PROCÉDURE DE CLASSIFICATION ET DE TRAITEMENT DES INFORMATIONS

1. Objet

Cette procédure décrit les moyens spécifiques pour sécuriser et gérer les données et les informations, conformément à la politique de classification et de traitement des informations. Pour chaque catégorie de classification, cette procédure fournit des exemples de données et d'information, des actions effectuées sur les données, et des instructions supplémentaires sur le traitement.
Cette politique remplace toute autre communication ou politique existante sur les sujets qu'elle aborde.

2. Champ d'application

Cette procédure concerne **toutes** les données et les informations de WM.

3. Rôles et responsabilités

Tous les employés de WM et les tierces parties qui ont accès aux données de WM (désignées collectivement ci-après « le personnel de WM » ou « les personnes assujetties ») sont responsables du traitement exact des données et des informations en fonction de la catégorie de classification.
Le non-respect de cette procédure 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) ;
- les propriétaires de données du domaine qui approuvent l'évaluation des risques concernant une tierce partie, selon une notation de risque élevé ou moyen ;
- le directeur principal de la cybersécurité qui approuve l'évaluation des risques concernant une tierce partie, selon une notation de risque élevé ou moyen
- le directeur principal de la gestion des données 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 contribution du directeur principal de la cybersécurité, du directeur principal de la gestion des données et des responsables de la gestion des données.

4. Activité de traitement des informations et exemples de classification

Le tableau ci-dessous comprend des instructions par défaut pour le traitement des données et des informations pour toutes les phases du cycle de vie : collecte, création, utilisation, partage, transmission, conservation et destruction.
Utilisez ce tableau pour prendre des décisions de routine concernant le traitement des données et des informations. Les données et les informations ci-présentes sont mentionnées à titre représentatif seulement. Si des données ou des informations spécifiques ne figurent pas dans cette liste ou en cas de doute sur les techniques de traitement et les contrôles appropriés, il convient de consulter le responsable des données, le propriétaire des données du domaine ou l'équipe de gouvernance en matière de cybersécurité pour obtenir des conseils supplémentaires (*voir les liens dans la section Rôles et responsabilités pour les coordonnées des personnes à contacter*).

Catégorie de classification	**Fortement restreinte**	**Restreinte**	**Interne**	**Publique**
Risque	**Élevé**	**Moyen**	**Faible**	**Minimal**
Données / Informations non professionnelles et exemples	Propriété intellectuelle désignée « fortement restreinte » • Secrets commerciaux • Code source	Propriété intellectuelle, sauf si elle est désignée comme fortement restreinte • Propriété intellectuelle de logiciels • Propriété intellectuelle en matière d'ingénierie et de fabrication	• Notes et lettres d'information (non sensitives) internes seulement • Plans d'affaires • Guides de vente	Lieu du siège social/adresse de l'entreprise Articles de revue professionnelle

Catégorie de classification	**Fortement restreinte**	**Restreinte**	**Interne**	**Publique**
Risque	**Élevé**	**Moyen**	**Faible**	**Minimal**
	Identifiants gouvernementaux • SSN (États-Unis) • SIN/NAS (Canada) • PAN (India) • Numéro de permis de conduire • Numéro de passeport • Numéro d'identifiant de l'État • Numéro d'identification fiscal Numéro de compte / autres identifiants • ID de compte • ID de connexion • Mot de passe • Numéro de police d'assurance • Nom de jeune fille de la mère • Géolocalisation précise du client	Technologie opérationnelle Informations sensitives • Données financières de la société (jusqu'à ce qu'elles soient publiques) • Données financières de l'employé (p. ex., les salaires) • Informations concurrentielles (p. ex., la tarification, les stratégies marketing) • Résultats d'audit (jusqu'à ce qu'ils soient publics) • Signature numérique / Image de signature	Coordonnées professionnelles Organigrammes Documents juridiques • Contrats de vente & de marketing • Documents sur le regroupement d'entreprises • Éléments de preuves à préserver	Documents publics de la SEC (commission américaine de change et de valeurs mobilières) Communiqués de presse Matériels marketing après leur publication Offres d'emploi publiques

