

## **POLITIQUE D'UTILISATION DES APPAREILS MOBILES**

### **Politique :**

Waste Management (la « Société ») reconnaît que l'accès aux systèmes d'information de la Société à l'aide d'un appareil mobile est plus commode pour les utilisateurs (les employés) et augmente leur productivité. Dans le même temps, un appareil mobile peut présenter certains risques pour la Société. Les utilisateurs peuvent mener les activités de la Société et accéder aux systèmes d'information de la Société à condition qu'ils se conforment pleinement à la présente politique et qu'ils respectent l'accord d'utilisation des appareils mobiles de la Société. Toute violation peut entraîner la perte du privilège d'utiliser un appareil mobile pour accéder aux systèmes d'information de la Société, ainsi que des mesures disciplinaires pouvant aller jusqu'à la cessation d'emploi.

### **Objet :**

La présente politique vise à définir les exigences relatives à l'utilisation des appareils mobiles tout en réduisant les risques pour la Société. Cette politique vise, en particulier, à :

- a. protéger les systèmes d'information de la Société contre les logiciels et les codes malveillants ;
- b. empêcher l'accès non autorisé aux informations sensibles de la Société, ainsi que leur utilisation, leur divulgation ou leur acquisition ;
- c. veiller à ce que la Société puisse, à tout moment, obtenir l'accès aux informations de la Société et exercer un contrôle sur celles-ci.

La présente politique concerne l'utilisation de tout appareil mobile en vue d'accéder aux ressources de la Société, effectuer des tâches pour la Société ou accéder aux systèmes d'information de la Société par le biais d'appareils mobiles ou de plans de service pour appareils mobiles payés par la Société. Elle ne concerne pas les ordinateurs portables ou autres ordinateurs personnels complets, car ces appareils relèvent d'autres politiques, telles que la politique en matière de ressources informatiques et de sécurité des données.

### **Définitions**

- « Informations » désigne les données numériques sous quelque forme que ce soit, y compris, mais sans s'y limiter, les textos, les courriels, les images, le son et les vidéos
- « Systèmes d'information » désignent tous les systèmes détenus ou loués par la Société qui sont utilisés pour stocker, traiter ou transmettre des Informations, y compris, mais sans s'y limiter, les réseaux locaux ou régionaux, l'accès à Internet, l'intranet de la Société et les systèmes de courriel et de messagerie vocale de la Société
- « Appareil mobile » désigne tout appareil de stockage électronique portable (p. ex. Blackberry, iPad, iPhone ou autre téléphone intelligent, tablette ou technologie portable) utilisé par l'employé pour mener les activités de la Société et/ou accéder aux Systèmes d'information de la Société
- « Appareil mobile personnel » désigne tout appareil mobile acheté par l'employé et utilisé pour accéder aux Systèmes d'information de la Société
- « Informations sensibles de la Société » désigne toute information classée ou maintenue « confidentielle » par la Société, conformément à la politique de classification des informations

### **Sécurité**

La sécurité des employés et des entrepreneurs de WM est d'une importance capitale. Il est interdit aux employés et aux entrepreneurs de WM d'utiliser un appareil mobile personnel ou appartenant à WM lorsqu'ils conduisent ou utilisent un équipement mobile appartenant à WM.

Les véhicules et les équipements mobiles comprennent, sans s'y limiter,

- tous les véhicules appartenant à la Société, commerciaux et non commerciaux ;
- les équipements lourds et légers ;
- les véhicules hors route c.-à.-d les véhicules tout-terrain.

Il est interdit de répondre aux appels entrants, aux messages ou aux courriels, de les lire ou d'y répondre en conduisant ou en actionnant les commandes d'un véhicule ou d'un autre équipement mobile. Il est interdit d'accéder aux applications ou aux autres fonctionnalités de l'appareil ou de les utiliser pendant la conduite d'un véhicule. Dès qu'il est possible de le faire de manière sécuritaire, arrêtez le véhicule ou l'équipement dans une zone où il n'y a pas de risque d'accident ou de danger pour les autres et répondez au téléphone ou rappelez la personne qui vous a téléphoné. Les appels sortants, les messages ou les courriels ne peuvent être initiés, créés ou envoyés en conduisant ou en utilisant les commandes d'un véhicule ou d'un autre équipement mobile.

