POLITIQUE DES TECHNOLOGIES DE L'INFORMATION

Section 1 : Introduction – Objectif, portée et applicabilité

Cette politique en technologies de l'information (« Politique TI ») établit la gouvernance et l'utilisation acceptable des systèmes de technologie de l'information (« TI ») de McWane, Inc. (« McWane »).

Les termes suivants sont définis par la présente et ont la(s) signification(s) suivante(s), telle qu'utilisée tout au long de ce document :

- « Société » désignera McWane, Inc., ses divisions, filiales et affiliés.
- « TI d'entreprise » désigne le département TI opérant depuis le siège social de l'entreprise et inclut des équipes ou des membres désignés travaillant sous la supervision du personnel TI corporatif.
- « Division » ou « Divisions » désigne toutes les sociétés opérant sous McWane, Inc., y compris toutes les divisions, filiales et affiliées.
- La « TI de la Division » inclut tout le personnel, employé par les divisions, qui participe au soutien des systèmes informatiques.
- « Système(s) TI de l'entreprise » inclut tous les systèmes informatiques d'entreprise et tous les systèmes informatiques exploités par une division de la société; et
- « Système(s) TI d'entreprise » doit être défini(s) plus en détail comme suit :

    - « Réseau » – tout l'équipement, les technologies, les applications ou autres éléments utilisés pour interconnecter les systèmes et le personnel de la Compagnie, y compris celui utilisé pour connecter le réseau interne McWane à Internet, ainsi que toute autre technologie utilisée pour la communication entre divisions.

    - « Points d'extrémité » – tout ordinateur de bureau ou portable, tablette, téléphone, appareil mobile, écran vidéo ou similaire.

    - « Équipement de livraison de services TI » – inclut l'équipement d'infrastructure tel que serveurs, routeurs, commutateurs, contrôleurs et autres, qui sont utilisés pour fournir des services technologiques aux utilisateurs à travers le réseau McWane, ou tout segment de celui-ci; et,

    - « Connectivité Internet » – le réseau mondial de connectivité technologique qui offre des capacités de communication et l'accès à des agences externes, partenaires commerciaux et autres organisations, via le réseau McWane.

Les lignes directrices et procédures contenues ici visent à fournir des contrôles concernant l'accès à l'information, la sécurité et la propriété des informations et données qui peuvent exister ou être transmises entre les systèmes informatiques de l'entreprise.

Cette politique TI s'applique à, et ses directives et procédures doivent être suivies par tous les employés de l'entreprise (ou « membres de l'équipe »); il s'applique aussi aux agents et aux tiers ayant obtenu un accès accrédité aux systèmes informatiques de l'entreprise.

Le non-respect de cette politique informatique peut entraîner la résiliation de tout accès accordé et/ou des mesures disciplinaires, menant jusqu'à la fin de l'emploi avec l'entreprise. Cela peut aussi inclure des poursuites civiles et/ou criminelles en vertu des lois fédérales ou provinciales applicables.

Le personnel TI de l'entreprise, ainsi que celui de la division, partagent la responsabilité d'assurer le respect de cette politique informatique globale. Le personnel TI de l'entreprise est responsable de l'acquisition, du développement, de la mise en œuvre et de la gestion des ressources d'infrastructure informatique à usage courant à travers l'entreprise. Les cadres supérieurs et/ou cadres de chaque division sont responsables de la performance des ressources TI qui relèvent exclusivement de cette division. Le personnel TI de la Division ou d'autres personnes peut demander l'aide du département TI corporatif pour les questions relatives aux systèmes et opérations TI autonomes, à tout moment, mais ces divisions portent la responsabilité de la performance et des coûts de ces systèmes.

Cette politique TI peut être complétée par des lignes directrices et procédures en place dans les divisions, mais ces suppléments ne peuvent pas contrevenir ni affaiblir les principes contenus dans cette politique TI. Chaque division doit fournir rapidement au département TI corporatif une copie de tout supplément local, et ces suppléments peuvent être examinés pour vérifier leur conformité à cette politique. Des audits périodiques de conformité à cette politique, ainsi que des audits ou des examens de tout supplément local à cette politique, peuvent être effectués de temps à autre par le personnel informatique de l'entreprise ou leurs représentants désignés, selon ce qui est jugé nécessaire et approprié. Des versions mises à jour de cette politique TI seront distribuées et publiées, au besoin.

Tous les membres de l'équipe McWane, contractuels, consultants, travailleurs temporaires ou autres ayant accès aux systèmes informatiques de l'entreprise (collectivement « utilisateurs ») doivent suivre cette politique informatique. Il incombe au membre de l'équipe de la compagnie qui demande l'accès de communiquer cette exigence à tout utilisateur tiers qui pourrait se voir accorder. Les questions concernant la politique informatique de McWane, son application et son fonctionnement pratique peuvent être adressées au département juridique corporatif de McWane, ou au vice-président corporatif et chef de l'information de McWane.

Bien que cette politique touche aux questions informatiques, elle ne tient pas seule; ce document est élaboré conjointement avec et considéré comme faisant partie des politiques générales du Code de conduite de la société, qui peuvent être publiées de temps à autre par McWane Corporate Legal, Human Resources ou d'autres départements. Des références à ces autres politiques peuvent être incluses tout au long de ce document, et il est conseillé aux utilisateurs de suivre les politiques générales du Code de conduite de McWane, en plus des directives spécifiques énoncées dans cette politique informatique.

Section 2 : Utilisation autorisée et restrictions d'utilisation

Cette section fournit des divulgations ainsi que des lignes directrices et procédures pour les utilisateurs relatives à l'utilisation autorisée et aux restrictions sur l'utilisation des systèmes informatiques de l'entreprise. Ces éléments sont conçus pour informer et protéger tous les membres de l'équipe, les fournisseurs et les clients lors de l'accès aux systèmes informatiques de l'entreprise.

Préambule :

L'accès aux systèmes informatiques de l'entreprise est principalement fourni à des fins commerciales. L'utilisation personnelle occasionnelle et accessoire est permise, à condition que cette utilisation soit conforme à cette politique informatique et n'interfère pas avec l'exécution de ses fonctions par l'employé. Aucun utilisateur ne devrait jamais accomplir délibérément un acte qui affecterait négativement le fonctionnement des systèmes informatiques de l'entreprise.

2.1 Aucune attente de vie privée

Les utilisateurs ne devraient pas s'attendre à la vie privée lorsqu'ils utilisent le réseau McWane via des appareils connectés. Les utilisateurs doivent savoir que les données qu'ils créent sur le réseau de l'entreprise restent la propriété de la société; par conséquent, les utilisateurs devraient éviter, dans la mesure du possible, de stocker ou de transmettre leurs renseignements personnels confidentiels ou sensibles, sur ou entre les systèmes informatiques de l'entreprise.

2.2 Internet et courriel au travail

L'entreprise offre l'accès Internet et la capacité de courriel, afin d'augmenter la productivité, de permettre les communications électroniques et de faire des transactions commerciales. Des services Internet et courriel sont fournis au besoin pour les utilisateurs autorisés, afin d'aider à la performance et à l'accomplissement des responsabilités du poste.

Tous les utilisateurs doivent savoir qu'en devenant un utilisateur autorisé des systèmes informatiques d'entreprise, l'utilisation d'Internet et du courriel peut être surveillée. L'entreprise se réserve le droit de surveiller, d'inspecter ou de suspendre cette utilisation par les utilisateurs autorisés, avec ou sans leur connaissance ou leur présence. Les utilisateurs consentent intrinsèquement, par toute utilisation d'Internet et/ou de courriel en milieu de travail, à la surveillance de cette utilisation par la Société.

Les preuves de violations des directives d'utilisation d'Internet et de courriels de la Société, qui pourraient être découvertes lors de la surveillance par la Société, seront signalées à la direction et/ou au département des ressources humaines de la société ou de la division approprié. La société se réserve le droit de prendre les mesures appropriées en cas de toute infraction qui pourrait être constatée.

- Les divisions doivent utiliser uniquement les systèmes de courriel, les connexions Internet et les fournisseurs de services Internet approuvés par le service informatique corporatif.

