité réglementaire. **Remarque :** le personnel de WM doit immédiatement signaler tout cas réel ou suspect d'accès non autorisé, de divulgation ou de compromission d'informations fortement restreintes. Signalez ces incidents à la direction locale et par courriel à InfoSec@wm.com.

Catégorie	**Restreinte**
Étiquette	Restreinte
Définition	Cette classification concerne les informations présentant un **risque moyen** et nécessitant des contrôles de protection de la sécurité. La divulgation, l'altération ou la destruction non autorisée d'informations restreintes peut avoir des **conséquences négatives** pour WM. Cela inclut les informations de WM qui peuvent l'exposer à des désavantages concurrentiels ou la disqualifier dans le cadre des appels d'offres.
Catégorie	**Interne**
Étiquette	Interne ou usage interne uniquement

	Cette classification concerne les informations qui présentent un **faible niveau** de risque et nécessitent des contrôles de protection de la sécurité. Les données et les informations professionnelles qui n'atteignent pas le niveau de risque défini par les catégories « fortement restreinte » ou « restreinte » et qui ne relèvent pas d'une diffusion publique sont classées dans la catégorie « interne ».
Catégorie	**Publique**
Étiquette	Publique ou usage public uniquement
Définition	Cette classification concerne les informations qui ne sont pas sensibles et qui présentent un **risque minimal** pour WM. Il s'agit d'informations facilement accessibles au public, y compris les rapports qui doivent être rendus publics, tel que l'exigent les autorités réglementaires. Les projets de documents ne relèvent pas d'une divulgation publique et sont donc classés comme « fortement restreints », « restreints » ou « internes » en fonction de la classification des informations sous-jacentes.

6. Application et conformité

Conformément au code de conduite de WM, à la politique de sécurité des ressources informatiques et des données (que tous les employés et les tiers disposant d'un compte de connexion WM sont tenus de lire et de signer), et aux documents contractuels de tierces parties, tous les individus ont des obligations légales, contractuelles et autres, de protéger toutes les informations de WM, y compris les informations collectées auprès de nos clients, nos fournisseurs, nos vendeurs, et d'autres tiers. Les violations intentionnelles qui ne respectent pas la procédure sur les exceptions sont passibles de mesures disciplinaires pouvant aller jusqu'à la cessation d'emploi, à la résiliation d'un contrat avec un tiers ou d'un accord de service, et/ou à des poursuites judiciaires. Toute demande d'exception en matière de classification des données doit être transmise à l'autorité de classification initiale appropriée pour être examinée.

7. Références et documents connexes

Politique de gestion de l'accès
Procédure de traitement des informations relatives aux paiements par carte
Politique en matière de ressources informatiques et de sécurité des données
Procédure et formulaire d'approbation de dérogation en matière de cybersécurité
Procédure de classification et de traitement des informations
Politique de préservation de la preuve
Politique de destruction des informations protégées
Politique de gestion des dossiers et des informations
Procédure de destruction des dossiers
Procédure de conservation des dossiers
Modèle de gestion des données d'entreprise WM (cliquer ici)

8. Approbation des dérogations

Les dérogations à cette politique doivent être obtenues auprès du propriétaire de la politique. Les dérogations doivent être demandées à l'aide de la procédure et du formulaire d'approbation de dérogation en matière de cybersécurité.

9. Historique de révision

La présente politique est un document évolutif qui est modifié en fonction des besoins pour tenir compte des changements apportés aux systèmes, aux opérations ou à

l'organisation. Les modifications apportées à ce document sont enregistrées dans la matrice de l'historique des versions ci-dessous.

Cette matrice de l'historique est conservée pendant toute la durée de vie du document et des systèmes associés.

n°	Date	Description	Version :	Auteur :
1	2022	publication initiale	1.0	Sandy Morgan
2				