	Informations sur les cartes de paiement / informations sur les transactions financières • Numéro de carte de débit • Numéro de carte de crédit • Numéro de compte bancaire • Numéro de compte bancaire international (IBAN) • Codes SWIFT Ethnicité / Race / Religion / Statut syndical / Sexe • Ethnicité / Race • Croyances religieuses / philosophiques • Affiliations professionnelles / syndicales • Orientation sexuelle Données biométriques, génétiques et médicales • Empreintes digitales • Photos/images du visage • Groupe sanguin • Échantillons prélevés sur le corps • Dossier médical • Informations en matière d'assurance maladie • Date de naissance			

Catégorie de classification	**Fortement restreinte**	**Restreinte**	**Interne**	**Publique**
Risque	**Élevé**	**Moyen**	**Faible**	**Minimal**
Exigences en matière de stockage				
Emplacement des données	Bureau de l'ordinateur/ordinateur portable et appareils mobiles enregistrés de l'entreprise Base de données et applications de logiciels-services autorisés de l'entreprise	Bureau de l'ordinateur/ordinateur portable et appareils mobiles enregistrés de l'entreprise Base de données et applications de logiciels-services autorisés de l'entreprise	Bureau de l'ordinateur/ordinateur portable et appareils mobiles enregistrés de l'entreprise Base de données et applications de logiciels-services autorisés de l'entreprise	Pas de restrictions
Protection de données électroniques (y compris ePHI et ePII et les données sur des appareils mobiles)	Authentication multifacteur Cryptage des données au niveau de l'ordinateur portable et de l'appareil mobile enregistré Surveillance en continu	Authentication multifacteur Cryptage des données au niveau de l'ordinateur portable et de l'appareil mobile enregistré	Authentification du mot de passe	Pas requis.
Protection des données physiques	Accès limité et contrôlé	Accès limité et contrôlé	Précautions raisonnables pour restreindre l'affichage et l'accès	Pas de restrictions
Instructions sur l'étiquetage				
Données électroniques	Étiqueter tout dispositif électronique (Word, Excel, PowerPoint courriels, et autres) avec la mention « fortement restreint »	Étiqueter tout dispositif électronique (Word, Excel, PowerPoint courriels, et et autres) avec la mention « confidentiel » lorsque c'est possible.	Toutes les données non étiquetées doivent être considérées « internes » sauf si elles sont définies ou étiquetées autrement.	Doivent être explicitement étiquetées « publiques » dans les classifications de données WM
Données physiques	Le lieu de stockage (armoire, dossier, etc.) etc.) doit être explicitement étiqueté. Les documents doivent être étiquetés puisqu'ils sont déplacés.	Le lieu de stockage (armoire, dossier, etc.) etc.) doit être explicitement étiqueté. Les documents doivent être étiquetés puisqu'ils sont déplacés, lorsque c'est possible.	Toutes les données non étiquetées doivent être considérées « internes » sauf si elles sont étiquetées ou définies autrement.	Le lieu de stockage (armoire, dossier, etc.) etc.) doit être explicitement étiqueté. Les documents publics générés par WM doivent être étiquetés puisqu'ils sont déplacés

Contrôles d'accès				
Personne autorisant l'accès	Le propriétaire ou le responsable de données désigné par quelqu'un	Le propriétaire ou le responsable de données désigné par quelqu'un	Le propriétaire ou le responsable de données désigné en raison de ses fonctions	Pas de restrictions
Transmission				
par courriel	Données cryptées seulement. Il est demandé destinataires externes de courriel de respecter un accord de non-divulgation ou des obligations de confidentialité.	Données cryptées seulement lorsque c'est possible, et il est demandé destinataires externes de courriel de respecter un accord de non-divulgation ou des obligations de confidentialité.	Pas de restrictions externes. Il est demandé destinataires externes de courriel de respecter un accord de non-divulgation ou des obligations de confidentialité.	Pas de restrictions
par partage de document	Données cryptées. Données par courriel WM seulement ou via une plateforme de partage de contenu autorisée.	Données cryptées seulement lorsque c'est possible. Données par courriel WM seulement ou via une plateforme de partage de contenu autorisée.	Données par courriel WM seulement ou via une plateforme de partage de contenu autorisée.	Pas de restrictions