- Les TI d'entreprise mettront en place des protocoles de sécurité et des contrôles techniques autour des systèmes de courriel et de l'accès Internet afin de maintenir la sécurité du réseau.

- Aucune division ne peut établir une connexion séparée à Internet sans l'approbation explicite des TI de l'entreprise; de plus, les TI d'entreprise peuvent isoler, déconnecter ou prendre d'autres mesures appropriées concernant toute ou ces connexions qui pourraient avoir été ou auraient pu être mises en place par les divisions.

- Les utilisateurs ne doivent pas mener leurs affaires de l'entreprise en utilisant des comptes courriel autres que ceux émis et autorisés par McWane Corporate IT ou ses divisions.

    - L'utilisation de comptes courriel personnels par les membres de l'équipe à des fins de transmission ou de réception d'informations liées à l'entreprise et/ou à l'entreprise est interdite.

    - Il est interdit aux utilisateurs de créer toute réexpédition de courriel·les ou autres actions automatisées en utilisant leur compte courriel émis par la société, qui enverrait autrement des informations liées à l'entreprise à n'importe quel ou quels comptes courriel contrôlés personnellement.

    - Le personnel informatique corporatif ou local, et à la seule discrétion de la société et sans préavis aux utilisateurs, peut inspecter les dossiers courriel dans les systèmes de McWane à la recherche d'indications d'utilisation de comptes courriel personnels par les utilisateurs pour mener des affaires liées à l'entreprise; dans les cas où des violations sont détectées, la Société peut prendre les mesures nécessaires pour bloquer cette activité et récupérer, supprimer ou effacer les informations commerciales liées à la Société de ces comptes personnels et/ou appareils.

- En plus des lignes directrices, procédures et restrictions applicables qui sont, ou peuvent être contenues dans d'autres sections de cette politique informatique, les directives explicites suivantes s'appliquent aux utilisateurs autorisés, lorsqu'ils utilisent des services Internet et courriel fournis par l'entreprise :

    - L'utilisation excessive des services Internet et courriel fournis par l'entreprise peut être restreinte ou bloquée, selon ce que les administrateurs informatiques jugent nécessaire et approprié.
    - Les utilisateurs ne doivent pas utiliser les services Internet ou courriel fournis par l'entreprise pour mener des activités de jeu ou de jeu.

- Les utilisateurs ne doivent pas sciemment envoyer des courriels ni accéder à du contenu Internet qui pourrait contenir des contenus illégaux ou autrement offensants de nature graphique, tels que du contenu pornographique, violent ou raciste.
- Les informations confidentielles liées à la Société doivent être transmises à des tiers, par courriel ou Internet, seulement au besoin, et dans tous les cas, doivent être protégées de manière appropriée par les utilisateurs. Tous les courriels contenant des informations sensibles, confidentielles ou propriétaires doivent être marqués comme suffisamment sécurisés, d'une manière qui répond aux préoccupations de confidentialité associées à toute transmission de ces informations. L'entreprise peut fournir des outils de messagerie électronique sécurisés, et tout utilisateur devrait contacter un administrateur informatique pour obtenir de l'aide afin de protéger des informations confidentielles, avant d'envoyer ces informations par courriel ou par Internet.
- Lorsqu'ils correspondent avec les avocats de la Société sur toute question juridique, les utilisateurs doivent toujours marquer les messages adressés aux avocats comme « Confidentiel — Secret professionnel avocat-client. »
- Les utilisateurs ne devraient jamais essayer délibérément de contourner ou de désactiver Internet ou les logiciels de filtrage et de suivi des courriels utilisés par l'entreprise.

2.3 Télécommunications et appareils mobiles sans fil au travail

Tous les téléphones et équipements téléphoniques installés pour les installations de McWane, y compris les boîtes vocales, appartiennent à la Société. Le personnel TI corporatif et des TI de la division est responsable de l'installation et de l'entretien de tous les téléphones et équipements annexes, y compris l'attribution des comptes de numéro de téléphone et de messagerie vocale. Il est recommandé aux utilisateurs de protéger ce type d'équipement contre les dommages dans la mesure du possible et de mettre en place un accès sécurisé approprié à leur boîte vocale.

Dans certains cas, McWane peut distribuer des appareils mobiles sans fil appartenant à l'entreprise aux membres de l'équipe. En tout cas, les appareils mobiles sans fil utilisés pour se connecter et accéder aux données, informations et applications situés dans les systèmes informatiques de l'entreprise doivent être authentifiés et enregistrés comme appareils approuvés sur la plateforme de gestion des appareils de l'entreprise.

En général, l'utilisation personnelle du téléphone, des appareils mobiles sans fil et des services de messagerie vocale appartenant à l'entreprise est permise, mais ne doit pas nuire à la performance des affaires officielles ou du travail individuel. Il est conseillé aux utilisateurs que, pour protéger les données McWane, prévenir les abus et respecter les obligations légales existantes, la Société se réserve le droit de surveiller ses systèmes de messagerie et les données créées sur, reçues ou transmises par tout téléphone ou appareil mobile sans fil utilisé pour se connecter à l'infrastructure informatique de la Société. La société peut également modifier, ou effacer à distance ou réinitialiser selon les paramètres d'usine, tout appareil mobile authentifié ou enregistré par le système. La Compagnie fournira un avis préalable, lorsque possible, si un appareil connecté doit être effacé. Cependant, il est de la

responsabilité de l'utilisateur de sauvegarder régulièrement le contenu de ce type d'appareil, afin de ne pas perdre d'informations si un appareil est effacé.

- En plus des lignes directrices, procédures et restrictions applicables qui sont, ou peuvent être contenues dans d'autres sections de cette politique informatique, les directives explicites suivantes s'appliquent aux télécommunications et aux appareils mobiles sans fil :

    - Les utilisateurs doivent coordonner avec le personnel informatique afin d'établir un service téléphonique et/ou mobile sans fil approprié, conformément aux stratégies d'achat de la Société – y compris, mais sans s'y limiter, l'obtention de tout service d'itinérance ou de communication internationale ou de fonctionnalités similaires, qui peuvent être nécessaires pour que le téléphone ou l'appareil mobile sans fil de l'utilisateur fonctionne adéquatement aux fins commerciales de McWane.
    - Les membres de l'équipe doivent immédiatement signaler tout appareil mobile de télécommunications ou sans fil utilisé pour mener des affaires McWane qui est perdu, volé, accédé par des personnes non autorisées ou autrement compromis. Ainsi, la société peut évaluer le risque et, si nécessaire, effacer à distance tout le contenu McWane ou l'intégralité du contenu de l'appareil, ce qui peut inclure le contenu personnel de l'utilisateur.
    - Lorsqu'on le demande, les utilisateurs doivent fournir rapidement à l'entreprise l'accès à tout téléphone ou appareil mobile sans fil, y compris en cas d'incident ou d'enquête sur la sécurité.
    - Les utilisateurs devraient éviter, dans la mesure du possible, de connecter des appareils mobiles sans fil à des réseaux Wi-Fi non sécurisés, surtout lorsqu'ils mènent des affaires à McWane ou transmettent des informations de l'entreprise.
    - Les utilisateurs devraient conserver les paramètres des appareils mobiles sans fil (sécurité, restrictions de contenu, mots de passe ou phrases secrètes, etc.) qui sont conformes à cette politique informatique globale.
    - Les utilisateurs ne doivent en aucun cas chercher à obtenir un accès non autorisé aux téléphones, aux boîtes vocales ou aux appareils mobiles sans fil de leurs collègues professionnels.
    - Il est conseillé aux utilisateurs de respecter toutes les lois ou règlements fédéraux, provinciaux ou locaux applicables concernant l'utilisation des appareils mobiles sans fil, particulièrement lorsqu'ils voyagent, conduisent ou utilisent des machines ou équipements.

