

POLITIQUE EN MATIÈRE DE RESSOURCES INFORMATIQUES ET DE SÉCURITÉ DES DONNÉES

Objet :

Communiquer les objectifs de la direction concernant l'utilisation acceptable des ressources fournies par la société et l'utilisation de données sécurisées par tous les employés et les agents de WM (désignés ci-après les « Utilisateurs ») et de ses filiales (désignés collectivement ci-après « WM » ou la « Société »).

Cette politique s'applique à tous les équipements appartenant à la Société ou loués par elle, aux équipements de transmission de données, aux dispositifs de stockage de données, aux imprimantes, aux dispositifs d'affichage et aux données, et ce quel que soit l'emplacement de l'équipement ou des données. Cette politique s'applique également aux appareils personnels lorsqu'ils sont utilisés dans le cadre des activités de la Société. Toutes les méthodes autorisées par la Société pour sécuriser les ressources informatiques (c'est-à-dire l'accès aux installations informatiques, l'accès à la sécurité, les informations sur les comptes de la Société et les mots de passe) sont également incluses dans cette politique.

Politique :

La Société fournit des ressources qui sont essentielles aux fonctions administratives pour l'ensemble de WM. L'utilisation de ces ressources est accordée au personnel dans le but explicite d'accomplir son travail. Il s'agit, par exemple, des ordinateurs, du courrier électronique et de l'accès à l'Internet/Intranet.

Tous les employés et les agents (désignés ci-après les « Utilisateurs ») :

- ont le devoir et la responsabilité personnelle de protéger les informations confidentielles dans le cadre de leur relation professionnelle avec WM ;
- doivent se conformer aux mesures de sécurité informatique et aux procédures de protection contre les virus ;
- doivent traiter les informations telles que les mots de passe, les codes d'identification et les autres informations confidentielles de manière sécurisée.

En conséquence, cette politique fournit des orientations en matière :

- d'utilisation ;
- d'accès aux ressources informatiques de WM ;
- des biens de la Société.

Le manuel de l'employé, qui peut être obtenu auprès d'un représentant local des ressources humaines, fournit des informations supplémentaires concernant l'utilisation et l'accès aux biens de la Société tels que le courrier électronique et Internet. Il est mis à jour périodiquement et si des informations diffèrent des détails contenus dans le présent document, il convient de se référer au manuel de l'employé.

Utilisation

La messagerie vocale, le courrier électronique et le réseau informatique de WM, y compris les logiciels et l'accès à Internet (désignées ci-après les « Systèmes »), sont mis à la disposition de ses employés, de ses contractants, de ses fournisseurs et d'autres personnes sélectionnées (ci-après désignés les « Utilisateurs autorisés ») pour l'exécution de leurs tâches professionnelles au sein de WM et des activités qui y sont liées.

L'accès aux services de courrier électronique et d'Internet/Intranet fournis par la Société doit être approuvé. Avant de pouvoir accéder aux services de courrier électronique et

d'Internet/Intranet fournis par la Société, l'Utilisateur autorisé est tenu d'accuser réception, de comprendre la présente politique, et de signer une déclaration d'acceptation.

Internet

L'Internet est un outil commercial utile et les Utilisateurs autorisés doivent faire preuve de discernement dans l'utilisation de cet outil. L'utilisation des ressources informatiques de la Société pendant le temps de travail à des fins autres que celles spécifiquement autorisées est interdite. Le « Temps de travail » désigne le temps pendant lequel une personne est occupée ou devrait être occupée à effectuer son travail pour la Société. L'utilisation personnelle des services de courrier électronique et d'Internet/Intranet fournis par la Société est autorisée en dehors du Temps de travail, à condition qu'elle n'enfreigne pas les politiques de la Société, qu'elle n'affecte pas négativement le fonctionnement de ces Systèmes ou qu'elle n'entrave pas de manière substantielle la productivité.

Toutes les informations publiées sur Internet au nom de WM doivent être approuvées par le département approprié de la Société et être conformes à la politique de la Société en matière de communication d'informations au public.