Tous les employés doivent respecter les restrictions locales, nationales ou provinciales concernant l'utilisation d'appareils de communication au volant, lorsque ces restrictions sont plus contraignantes que la présente politique.

### **Approbation, remboursement et acquisition**

Tous les employés doivent obtenir l'approbation de leur superviseur ou de leur gestionnaire direct avant d'utiliser un appareil mobile pour accéder à des informations de la Société ou effectuer des tâches pour le compte de la Société. Les employés sont tenus de signer l'accord d'utilisation des appareils mobiles de la Société dans le cadre de la procédure d'approbation.

Toute personne autorisée en vertu de la présente politique à utiliser un appareil mobile appartenant à la Société a droit à un appareil de la Société standard fourni par Société. Les utilisateurs peuvent avoir plus d'un appareil standard fourni par la Société et un forfait de services payé par la Société. Toutefois, tout écart par rapport au plan de service doit être approuvé au niveau du vice-président ou du chef de service.

Les utilisateurs d'appareils mobiles personnels doivent respecter les dispositions de la présente politique et celles de l'accord d'utilisation des appareils mobiles de la Société afin de pouvoir connecter leurs appareils aux Systèmes d'information de la Société. La Société ne rembourse aucuns équipement ou frais de service et d'utilisation récurrents pour les appareils personnels, sauf si la loi l'exige lorsqu'ils sont utilisés dans le cadre des activités de la Société. Pour les appareils mobiles appartenant à la Société, l'acquisition de nouveaux équipements mobiles et les transactions de facturation périodiques doivent être placées dans le portail TEMS (Telecom Expense Management System). Le portail TEMS est situé sur Visor, <http://visor.wm.com/Pages/default.aspx> sous l'onglet des applications de WM.

Les appareils personnels fabriqués par les sociétés Huawei Technologies, ZTE Corporation ou toute filiale ou société affiliée de ces entités sont spécifiquement interdits pour mener les activités de la Société ou pour accéder aux informations de la Société.

### **Minutage**

Les salariés rémunérés à l'heure ou non exemptés peuvent bénéficier d'un appareil mobile appartenant à la Société avec l'approbation du vice-président ou du chef de service concerné. Il est interdit à ces employés d'utiliser un appareil mobile pour mener des activités de la Société en dehors du temps de travail prévu, sauf si c'est conforme avec la politique

de comptabilisation du temps de la Société, telle qu'elle est décrite dans le manuel de l'employé et dans la base de données de la politique.

### **Sécurité**

Pour pouvoir utiliser un appareil mobile, l'utilisateur doit autoriser le département numérique à configurer l'appareil et à mettre en œuvre des contrôles de sécurité, jugés nécessaires par la Société, à sa seule discrétion, pour protéger l'intégrité des informations et des Systèmes d'information de la Société.

Ces contrôles de sécurité peuvent inclure, sans s'y limiter, le cryptage, la protection par mot de passe, la capacité d'effacement à distance, le verrouillage de l'appareil après des périodes d'inactivité, le verrouillage de l'appareil ou la suppression des données après la saisie d'un mot de passe non valide, et les logiciels antivirus et anti-programmes malveillants. La Société peut activer ou installer une application de localisation à distance pour aider à localiser l'appareil mobile en cas de perte ou de vol. Il est interdit aux utilisateurs de contourner, de modifier, de désactiver ou de supprimer les contrôles de sécurité mis en place par la Société sans l'accord préalable du département numérique.

Les utilisateurs ne doivent pas télécharger ou accéder à du contenu qui violerait toute autre politique de la Société et restent responsables de leurs actions à cet égard.