2.4 Les médias sociaux en milieu de travail

« Médias sociaux » désigne une variété de ressources en ligne telles que les blogs, les réseaux sociaux, les salons de discussion, les services de messagerie et/ou d'autres forums Internet. Parmi les exemples, on retrouve Facebook, LinkedIn, X, Instagram, Pinterest et/ou l'une des nombreuses autres plateformes en ligne accessibles aux utilisateurs. L'entreprise n'a pas l'intention de contrôler ce que les utilisateurs peuvent publier sur les sites de médias sociaux personnels, mais tous les membres de l'équipe sont

responsables de se conformer au Code de conduite éthique de l'entreprise ***en milieu de travail, lorsqu'ils*** sont connectés ou travaillent depuis les systèmes informatiques de la société, et/ou dans ses installations physiques, et utilisent les médias sociaux.

De plus, l'entreprise a établi une politique spécifique applicable à tous les membres de l'équipe, dans le cadre de ses politiques générales du Code de conduite publiées par le département juridique de McWane, intitulée ***« Politique sur les médias sociaux ».*** Cette politique et ses déclarations sont incorporées ici, par référence, et aucune des dispositions de cette politique informatique n'a l'intention d'être contraire.

2.5 Lignes directrices générales sur l'utilisation des systèmes informatiques de l'entreprise

Les activités suivantes sont interdites :

- Utilisation des systèmes informatiques de l'entreprise à toute fin qui violerait les lois fédérales, étatiques ou locales applicables.
- Obtenir ou tenter d'obtenir un accès non autorisé à tout type de réseau, service, information, communication ou installation ou ressource, par tous les moyens.
- Endommager ou détruire l'intégrité d'un système informatique, ou des données ou programmes stockés sur un système informatique.
- Télécharger ou installer des logiciels non autorisés ou obtenus illégalement.
- Interférer avec les responsabilités d'un autre utilisateur; et/ou,
- Utilisation des systèmes informatiques de l'entreprise pour mener des activités commerciales, personnelles ou politiques non autorisées.

Les utilisateurs ne doivent pas prendre de mesures qui portent un impact négatif sur la Société, son personnel ou ses opérations, ni exposant la Société à une responsabilité juridique potentielle ou à des dommages à la réputation.

Les utilisateurs doivent savoir que le transfert électronique de certains types de documents est illégal et passible d'une amende ou d'une peine de prison aux États-Unis et ailleurs. La Compagnie remettra immédiatement toute preuve de conduite illégale sur ses systèmes aux autorités compétentes.

Les utilisateurs qui prennent connaissance qu'un autre utilisateur enfreint cette politique doivent en informer leur superviseur ou le département des ressources humaines de la direction ou de la division concerné.

La présente politique n'a pas pour but de restreindre les communications ou les actions protégées ou requises par la loi provinciale ou fédérale.

2.6 Appareils utilisateurs finaux

Les utilisateurs ne peuvent accéder aux systèmes informatiques d'entreprise qu'à l'aide d'appareils approuvés par les utilisateurs finaux qui répondent aux normes minimales de sécurité de l'information de l'entreprise. Les appareils à usage final appartenant à McWane devraient être configurés pour recevoir automatiquement des mises à jour rapides et des correctifs, lorsque possible. Les utilisateurs peuvent se voir refuser l'accès à distance s'ils essaient d'utiliser des appareils non appartenant à l'entreprise pour se connecter aux systèmes informatiques d'entreprise.

Toute l'utilisation des dispositifs de stockage connecté par port USB (clés USB, disques durs portables, disques connectés, etc.) sera contrôlée ou limitée par un logiciel de sécurité, tel que configuré sur tous les serveurs et stations de travail de l'entreprise, par le personnel informatique de l'entreprise. Dans tous les cas, seuls les appareils connectés par port USB approuvés seront acceptables pour l'utilisation.

- Toute utilisation d'appareils connectés par port USB doit être surveillée et peut être bloquée, selon le nécessaire, afin d'empêcher le transfert ou le partage de données inapproprié ou non approuvé par les utilisateurs, par l'utilisation de tels appareils; et,
- Tout dispositif de stockage connecté à un port USB qui a été connecté ou utilisé par un membre de l'équipe sera soumis à une inspection et/ou une confiscation, à tout moment et selon la jugée nécessaire, par un administrateur informatique.

Tous les périphériques USB identifiés comme contenant des informations de la Société doivent être récupérés par, ou retournés à, un administrateur ou superviseur informatique local, à la fin de l'affiliation ou de l'emploi de tout utilisateur avec la Société; le non-identification et/ou le retour de ces dispositifs à la Société peut amener la Société à chercher un recours approprié, légal ou autre, selon les besoins, pour protéger sa propriété et/ou ses informations propriétaires contre toute mauvaise utilisation.

2.7 Accès aux identifiants

Chaque utilisateur se voit attribuer un identifiant utilisateur unique et doit configurer un mot de passe ou une phrase secrète, selon les besoins, pour accéder aux systèmes informatiques d'entreprise (« utilisateur(s) autorisé(s) »). Les mots de passe et les phrases secrètes sont considérés comme confidentiels et ne doivent pas être partagés. Les utilisateurs doivent immédiatement informer le service informatique corporatif s'ils savent ou soupçonnent qu'une combinaison nom d'utilisateur/mot de passe a été mal partagée, compromise ou utilisée; et/ou si la sécurité de l'information associée à un identifiant utilisateur a été violée d'une quelconque façon.

2.8 Sécurité associée aux appareils utilisateurs finaux et aux identifiants d'accès

Dans la mesure où cela n'est pas spécifiquement spécifié dans cette politique informatique, les administrateurs informatiques de l'entreprise (corporatif, local et service d'assistance) doivent adopter des mesures de sécurité appropriées lors de la mise à jour de nouveaux points de terminaison ou

identifiants d'accès existants sur le réseau de l'entreprise, y compris, mais sans s'y limiter, les éléments suivants :

- Assurez-vous que chaque point de terminaison déployé pour une utilisation dans l'environnement réseau de l'entreprise est protégé par des logiciels de sécurité autorisés par l'entreprise, correctement fonctionnels et configurés (actuellement Microsoft Defender, CrowdStrike et/ou Airlock).
- Assurez-vous que chaque point de terminaison est correctement inscrit dans le système de gestion des appareils de l'entreprise approprié, car cela peut être spécifié par l'informatique de l'entreprise de temps à autre.
- Assurez-vous, dans la mesure du possible, que chaque ID utilisateur (membre de l'équipe, consultant, entrepreneur, fournisseur ou autre) soit ajouté et conservé dans le groupe de sécurité approprié pour la phrase de passe fine ou la politique de mot de passe, tel qu'existant et applicable à chaque division.
- S'assurer que chaque identifiant utilisateur est configuré et maintenu selon le principe du moindre privilège; et,
- Assurez-vous, dans la mesure du possible, que chaque ID utilisateur est correctement inscrit et a appliqué toute politique d'authentification multifacteur (ou « MFA ») applicable, telle que spécifiée par l'informatique corporative de temps à autre.

Les utilisateurs doivent s'abstenir de télécharger, ouvrir, exécuter ou exécuter des applications et programmes non sollicités ou non autorisés sur les réseaux, systèmes ou points d'extrémité informatiques de l'entreprise.

- Le bureau à distance, l'accès à distance ou les logiciels de support à distance (aussi appelés « RAT ») offrent un moyen aux utilisateurs d'ordinateurs et au personnel de soutien administratif de partager des écrans, et/ou d'accéder aux réseaux informatiques ou aux points de terminaison de l'entreprise depuis des emplacements distants, et vice versa. Ces outils peuvent aussi fournir une porte dérobée vers le réseau et les systèmes de McWane et/ou de divisions, qui pourraient être utilisés pour le vol d'accès non autorisé et/ou la destruction d'actifs. Par conséquent, seuls les logiciels de bureau à distance approuvés par l'entreprise, ou les logiciels de support à distance, qui sont surveillés, correctement configurés et contrôlés par les administrateurs TI, peuvent être utilisés pour accéder au réseau McWane et/ou Division ainsi qu'aux systèmes ou points de terminaison associés.