La Société se réserve le droit d'accorder, de restreindre ou de supprimer à tout moment l'accès aux sites Web. L'accès à Internet est surveillé et les connexions réelles aux sites Web sont enregistrées à des fins de gestion légitime. Toute utilisation inappropriée peut entraîner la perte des privilèges d'accès et/ou d'autres mesures appropriées.

Médias sociaux

Les médias sociaux peuvent inclure, sans s'y limiter, les sites de réseautage, les pages Web personnelles, les blogues, les vidéos, les balados, les clavardages en direct, les forums de discussion sur Internet, les micromessages, les textos et les messages instantanés. En tant qu'Utilisateur autorisé, l'utilisation des médias sociaux pour publier des informations, des commentaires et échanger des idées concernant WM ou ses activités, comprend l'obligation d'agir de manière responsable.

WM a développé des lignes directrices auxquelles les personnes doivent adhérer lorsqu'ils utilisent les médias sociaux (ou d'autres technologies similaires) pour publier des informations, des commentaires ou échanger des idées concernant WM ou ses activités :

- connaître et respecter les politiques et les règles de WM ;
- ne pas divulguer les informations confidentielles et exclusives de WM ou d'une tierce partie ;
- ne pas publier d'informations ou de déclarations qui dénigrent les clients, les partenaires ou les fournisseurs ;
- ne pas parler au nom de WM ;
- chaque Utilisateur autorisé est personnellement responsable (et tenu responsable) du contenu de toute publication ;
- ne pas discréditer les services ou les produits de WM ;
- ne pas utiliser les médias sociaux en conduisant ou en utilisant les machines de la Société ou l'équipement que nous fournissons. Toute utilisation personnelle des médias sociaux pendant les heures de travail doit être réduite au minimum et se conformer à toutes les politiques applicables de la Société.

Le non-respect de ces lignes directrices peut entraîner des mesures disciplinaires, y compris la cessation d'emploi. Il est interdit d'exercer des représailles à l'encontre d'une personne qui aurait signalé un éventuel écart ou qui aurait coopéré à une enquête. Des informations plus détaillées sur ces lignes directrices figurent dans le manuel de l'employé.

Courriel

Un courriel est considéré par la Société comme une forme de communication non permanente et les messages doivent être rapidement supprimés après utilisation. Les courriels stockés dans des dossiers ou archivés ne doivent être conservés que tant qu'ils restent utilisés et doivent être supprimés par la suite. Il existe une dérogation à cette politique lorsqu'un Utilisateur autorisé reçoit un avis du département juridique selon lequel les courriels doivent être conservés. Les Utilisateurs autorisés recevant une telle notification recevront des instructions spécifiques concernant la conservation des courriels qu'ils doivent suivre.

Les destinataires de messages ou d'informations envoyés par inadvertance ou mal adressés ne doivent pas copier, conserver ou divulguer le contenu de ces messages. Conformément à la politique de la Société, il convient de supprimer de tels messages et d'en informer, si possible, l'expéditeur du message mal adressé ou mal dirigé.

Messagerie vocale, Systèmes informatiques

Les Systèmes, les messages connexes, les documents et les informations reçus, stockés et traités par le système sont et restent la propriété de WM. Tous les codes d'accès aux Systèmes doivent être disponibles pour WM et les personnes ne peuvent pas utiliser des codes d'accès inconnus de WM. Il est interdit aux Utilisateurs autorisés d'utiliser sans autorisation le code d'accès d'autres personnes et d'accéder ou de tenter d'accéder sans autorisation à des zones interdites des Systèmes, telles que les dossiers du personnel, les informations comptables, etc.

Les logiciels nécessaires à l'exercice des fonctions de chaque Utilisateur autorisé au sein de WM sont installés sur le réseau et doivent être utilisés en stricte conformité avec les licences applicables. Il est strictement interdit aux Utilisateurs autorisés (i) de reproduire sans autorisation des programmes logiciels pour les utiliser chez WM ou ailleurs, et (ii) d'installer ou de télécharger des logiciels à partir d'Internet sur le réseau de WM ou sur toute unité centrale de WM, ou de télécharger des logiciels à partir d'Internet sans l'autorisation expresse du directeur principal de la cybersécurité.