Les utilisateurs doivent prendre des mesures raisonnables pour protéger les appareils mobiles appartenant à la Société ainsi que les appareils personnels contre la perte ou le vol et pour empêcher l'accès non autorisé aux informations de l'entreprise stockées sur l'appareil mobile, ainsi que l'utilisation, la divulgation ou l'acquisition de ces informations. Il s'agit notamment de mettre à jour tous les logiciels (y compris les systèmes d'exploitation).

Le département numérique de la Société peut établir des critères minimaux pour les appareils mobiles, tels que le fabricant du matériel, la version du système d'exploitation, et interdire/empêcher les appareils mobiles qui ne répondent pas à ces critères d'accéder aux Informations de la Société.

La Société peut accéder à ces appareils mobiles conformément à la politique relative aux ressources informatiques et à la sécurité des données, notamment pour contrôler le volume et le contenu du trafic de communication (p. ex., l'Internet, les courriels, les textos, les messages instantanés, les messages vocaux, les photos, le calendrier et la liste de contacts), maintenir le contrôle et la sécurité des données de la Société, assurer l'assistance technique, la réparation et la gestion des logiciels, garantir la continuité des processus de travail, améliorer les processus de travail et gérer la productivité, ainsi que pour garantir le respect des politiques applicables et de la loi. La Société peut utiliser des fonctions de surveillance disponibles par l'intermédiaire de son logiciel de gestion des appareils mobiles ou via les fonctionnalités intrinsèques de l'appareil mobile.

La Société peut avoir besoin d'un accès physique à un appareil mobile à des fins professionnelles légitimes, par exemple pour enquêter sur des allégations de violation de la politique ou pour suspendre l'accès en cas de litige. La Société fera la demande d'accès à un appareil mobile, à sa discrétion, afin que la Société puisse inspecter les informations stockées sur l'appareil aux fins susmentionnées ou à d'autres fins professionnelles légitimes. Sur demande, les utilisateurs doivent présenter leur appareil mobile à l'inspection dans un état qui rend l'inspection possible. Plus précisément, les utilisateurs fourniront sur demande les codes NIP, les codes d'accès ou les mots de passe de cryptage de sauvegarde de l'appareil mobile. La Société peut également demander aux utilisateurs de fournir les factures mensuelles de l'appareil mobile à des fins d'inspection dans le cadre d'une enquête

menée par la Société. Dans ce cas, la Société demandera à l'utilisateur de supprimer les informations sans rapport avec l'objet de la demande.

Lorsqu'un représentant de la Société accède à des informations stockées sur un appareil mobile, il fait des efforts raisonnables pour limiter l'accès aux informations de la Société et à d'autres informations pertinentes pour l'objet de l'inspection. Toutefois, l'inspection peut entraîner un accès fortuit à des Informations stockées sur l'appareil mobile qui n'ont rien à voir avec cet objectif ou qui n'ont rien à voir avec la Société.

### **Discipline**

La Société peut suspendre ou mettre fin au privilège d'utiliser un appareil mobile pour accéder aux Systèmes d'information de la Société, à tout moment, à sa seule discrétion, en réponse à une violation de la présente politique ou pour tout autre raison. De plus, les utilisateurs sont responsables de la protection des Informations de la Société qui sont stockées sur un appareil mobile. Ils seront également tenus responsables de leurs actions qui exposent les informations de la Société à des tiers non autorisés. Tout utilisateur qui enfreint la présente politique peut faire l'objet de mesures disciplinaires (en plus de la suspension ou de la perte de privilèges), pouvant aller jusqu'à la cessation d'emploi.

### **Exigences d'approbation :**

Tout écart par rapport au plan de service inclus dans ce document doit être approuvé au niveau du vice-président/chef de département. Les utilisateurs d'appareils mobiles personnels doivent se conformer aux dispositions énoncées dans la présente politique et dans l'accord d'utilisation des appareils mobiles de la Société afin de pouvoir connecter leurs appareils aux Systèmes d'information de la Société.