Les utilisateurs doivent faire preuve de prudence lorsqu'ils ouvrent des pièces jointes de courriels contenues dans des communications provenant d'expéditeurs inconnus, car ces pièces jointes peuvent contenir des logiciels malveillants, du code malveillant ou d'autres menaces à la sécurité de l'information pouvant compromettre l'utilisateur. Les utilisateurs ne doivent pas répondre aux courriels ou autres messages constituant des demandes d'informations confidentielles, ne demandant pas de modifications aux informations personnelles d'identification des employés ou aux informations bancaires/de dépôt direct, ou qui demandent des transferts de fonds de l'entreprise ou de membres de

l'équipe, à moins d'avoir vérifié séparément l'identité de l'expéditeur et d'être certain de la validité de l'origine et de l'objet du message.

De plus, les utilisateurs devraient prendre l'initiative de connaître et de suivre strictement les procédures établies par les services de comptabilité, finance, ressources humaines ou autres départements d'entreprise ou de division, lorsqu'ils manipulent toute information pouvant être considérée comme des renseignements personnels identifiables (ou « PII ») d'un membre de l'équipe, d'un client, d'un fournisseur ou d'un autre partenaire commercial.

2.9 Politique d'intelligence artificielle générative (« GenAI »)

Dans la mesure où un outil particulier d'intelligence artificielle générative (« GenAI » ou « IA ») a été approuvé, tous les membres de l'équipe McWane doivent utiliser ces outils de manière éthique et responsable, conformément aux pratiques de sécurité de l'information déclarées par l'entreprise. Les membres de l'équipe devraient prioriser l'évaluation des risques de sécurité liés à l'utilisation des outils GenAI et pratiquer une protection stricte de toute information confidentielle de l'entreprise ou personnelle lorsque ces outils approuvés sont utilisés.

2.9.1 Principes généraux pour l'approbation et l'utilisation des outils GenAI

a. **Utilisez UNIQUEMENT des outils GenAI approuvés :** Les membres de l'équipe McWane sont autorisés à utiliser les outils GenAI pour les affaires de l'entreprise qui ont été vérifiés et approuvés par le Comité de gouvernance de l'IA de McWane (« AIGC »). Microsoft CoPilot est l'outil GenAI par défaut approuvé pour une utilisation dans l'environnement McWane et devrait être le seul outil GenAI utilisé par les membres de l'équipe, sauf si d'autres outils sont spécifiquement approuvés selon le processus décrit ici. Une liste de tout autre outil GenAI approuvé pour l'utilisation par les membres de l'équipe sur les points de terminaison McWane ou sur le réseau sera conservée, publiée et mise à jour par les administrateurs SharePoint d'entreprise à un emplacement approprié sur l'intranet de l'entreprise.

b. **Utilisez UNIQUEMENT les outils GenAI abonnés via des comptes contrôlés par l'entreprise :** Les abonnements aux outils GenAI destinés au travail via des comptes contrôlés personnellement sont strictement interdits. Ainsi, le travail assisté par l'IA devrait être effectué par les membres de l'équipe via des abonnements d'IA de niveau entreprise fournis par l'entreprise, incluant au minimum des protections contractuelles de la confidentialité des données et des clauses de « non-formation », et *l'utilisation d'outils d'intelligence artificielle gratuits ou publics pour les tâches liées au travail devrait être évitée par tous les membres de l'*équipe.

c. **Soumettre des propositions d'utilisation des nouveaux outils GenAI au comité de gouvernance de l'IA de McWane :** Les membres de l'équipe peuvent soumettre des propositions d'utilisation de nouveaux outils GenAI, au fur et à mesure qu'ils deviennent

disponibles pour un usage commercial. Dans le cadre du processus de vérification, le personnel approprié sera engagé pour évaluer la sécurité de tout outil GenAI proposé pour l'utilisation. Cela inclut la révision des caractéristiques de sécurité de l'outil, des conditions d'utilisation et de la politique de confidentialité, ainsi que la vérification de la réputation du développeur de l'outil ainsi que de tout service tiers utilisé par l'outil avant qu'il puisse être soumis à l'AIGC de McWane pour approbation.

1. **Principes de gouvernance applicables à tous les outils GenAI soumis pour utilisation :** Tout outil GenAI proposé pour l'utilisation par les membres de l'équipe de McWane doit être vérifié pour être conforme aux principes suivants avant soumission pour approbation – équité (évite les biais), transparence (produit des résultats explicables), responsabilité (permet une surveillance claire et des contrôles d'accès), confidentialité (protège la confidentialité et respecte les lois sur la vie privée). la sécurité (protège les systèmes contre les abus) et la supervision humaine (soutient mais ne remplace pas la prise de décision humaine).

2. **Outils GenAI « gratuits à utiliser » :** Les outils GenAI qui ne disposent pas de capacités suffisantes de licence payante ou d'autres licences formelles *seront généralement interdits d'être considérés pour approbation par l'AIGC de McWane*. Les équipes TI d'entreprise et réseau de McWane prendront des mesures pour s'assurer que ces outils soient identifiés et bloqués pour les membres de l'équipe, les ordinateurs ou autres appareils utilisés à des fins commerciales dans l'environnement.

3. **Liste de vérification pour les propositions d'outils GenAI** : Les analyses ou autres informations suivantes doivent accompagner toute proposition d'utilisation d'un outil GenAI :
   - Nom de l'outil et fournisseur (y compris toute référence au site web)
   - Cas d'utilisation prévu et justification commerciale (description du projet ou autre)
   - Types et sensibilités des données qui seront traitées
   - Documentation sur la confidentialité, la conformité et la sécurité associée à l'outil
   - Plan d'identification et d'atténuation des risques, si applicable à l'outil
   - Conditions d'utilisation, dépendances tierces, coûts et informations sur la licence
   - Coordonnées du proposant et de son département

4. **Processus de soumission et d'examen :** Les membres de l'équipe qui souhaitent obtenir l'approbation d'un outil GenAI à utiliser dans l'environnement McWane doivent soumettre leur proposition, incluant tous les éléments de la liste de vérification pour une révision préliminaire, à l'informatique d'entreprise, par courriel ou via le portail Service Now (Centre d'assistance). Le service informatique de l'entreprise accusera

réception de ces propositions dans un délai de 3 jours ouvrables, examinera les propositions pour en assurer leur exhaustivité, demandera des clarifications au besoin, et les prochaines étapes seront communiquées au proposant afin de permettre la planification de l'examen par l'AIGC de McWane lors de sa prochaine réunion régulière (généralement tenue toutes les deux semaines). Si elle est approuvée, le(s) membre(s) de l'équipe soumettant la proposition seront informés, et l'outil sera ajouté à la liste approuvée des outils GenAI maintenus par les administrateurs de McWane Corporate SharePoint. En cas de refus, des raisons et/ou des recommandations d'alternatives seront fournies au proposant.

2.9.2 Les meilleures pratiques de sécurité doivent être appliquées par les membres de l'équipe lorsqu'ils utilisent des outils GenAI :

a. **Protégez les données confidentielles :** Les membres de l'équipe ne doivent pas téléverser ni partager des données confidentielles, propriétaires ou protégées par la réglementation sans l'approbation préalable du département juridique corporatif de McWane. Cela inclut les données relatives aux clients, aux membres de l'équipe et/ou à tout autre partenaire d'affaires. Les membres de l'équipe ne doivent jamais inclure de contenu sensible dans les requêtes utilisant des outils GenAI, tels que :
   - Informations personnelles identifiables (PII);
   - Renseignements personnels sur la santé (PHI);
   - Informations sur les prix de l'entreprise ou des clients.
   - Identifiants d'utilisateur, mots de passe ou phrases secrètes délivrés par McWane.
   - La propriété intellectuelle ou les secrets commerciaux de la Compagnie.
   - Autres membres confidentiels de l'équipe, clients ou informations tierces.
   - Informations provenant de documents marqués Confidentiel, Sensible ou Propriétaire.
   - Informations stratégiques, y compris des questions qui ne semblent pas particulièrement problématiques mais qui pourraient involontairement révéler des plans organisationnels stratégiques (Exemple : demander à l'outil GenAI de résumer les notes d'une réunion durant laquelle des mises à jour financières et des changements à venir confidentiels sont discutés).
   - Autres informations non publiques de la Société qui pourraient être utiles aux concurrents ou nuisibles à la Société si elles sont divulguées.