Nonobstant l'interdiction d'accès non autorisé, WM ne peut pas garantir que les fichiers, les messages, les documents et les autres informations stockés, créés, récupérés ou transmis par une personne resteront confidentiels. De plus, WM se réserve le droit d'accéder, d'examiner et d'utiliser à n'importe quelle fin tous les messages et/ou informations sur ses Systèmes, à tout moment, sans notification, sur une base régulière ou aléatoire, et sans tenir compte de :

- l'utilisation de mots de passe ou de codes d'accès ;
- qui a composé, placé ou reçu l'information, le document ou le message.

Accès aux ressources informatiques de WM

Seuls les logiciels approuvés par la Société peuvent être utilisés lors de la connexion à Internet via le réseau de la Société. Les identifiants de compte et les mots de passe des services sont strictement réservés à l'usage de l'Utilisateur autorisé et ne doivent pas être partagés ou rendus accessibles à d'autres personnes. Dans les cas où les mots de passe doivent être fournis à d'autres personnes pour obtenir l'accès à l'ordinateur, par exemple lors de la maintenance ou de la réparation du Système, un nouveau mot de passe doit être créé et utilisé une fois ce processus effectué.

L'accès aux ressources informatiques de l'entreprise sera enregistré (journalisé). Les enregistrements seront conservés selon les exigences de la fonction administrative bénéficiant de ce soutien informatique, ainsi que des exigences techniques et juridiques. La

Société a le droit d'utiliser ces enregistrements à des fins commerciales et d'enquête, y compris pour identifier les personnes qui utilisent abusivement les ressources informatiques de WM.

Connexions externes

Il est interdit à toute personne non autorisée de se connecter au réseau privé de WM. Il convient de reconnaître que, dans certaines conditions, ces actions peuvent également constituer une violation des lois étatiques, provinciales et/ou fédérales.

Les employés, les contractants, les fournisseurs et les autres personnes susceptibles d'avoir accès aux réseaux de la Société ne doivent prendre aucune mesure susceptible de bloquer ou de restreindre les efforts menés par la Société pour surveiller ou gérer ces ressources.

Accès à distance

WM fournit un « accès à distance » au réseau privé de la Société pour permettre aux employés et aux autres Utilisateurs autorisés de prendre en charge certaines fonctions administratives. Il expose également le réseau de la Société à des risques supplémentaires d'intrusion non autorisée. Dans les connexions d'accès à distance, le niveau et le type de sécurité appliqués sur le lieu éloigné sont l'un des principaux facteurs permettant de déterminer si les informations de la Société sont suffisamment protégées. Les connexions d'accès à distance feront l'objet d'un contrôle aléatoire périodique pour des raisons professionnelles.

WM exige que la responsabilité individuelle soit maintenue à tout moment. Pour garantir la responsabilité individuelle lors de l'accès à distance aux ressources de WM, l'identification et l'authentification de la personne qui tente d'accéder aux ressources seront vérifiées avant que la connexion ne soit établie.

Une autorisation appropriée de la direction de WM est requise pour accéder aux ressources informatiques de la Société à partir d'un site distant. Cette autorisation s'ajoute à toutes les autres autorisations d'accès qui peuvent exister. Les codes d'accès ne seront pas partagés. L'autorisation d'accès à distance est accordée spécifiquement à une personne et ne doit pas être partagée sans l'autorisation expresse de la direction de WM.

Accès sans fil

Les connexions sans fil aux réseaux et ressources de WM sont réservées à l'usage professionnel des employés de WM et des personnes travaillant avec ou pour WM. Le département numérique gèrera et contrôlera les appareils sans fil afin de maintenir la disponibilité sans fil dans le cadre de paramètres spécifiés. Le département de la cybersécurité surveillera également le réseau sans fil de WM afin de garantir uniquement l'accès autorisé et de surveiller en permanence les intrusions. Les Utilisateurs non autorisés seront exclus du service.