Catégorie de classification	**Fortement restreinte**	**Restreinte**	**Interne**	**Publique**
Risque	**Élevé**	**Moyen**	**Faible**	**Minimal**
Transferts de données de grande taille	Consulter les services juridiques, de cybersécurité, et le responsable/propriétaire des données	Consulter les services juridiques, de cybersécurité, et le responsable/ propriétaire des données	Consulter les services juridiques, de cybersécurité, et le responsable/ propriétaire des données	Pas de restrictions
Imprimer/Copier				
Imprimer	Le responsable ou le propriétaire des données délègue l'impression. Si l'application d'impression utilisée n'est pas sécurisée, il doit être présent à l'imprimante.	Le responsable ou le propriétaire des données délègue l'impression. Si l'application d'impression utilisée n'est pas sécurisée, il doit être présent à l'imprimante.	Le responsable ou le propriétaire des données délègue l'impression. Si l'application d'impression utilisée n'est pas sécurisée, il doit être présent à l'imprimante.	Pas de restrictions
Copier	Copies sur site. Un contrat de fournisseur approuvé est requis pour les copies à l'extérieur. Déchiqueter les mauvaises feuilles de tirage et les dépassements d'impression.	Copies sur site. Un contrat de fournisseur approuvé est requis pour les copies à l'extérieur. Déchiqueter les mauvaises feuilles de tirage et les	Privilégier les copies sur site. Déchiqueter ou jeter au rebut les mauvaises feuilles de tirage et les	Toute restriction

		dépassements d'impression.	dépassements d'impression. Si les copies sont effectuées à l'extérieur, le document original doit être retourné à l'entreprise et les mauvaises impressions détruites par le fournisseur.	
Méthodes de destruction				
Données électroniques	Suivre les procédures de destruction des dossiers et la politique de destruction des informations protégées	Suivre les procédures de destruction des dossiers et la politique de destruction des informations protégées	Suivre les procédures de destruction des dossiers et la politique de destruction des informations protégées	Toute restriction
Données physiques	Déchiquetées	Déchiquetées	Déchiquetées ou mises au rebut.	Toute restriction

5. Instructions supplémentaires pour le traitement et la sécurisation des informations

La politique de gestion des dossiers et des informations définit le traitement des dossiers de l'entreprise. La politique de destruction des informations protégées définit le traitement des informations protégées afin de garantir le respect des exigences légales fédérales et provinciales.

Sauf dans le cas de relations professionnelles ou juridiques préalablement approuvées, les données WM ne sont traitées que sur des équipements WM approuvés. Tout traitement de données sur le système informatique d'un tiers doit suivre les procédures établies de gestion des risques des tiers et, en cas de risque élevé ou moyen, doit être approuvé à l'avance par le propriétaire des données du domaine et le directeur principal de la cybersécurité.

Il est interdit au personnel de WM d'envoyer des données ou des informations WM à des comptes externes, sauf en cas (1) d'autorisation préalable du propriétaire des données du domaine ou du responsable des données, et (2) de la nécessité de les transmettre pour la conduite des activités de WM.

1. Informations fortement restreintes

- Le cryptage doit être utilisé lors de la transmission ou du stockage de données et des informations fortement restreintes, sur les systèmes WM ou dans les dépôts de données WM, situés dans les locaux ou le nuage informatique.

2. Informations restreintes

- Pour les projets et les documents afférents qui comportent des exigences spécifiques en matière de traitement des informations contrôlées et non classifiées, il convient de se référer à ces instructions au cas par cas.

- En raison de la nature et de la diversité des informations à diffusion restreinte, les contrôles de protection de la sécurité peuvent varier en fonction du domaine de données.
- Par défaut, sauf indication contraire de la réglementation ou de l'autorité de classification d'origine, il convient, dans la mesure du possible, d'utiliser le cryptage lors de la transmission ou du stockage de données et d'informations restreintes sur les systèmes WM ou dans les dépôts de données WM, situés dans les locaux ou le nuage informatique.

6. Application et conformité

Conformément (1) à la politique de sécurité des ressources informatiques et des données selon laquelle tous les employés et les tiers disposant d'un compte de connexion WM sont tenus de lire et de signer, (2) au code de conduite de WM, et (3) aux documents contractuels de tierces parties, tous les individus sont soumis à diverses obligations notamment légales, et contractuelles visant à 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 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 de l'information
- 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 en vigueur. 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 la révision

La présente procédure est un document évolutif qui est modifié en fonction des besoins pour tenir des 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	Octobre 2022	Publication initiale	1.0	Sandy Morgan
2				