b. **Confirmez l'exactitude des informations reçues :** les outils GenAI n'ont pas la capacité de se rappeler ou de citer les sources spécifiques d'où proviennent leurs réponses. Au lieu de citer des phrases spécifiques, leurs réponses sont construites à partir de schémas qu'ils ont appris à partir d'une vaste gamme de sources. Cela signifie que les réponses qu'un membre de l'équipe pourrait recevoir peuvent ne pas être 100% exactes. Par conséquent, les membres de

l'équipe devraient confirmer l'exactitude de l'information en recoupant les sources fiables qu'ils utiliseraient habituellement pour accomplir les tâches assignées ou prendre des décisions, examiner le contenu pour détecter des erreurs et corriger les erreurs, et vérifier que toute réponse provenant d'un outil GenAI que le membre de l'équipe souhaite utiliser est appropriée, éthique, et non biaisée, ce n'est pas une violation de la propriété intellectuelle ou de la vie privée d'une autre personne ou entité, et c'est conforme aux politiques de l'entreprise et aux lois *applicables*.

c. **Utilisez les outils GenAI pour améliorer, et non remplacer, le travail des membres de l'équipe : Les membres de l'**équipe ne doivent pas utiliser ces outils pour remplacer les compétences, les analyses et la capacité de prise de décision uniques que chaque membre apporte à son rôle. Les outils GenAI ne remplacent pas le jugement et la créativité humains. Les membres de l'équipe doivent évaluer la qualité et la pertinence des informations fournies par l'outil GenAI et utiliser leur propre capacité et jugement pour prendre des décisions éclairées sur ce qu'ils devraient inclure dans leur travail. Ils doivent aussi informer leur superviseur s'ils utilisent des outils GenAI génératifs dans le cadre de la rédaction ou de la création de tout contenu qui sera publié pour être consommé à l'extérieur de l'entreprise.

d. **Respectez les normes légales et éthiques : Les membres de l'équipe** doivent respecter les normes légales et éthiques lors de l'utilisation des outils GenAI. Les membres de l'équipe doivent éviter de s'engager dans des activités pouvant porter atteinte à la vie privée ou aux droits de propriété intellectuelle, ou enfreindre des règlements ou des lois. Lors de la création de contenu de quelque nature que ce soit, les membres de l'équipe doivent clairement distinguer entre leur propre contribution et les réponses générées par GenAI et attribuer de manière appropriée lors du partage d'informations.

e. **Contrôle de l'accès : Les membres de l'équipe** doivent toujours utiliser un identifiant utilisateur fourni par l'entreprise pour se connecter à un outil GenAI à usage professionnel. Les membres de l'équipe ne doivent pas donner accès aux outils GenAI à l'extérieur de l'entreprise sans l'approbation préalable du département ou du gestionnaire approprié et des processus ultérieurs au besoin pour répondre aux exigences de conformité en sécurité. Cela inclut le partage des identifiants de connexion ou d'autres informations sensibles avec des tiers. Les membres de l'équipe doivent également appliquer les mêmes meilleures pratiques de sécurité utilisées pour toutes les données de l'entreprise et des clients. Cela inclut l'utilisation de mots de passe forts, la mise à jour du logiciel et le respect de la politique de conservation des dossiers de l'entreprise.

f. **En cas de doute, erreur de prudence : les membres de l'équipe** doivent toujours être délibérés et diligents dans leurs efforts pour protéger l'entreprise et les personnes que nous servons lorsqu'ils utilisent la technologie GenAI générative.

LES MEMBRES DE L'ÉQUIPE NE DOIVENT PAS :

- Utilisez les outils GenAI pour prendre ou aider à prendre des décisions d'emploi concernant les candidats ou d'autres membres de l'équipe, y compris le recrutement, l'embauche, la rétention, les promotions, les transferts, la surveillance de la performance, la discipline, la rétrogradation ou les licenciements.
- Représenter le travail généré par un outil GenAI comme étant leur propre œuvre originale; et/ou
- Intégrez tout outil GenAI avec les logiciels ou programmes internes de l'entreprise sans d'abord obtenir une autorisation écrite spécifique de leur superviseur et du département informatique corporatif.

2.10 Exigences et normes en matière de sécurité de l'information tierces parties

Ces normes et exigences en matière de sécurité de l'information s'appliquent à toutes les tierces parties engagées par McWane et/ou toute une de ses divisions et/ou filiales (collectivement, la « Société »). Les « tiers », tels que mentionnés dans la présente, incluent tout fournisseur, consultant, contractuel ou autre personne non employée qui cherche à obtenir, exiger ou obtenir accès à l'ensemble des réseaux, systèmes et équipements connexes de technologie informationnelle et opérationnelle (« TI » ou « OT ») de la Société.

Selon la politique informatique de l'entreprise, les contrats (ou accords de service) signés avec des tiers pour des services liés aux TI ou aux OT doivent spécifier toute exigence matérielle et/ou norme de sécurité de l'information à respecter lors de l'exécution de ce type de travail pour la société. Ainsi, toutes les tierces parties doivent, au minimum :

- accepter de suivre la politique de technologie de l'information de McWane, ou toute autre politique applicable de l'entreprise, telle que publiée et/ou révisée de temps à autre, et si elle peut être annexée ou intégrée à tout accord de services tiers.
- Fournir un accusé de réception écrit de la réception des politiques annexées ou intégrées à tout accord de services tiers (y compris la vérification de la livraison de celles-ci à ses employés), ainsi qu'un accord de confidentialité signé de manière appropriée.
- accepter toute vérification des antécédents requise (effectuée sur l'entité tierce ou ses employés), selon ce que la société jugera appropriée.
- Permettre rapidement l'inspection ou l'audit de tout le matériel ou logiciel informatique proposé pour être utilisé par le tiers, avant et/ou pendant l'exécution du travail pour la Société.
- s'engage à maintenir et à corriger et/ou mettre à jour régulièrement tout matériel ou logiciel informatique à utiliser par le tiers dans le cadre de la performance du travail pour la société.

- s'engage à suivre toutes les normes de sécurité de l'information pour l'accès aux réseaux et/ou aux systèmes, selon ce qui peut être spécifiquement prescrit par la Société, y compris, mais sans s'y limiter :
    - spécifications d'authentification réseau et/ou système.
    - Spécifications d'identité tierce ou d'employé.
    - Spécifications d'utilisation et de protection des accréditations d'utilisateur.
    - exigences en matière de protection de l'information et/ou des données et de confidentialité; et/ou,
    - Exigences de formation ou de sensibilisation à la sécurité de l'information.
- Sur demande, remplissez un questionnaire écrit de sécurité signé par un employé autorisé du tiers, et acceptez de conserver et de fournir des preuves de conformité à toutes les normes de sécurité de l'information qui pourraient être spécifiquement prescrites par la société pour le tiers.
- engagez à aviser rapidement la Société de tout incident ou violation de sécurité causé par le tiers, et qui pourrait affecter la Société.
- s'engager à collaborer avec la société pour atténuer tout impact négatif (y compris financier) résultant d'un incident ou d'une faille de sécurité causé par le tiers; et,
- Acceptez de suivre tout avis de conservation et/ou de litige documentaire qui pourrait être émis par la Société, si nécessaire.

Section 3 : Sécurité de l'information et gestion des données

3.1 Opérations de sécurité de l'information

L'informatique de l'entreprise gérera les opérations de sécurité de l'information (« InfoSec ») à travers les systèmes informatiques de l'entreprise. À ce titre, le service TI corporatif fournira des conseils sur les pratiques de sécurité de l'information, gérera la sécurité de l'information et d'autres initiatives de formation et d'éducation en cybersécurité, attribuera des rôles de sécurité des systèmes, examinera les journaux des systèmes d'opérations de l'InfoSec, examinera les mises en œuvre matérielles et/ou logicielles des systèmes avec le personnel de la division, et surveillera en continu les opérations globales de sécurité de l'information de l'organisation. Les TI de l'entreprise peuvent également effectuer d'autres analyses périodiques de la posture de sécurité des systèmes informatiques de l'entreprise, selon ce qu'il est approprié.