Biens de la Société

Les employés et les autres Utilisateurs autorisés sont tenus d'assurer un contrôle et une protection raisonnables des biens de la Société qui leur ont été remis ou confiés. L'utilisation du temps, des équipements, des fournitures et des installations de la Société à des fins personnelles doit être raisonnable et conforme à la loi. L'utilisation d'équipements appartenant à la Société en dehors de ses locaux à des fins personnelles n'est autorisée que si elle a été préalablement approuvée par le gestionnaire de la personne concernée.

Les ordinateurs capables d'accéder en direct aux services de courrier électronique et d'Internet/Intranet fournis par la Société ne doivent pas être laissés sans surveillance. Les

informations relatives à la Société doivent être protégées lorsqu'elles sont stockées ou transmises par l'intermédiaire des services.

Alors que notre politique vise à respecter la vie privée, les employés et autres Utilisateurs autorisés doivent reconnaître que les ordinateurs, les téléphones et les espaces de travail appartiennent à la Société et sont mis à leur disposition à des fins professionnelles. La Société se réserve le droit de surveiller et de rechercher tous ses biens.

Biens liés aux technologies de l'information

Tous les Utilisateurs autorisés sont tenus de s'assurer que les contrôles de cybersécurité (y compris la protection par mot de passe du Système) sont effectués de manière à préserver les objectifs de sécurité que sont la confidentialité, l'intégrité et la protection des biens informationnels de WM.

Biens de matériel de bureau

Le téléphone de bureau, le télécopieur, les services de vérification de crédit, les photocopieuses, UPS et autres services de livraison sont réservés à des fins professionnelles. Il est admis que certains appels téléphoniques ou télécopies personnels peuvent être nécessaires, mais ils doivent être réduits au minimum et ne doivent pas enfreindre les politiques de la Société, affecter négativement le fonctionnement de ces Systèmes ou entraver de manière substantielle la productivité. Toute utilisation abusive du téléphone ou de l'un des services susmentionnés qui sera signalée peut donner lieu à des mesures disciplinaires pouvant aller jusqu'à la cessation d'emploi.

Biens de téléphonie mobile

Il est interdit aux employés de la Société et aux autres Utilisateurs autorisés d'utiliser un appareil de communication personnel ou de la Société lorsqu'ils conduisent ou utilisent un véhicule ou un équipement mobile appartenant à la Société ou loué par elle. Tous les Utilisateurs autorisés doivent respecter les restrictions locales, provinciales ou fédérales concernant l'utilisation d'appareils de communication en conduisant, lorsque ces restrictions sont plus contraignantes que la présente politique.

Veillez vous référer à la [Politique en matière d'appareils mobiles](#) pour plus d'informations sur l'utilisation des cellulaires.

Appareils informatiques mobiles

Les personnes qui accèdent ou conservent une copie des informations de WM sur des appareils mobiles tels que des ordinateurs portables, des disques externes ou des assistants numériques communicants sont responsables de la protection de ces dispositifs. Les personnes doivent prendre des mesures raisonnables pour protéger ces appareils, et les informations qu'ils contiennent, contre la perte ou le vol. En cas de perte ou de vol, le département de la sécurité doit être immédiatement informé.

Veillez consulter la [Politique de classification et de traitement de l'information](#) pour plus de détails sur les informations confidentielles.

La divulgation non autorisée constitue une violation de la politique de la Société et, dans certains cas, peut également constituer une violation de la loi pouvant entraîner des amendes, des pénalités ou des poursuites judiciaires à l'encontre de WM et/ou des personnes impliquées. De plus, toute violation de ces politiques par un employé de la Société ou par toute personne autre qu'un employé de la Société peut entraîner des mesures disciplinaires pouvant aller jusqu'à la cessation d'emploi ou à la résiliation d'un contrat ou d'un accord de service.