Les cadres supérieurs et cadres de chaque division sont responsables de s'assurer que leur division respecte les pratiques générales de sécurité de l'information de l'entreprise, telles que définies de temps à autre par les TI corporatives.

Tous les membres de l'équipe McWane sont responsables de connaître et de respecter les politiques, normes et procédures de la sécurité de l'information afin de protéger l'information contre l'accès, l'utilisation et la diffusion non autorisés, tant à l'intérieur qu'à l'extérieur de l'entreprise. Les membres de l'équipe McWane qui soupçonnent ou voient une violation des normes de sécurité de l'information de

l'entreprise, remarquent tout ce qui pourrait constituer une violation possible de la sécurité de l'information, ou prennent connaissance de parties non autorisées cherchant à accéder aux systèmes, données ou informations de l'entreprise, doivent en informer immédiatement leur superviseur et/ou le personnel informatique local ou corporatif.

En aucun cas une norme ou pratique établie en InfoSec corporative ne doit être contournée par un utilisateur ou un tiers agissant en leur nom.

3.1.1 Pratiques de sécurité de l'information des systèmes informatiques, réseaux et/ou infonuagiques

Tout le personnel informatique ou autre personnel désigné de la Société, qu'il s'agisse de sociétés ou de division, doit travailler conformément aux pratiques et directives de base suivantes, lorsque et lorsque cela est possible, en lien avec la gestion continue des opérations de sécurité de l'information liées aux points de terminaison, réseaux, connectivité Internet et informatique en nuage qui composent les systèmes informatiques corporatifs :

- Les privilèges administratifs TI, qu'ils soient mondiaux, régionaux, locaux ou autres, seront régulièrement surveillés, révisés et ajustés en conséquence, afin d'offrir aux utilisateurs un accès approprié et sécurisé aux systèmes informatiques d'entreprise; des privilèges administratifs informatiques spécifiques peuvent être ajoutés, modifiés ou révoqués pour tout utilisateur, selon le nécessaire, et à tout moment, par l'informatique de l'entreprise.
- Les services, applications et/ou protocoles réseau inutiles doivent être identifiés et retirés rapidement par le personnel informatique approprié.
- Les administrateurs TI doivent toujours exercer leurs responsabilités et maintenir une séparation adéquate des tâches, lorsque c'est pratique et réalisable.
- Les contrôles d'accès au système informatique de l'entreprise doivent être mis en œuvre et surveillés, et, lorsque possible, des règles de pare-feu appropriées ainsi que la segmentation du réseau doivent être mises en place pour assurer des couches de sécurité de l'information tout au long.
- L'utilisation des services d'informatique en nuage, obtenus pour le compte ou utilisés par la Société, doit être étroitement surveillée, sécurisée et contrôlée par le personnel informatique autorisé, dans la mesure du possible.
- Seuls les outils et/ou logiciels avancés de sécurité de l'information et de protection contre les menaces approuvés par l'entreprise doivent être installés sur les appareils connectés ou utilisés dans l'ensemble du système informatique de l'entreprise; et,
- Les outils de connectivité sans fil, distants, réseaux privés virtuels ou autres outils de connectivité (« Wi-Fi », « VPN » et/ou éléments similaires du système) doivent être surveillés et sécurisés, lorsqu'ils sont utilisés pour fournir l'accès au système informatique de l'entreprise.

3.1.2 Principes de sécurité de la technologie opérationnelle (« OT »)

La technologie opérationnelle (« OT ») désigne les logiciels et matériels qui contrôlent des dispositifs physiques, des machines, des événements et/ou d'autres processus réalisés par les divisions qui fabriquent des produits dans l'environnement de McWane. Puisque les actifs OT peuvent être directement connectés au réseau McWane et aux points d'extrémité associés ou dépendre d'eux, la protection de la technologie centrale aux opérations est un aspect important des meilleures pratiques de sécurité OT.

Ainsi, le personnel désigné de la Société, qu'il s'agisse d'une société ou d'une division, doit fonctionner selon les pratiques et directives de base suivantes, lorsque possible, en lien avec la gestion continue des actifs OT de McWane et de ses divisions :

- Les emplacements physiques et numériques de tous les appareils OT devraient être cartographiés, et les capacités de connectivité vérifiées comme légitimes et contrôlées par le personnel autorisé.
- Chaque personne, appareil, application et/ou réseau devrait être confirmé comme légitime avant d'être autorisé à se connecter à l'un des actifs OT de McWane ou de ses divisions. Des réglages logiciels de sécurité appropriés devraient être déployés pour gérer ces connexions, qu'elles soient ponctuelles ou de façon continue, et une forme acceptable d'authentification à facteurs multiples (« MFA ») devrait être utilisée en conjonction avec la mise en place de telles connexions.
- Assurez-vous que les paramètres de connexion par défaut et/ou les mots de passe intégrés dans les ressources OT, lorsqu'ils sont déployés à un emplacement de la division McWane, soient modifiés pour être uniques à cet actif, autant que possible.
- Assurez-vous que tout membre de l'équipe ou toute autre personne nécessitant l'accès à un atout OT obtient un accès sur une base de privilège minimum et que les identités, identifiants et mots de passe/phrases de passe utilisés, ainsi que l'application de l'authentification multifacteur, soient examinés régulièrement pour un ajustement rapide ou une terminaison, selon le besoin; et,
- Assurez-vous que tous les logiciels ou micrologiciels d'actifs OT sont maintenus, mis à jour et/ou corrigés pour corriger toute vulnérabilité de sécurité connue, selon les besoins et les appropriés.

3.1.3 Programme de formation et de sensibilisation à la sécurité de l'information

Les TI de l'entreprise coordonneront la prestation de la formation en sécurité de l'information ainsi que des bulletins d'information associés ainsi que d'autres documents de sensibilisation dans toute l'organisation. Tous les cadres, la direction, les membres de l'équipe, les contractuels, les fournisseurs et/ou tout autre personnel ayant reçu un accès courriel aux systèmes informatiques corporatifs recevront des formations et des documents de sensibilisation à la sécurité de l'information. La formation en sécurité de l'information sera offerte par les services informatiques d'entreprise au moins tous les trimestres, et tous les utilisateurs doivent participer et compléter toutes les tâches qui pourraient être

émises via la plateforme de formation en sécurité de l'information McWane. Tout utilisateur qui ne complète pas rapidement les exercices de formation en sécurité de l'information sera soumis à la suspension ou à la résiliation de ses droits de courriel externe ou d'accès au système.

Des divisions peuvent être engagées pour aider à développer et/ou fournir des contributions et des matériaux à utiliser au sein de l'organisation, dans le but de promouvoir et de sensibiliser à la sécurité de l'information au sein de l'entreprise. Les divisions peuvent également mener des exercices supplémentaires de sensibilisation ou de formation à la sécurité de l'information, selon que le personnel local en TI ou autres gestionnaires jugent approprié.

3.2 Gestion des renseignements confidentiels, propriétaires et personnels

La société a établi une politique spécifique applicable à tous les membres de l'équipe, dans le cadre de ses politiques générales du Code de conduite publiées par le département juridique de McWane, intitulée ***« Informations confidentielles et propriétaires ainsi que propriété intellectuelle ».*** Cette politique et ses déclarations sont incorporées ici, par référence, et aucune des dispositions de cette politique TI n'est destinée à entrer en conflit avec cette politique.

Toutes les données personnelles traitées par les membres de l'équipe seront assujetties aux exigences de la ***« Politique de protection des données personnelles »,*** établie dans le cadre du Code de conduite global de la Société et publiée par le département juridique de McWane. Cette politique et ses déclarations sont incorporées ici, par référence, et aucune des dispositions de cette politique TI n'est destinée à entrer en conflit avec cette politique.

Section 4 : Actifs TI, protection et gestion

4.1 Réseaux, centres de données centralisés et matériel

4.1.1 Réseaux

Les TI d'entreprise mettront en œuvre, géreront et soutiendront toute infrastructure réseau utilisée pour connecter les équipements TI corporatifs et les équipements TI de la division. Cela inclut les réseaux informatiques et téléphoniques, ainsi que les réseaux et technologies d'accès à distance utilisés par les membres de l'équipe McWane lorsqu'ils voyagent ou s'absentent de leur bureau de division.

L'informatique de l'entreprise fournira des conseils pour l'achat et l'acquisition d'équipements d'infrastructure connectés au réseau. Les divisions liées aux systèmes informatiques d'entreprise sont responsables de s'assurer que tout l'équipement connecté respecte les normes qui peuvent être publiées, de temps à autre, par les TI corporatives. Les divisions sont également responsables des coûts liés à l'accessibilité et aux interconnexions au système informatique corporatif.

4.1.2 Centre(s) de données centralisé(s)

Les TI d'entreprise géreront et soutiendront les centres de données TI centralisés qui assurent l'hébergement d'applications, de stockage de données, de sauvegarde de données, de reprise après sinistre ou d'autres services et équipements liés aux TI. De telles installations sont accessibles à toutes les divisions. Ces centres de données seront conservés dans un ou plusieurs emplacements physiques. Les TI d'entreprise peuvent facturer des coûts aux divisions, liés à la maintenance et à l'utilisation des installations TI centralisées.

4.1.3 Matériel

Les TI d'entreprise fournissent des normes et un catalogue publié pour tout le matériel et équipement approuvés pour être connectés aux systèmes informatiques d'entreprise. Toute exception concernant les types de matériel ou les normes doit être documentée, et les TI d'entreprise doivent être informés de ces exceptions avant l'achat, l'installation et/ou la connexion de l'équipement. Tout le matériel connecté doit être documenté conformément à la Section 4.2 de cette politique.

Les contrats avec des fournisseurs et fournisseurs de services tiers doivent préciser les exigences matérielles et les normes de sécurité à respecter, dans le cadre de toute entente ou ordre d'achat applicable.

Sauf disposition contraire dans cette politique informatique, ou si des exceptions peuvent être prévues, le matériel privé ne doit pas être connecté aux systèmes informatiques de l'entreprise. L'accès des visiteurs aux systèmes informatiques de l'entreprise peut être fourni aux visiteurs au besoin. Toutes les connexions matérielles invitées doivent être temporaires, sauf si une exception a été prévue autrement par le personnel IT corporatif ou TI de division dûment autorisé.

4.2 Protection et gestion des actifs TI

Tout équipement informatique doit être protégé contre l'accès non autorisé et les dommages physiques dans la mesure du maximum. Les équipements de prestation de services informatiques (serveurs, routeurs, commutateurs, etc.) nécessitent un niveau de protection physique plus élevé et, dans la mesure du possible, l'accès à ces équipements du système informatique de l'entreprise devrait être limité uniquement aux personnes ayant des responsabilités informatiques, aux tiers ayant besoin d'accès pour effectuer le travail au nom du personnel informatique de l'entreprise, et/ou du personnel informatique d'entreprise ou de division autorisé.

Dans la mesure du possible, les salles informatiques, les placards à données, les racks d'équipement et autres boîtiers contenant du matériel informatique doivent être protégés contre les menaces environnementales telles qu'incendie, inondation, panne de courant, température excessive, humidité ou autres menaces jugées nécessaires par le personnel TI de l'entreprise ou des divisions. Le propriétaire de l'installation comprenant ces pièces, garde-robes, racks et enceintes est responsable de

fournir cette protection et d'aviser le personnel informatique approprié des lacunes nécessitant des réparations.

Tout actif informatique (physique ou logiciel) qui est possédé ou utilisé pour mener les affaires de la société doit être inventorié et suivi par le personnel informatique approprié et autorisé, en utilisant des conventions d'identification conformes aux directives qui ont été ou peuvent être fournies par les TI corporatifs.

Lors de l'élimination de tout actif TI, toutes les applications et données, y compris tout matériel sensible, doivent être retirées avant leur élimination, et de manière à empêcher toute forme de récupération. Tout support stockant des informations confidentielles ou personnelles identifiables (PII) qui n'est pas réutilisé à l'interne doit être physiquement détruit avant sa destruction.

La divulgation d'informations propriétaires de McWane ou de garantie-propriétaire à des parties non autorisées, intentionnelle ou non, doit être signalée à l'informatique de l'entreprise, afin que des mesures puissent être prises pour examiner la divulgation et identifier si des efforts ou actions de remédiation sont nécessaires.

Tous les courriels, documents, données, journaux de système et informations associées, qu'ils soient contenus sur des appareils physiques ou associés à des services d'informatique en nuage, et qu'ils soient situés sur les systèmes informatiques de la société ou les systèmes informatiques corporatifs, seront soumis aux exigences énoncées dans la ***« politique de conservation des dossiers »,*** établie dans le cadre du Code de conduite global de la société, et publié par le département juridique de McWane. Cette politique et ses déclarations sont incorporées ici, par référence, et aucune des dispositions de cette politique informatique n'est destinée à entrer en conflit avec cette politique.

4.2.1 Gestion des correctifs

L'TI de l'entreprise coordonnera les responsabilités avec les divisions, s'assurant que les correctifs de sécurité ou autres correctifs et mises à jour recommandés soient installés pour tout le matériel, le firmware et les logiciels, au besoin. Les appareils non directement connectés au système informatique corporatif devraient être mis à jour et entretenus périodiquement par le personnel informatique de la division, soit par des contrôles automatisés, soit par des procédures manuelles.

Lorsque possible, et lorsque cela est possible, tous les correctifs de vulnérabilité matérielle, firmware ou logiciel doivent être appliqués, généralement dans les trente (30) jours suivant la sortie. Toute exception doit être documentée par les divisions, et tout matériel ou logiciel restant non corrigé ou obsolète doit être protégé par des contrôles compensatoires.

Les TI corporatifs, ainsi que le personnel TI de la Division, coordonneront tous les processus de correctifs, autant que possible et nécessaire, et travailleront à résoudre les problèmes identifiés et/ou à mettre en œuvre des mesures d'atténuation appropriées, jusqu'à ce que tout problème identifié soit complètement résolu.

Les administrateurs TI locaux ou les utilisateurs peuvent être invités à redémarrer des stations de travail ou des serveurs, selon les besoins de l'entreprise TI, afin de faciliter la réception des mises à jour et/ou des correctifs appropriés sur ces machines. Tout poste de travail ou serveur utilisé pour se connecter au réseau corporatif peut être restreint ou désactivé, temporairement ou définitivement, par le biais des contrôles de sécurité informatique corporatif, si cet équipement est jugé manquant de logiciels, de sécurité ou d'autres mises à jour et/ou correctifs appropriés, OU si un utilisateur n'a pas correctement connecté son poste de travail au réseau afin de recevoir des mises à jour en temps voulu.

4.2.2 Analyse des vulnérabilités et gestion qui en résulte

De temps à autre, les TI d'entreprise peuvent autoriser des tests de vulnérabilités internes, des numérisations ou des tests d'intrusion de systèmes externes, seuls, ou avec l'aide d'un fournisseur de services tiers. Tout outil de numérisation, de test ou de ressources de vulnérabilités ne doit être utilisé ni déployé par aucun personnel TI sans la connaissance préalable et l'approbation du personnel TI corporatif approprié.

Tout nouveau matériel, logiciel ou matériel informatique doit être scanné, évalué ou autrement confirmé, avec une documentation appropriée, afin qu'aucune vulnérabilité n'existe, avant que ces actifs ne soient mis en service dans le cadre des systèmes informatiques de l'entreprise.

Section 5 : Gestion de l'identité et des accès

Les TI corporatifs et/ou le personnel informatique autorisé de la division seront responsables de créer, sécuriser et maintenir les comptes de connexion des utilisateurs pour accéder à tous les systèmes.

Seul le personnel TI corporatif peut créer ou accorder un accès au niveau administrateur TI à tout compte de connexion utilisateur contenu dans les annuaires actifs des systèmes TI corporatifs ou des systèmes de division.

Chaque utilisateur autorisé est responsable de :

- Garder les mots de passe et/ou les mots de passe privés.
- Signaler une faille générale de sécurité à leur superviseur immédiat, au département informatique de l'entreprise et/ou à leur administrateur informatique local.
- Changer immédiatement leur mot de passe ou sa phrase secrète s'ils ont été compromis, sont soupçonnés d'avoir été compromis, divulgués à une autre personne ou peuvent être dirigés par les services informatiques d'entreprise.
- N'utilisez jamais l'identifiant de connexion ou le mot de passe ou la phrase de passe d'une autre personne.
- Éviter, lorsque possible, d'écrire des mots de passe et des phrases secrètes, et/ou de les stocker ou de les publier à la vue de tous; et,

- S'assurer qu'ils sont déconnectés de tous les systèmes, ou que leur poste de travail et/ou d'autres appareils utilisés pour l'accès au système sont verrouillés chaque fois que ces appareils sont laissés sans surveillance.

Les lignes directrices et/ou procédures suivantes s'appliqueront à tous les comptes utilisateurs autorisés par l'entreprise :

- Des identifiants de connexion uniques (dans leur ensemble, peuvent être référencés dans ce document comme « Identifiants d'utilisateur » ou « Identifiants ») sont requis pour chaque utilisateur autorisé.
- Des mots de passe et/ou des phrases secrètes sont requis pour tous les utilisateurs et doivent être configurés comme partie intégrante de toute accréditation utilisateur. Ces mots de passe ou phrases secrètes doivent être configurés, mis à jour, modifiés ou réinitialisés, selon des normes systématiquement appliquées, telles qu'elles peuvent être publiées et/ou imposées, de temps à autre, dans les systèmes informatiques de l'entreprise et/ou de l'entreprise.
- En général, tous les membres de l'équipe, sous-traitants, identifiants partagés, administrateurs, fournisseurs ou autres identifiants de compte utilisés de manière interactive pour se connecter au réseau, terminaux ou systèmes de McWane ou de ses divisions, devraient être soumis au niveau de protection par mot de passe ou phrase secrète le plus restrictif et le plus élevé prescrit par les TI corporatifs. De plus, lorsque possible, les comptes de service utilisés de manière interactive devraient également être soumis aux mêmes normes.
- Les identifiants ou comptes utilisateurs génériques ou partagés doivent être facilement identifiés comme tels, limités à ceux nécessaires, et dans tous les cas, configurés seulement après approbation par le personnel informatique autorisé.
- Pour qu'un utilisateur puisse accéder à distance aux systèmes informatiques d'entreprise, la technologie VPN et/ou l'authentification multifacteur (« MFA ») devront accéder à des équipements informatiques, serveurs ou autres environnements informatiques d'entreprise. Dans de tels cas, les utilisateurs recevront des instructions spécifiques ainsi que des identifiants VPN ou MFA appropriés, selon les besoins, pour initier des connexions locales ou distantes fonctionnelles.
- Tous les mots de passe fournis par le fournisseur et tout autre mot de passe par défaut doivent être modifiés avant que tout ordinateur, appareil ou autre système de communication soit connecté et utilisé à des fins commerciales; de même, les mots de passe ou les phrases secrètes doivent être changés lorsqu'un administrateur ou un contractuel TI ayant connaissance de ces éléments quitte ou est réaffecté.
- Les identifiants d'utilisateur ou les comptes doivent être désactivés, dès que raisonnablement possible, chaque fois qu'un utilisateur autorisé démissionne, est résilié ou quitte autrement son emploi auprès de l'entreprise ou de l'une de ses divisions.
- L'Active Directory (ou les annuaires) et les détails associés à toutes les identifiantes d'utilisateur et comptes qu'il contient, tels qu'utilisés pour accéder à tout système informatique d'entreprise ou d'entreprise, doivent être maintenus de manière complète, cohérente, ordonnée et à jour par le personnel informatique de la division.

- De temps à autre, le personnel TI d'entreprise peut effectuer des audits ou des examens de l'Active Directory (ou des annuaires), et exiger des ajustements structurels nécessaires, afin de faciliter l'identification et le rapport rapides des utilisateurs au niveau divisionnaire, des groupes d'utilisateurs et/ou d'autres détails liés à ces identifiants d'utilisateur qui y sont contenus.
- Toutes les permissions des comptes accrédités devraient être restreintes afin d'offrir le minimum de fonctionnalités de privilèges nécessaires.
- Tous les comptes accrédités devraient être examinés régulièrement pour assurer leur validité continue, et les comptes inactifs depuis plus de 90 jours devraient être désactivés et programmés pour suppression, sauf indication contraire d'un administrateur informatique.
- Toutes les identifiantes utilisateur restant dans l'active directory (ou les annuaires), et identifiées comme inutilisées pour une période supérieure à 120 jours, doivent être confirmées par les divisions pour besoins persistants ou peuvent être supprimées par le personnel informatique de l'entreprise.
- Lorsque possible, les comptes devraient avoir une date d'expiration précise établie.
- Pour tous les comptes, le champ « employeetype » dans Active Directory devrait être rempli, autant que possible, en utilisant l'une des valeurs acceptables suivantes :
    - « TeamMember » – pour les comptes créés et attribués à un employé individuel.
    - « Partagé » – pour les comptes créés uniquement au besoin, et pour supporter plusieurs utilisateurs partageant la même identité; Tous les utilisateurs partageant doivent être documentés, spécifiés et tenus à jour, pour tout compte de ce type.
    - « Service » – pour les comptes créés au besoin et utilisés pour des systèmes ou applications à authentifier sans aucune association avec une personne spécifique.
    - « Contractuel » – pour les comptes créés et attribués à une personne qui travaille pour le compte de McWane ou de ses divisions pour une période déterminée et qui a besoin d'accéder aux systèmes pour accomplir ses tâches assignées.
    - « Fournisseur » – pour les comptes créés et assignés à un fournisseur qui travaille avec McWane ou ses divisions. Ces comptes peuvent être partagés, avec la documentation appropriée, par des employés désignés de ce fournisseur; ou,
    - « Admin » – pour les comptes créés et attribués uniquement au personnel autorisé, selon les besoins nécessaires pour accomplir leurs tâches et responsabilités.

5.1 Création de comptes tiers et contrôles d'accès

Les lignes directrices suivantes s'appliquent à tous les identifiants ou comptes d'accès aux systèmes tiers autorisés par l'entreprise créés pour être utilisés :

DIRECTIVES GÉNÉRALES LIÉES AUX COMPTES TIERS

- Les tierces parties (« Partie » ou « Parties »), telles que mentionnées ici, incluent tout fournisseur, consultant ou autre non-employé qui souhaite obtenir une accréditation pour accéder aux réseaux des Entreprises et/ou à l'équipement technologique adjacent appartenant à la Société.
- Avant de faire une demande d'accès au système pour un tiers, un membre autorisé de l'équipe (commanditaire ou superviseur) autorisé par l'entreprise doit effectuer un contrôle visuel de conformité sur le tiers et l'un de ses délégués ET obtenir un accord de confidentialité signé (« NDA ») et/ou un accusé de réception et d'applicabilité signé de cette politique informatique, d'un agent autorisé de la troisième partie qui spécifie, au minimum :

    - le nom légal et l'adresse du tiers (nom de l'entreprise).
    - le nom, le titre, l'adresse courriel, le travail et les numéros de téléphone cellulaire de la personne désignée pour recevoir les avis au nom du tiers; et,
    - l'identité de toute personne ou de personnes associées à cette troisième partie pour laquelle un accès spécifique aux systèmes de la Compagnie sera accordé; et,

- Au moins 15 jours avant le début de tout travail effectué par un tiers via Systems Access, un membre autorisé de l'équipe de l'entreprise doit soumettre un billet d'assistance entièrement complété spécifiant la ou les personnes tierces pour lesquelles le ou les comptes d'accès utilisateur seront créés. Les membres autorisés de l'équipe (commanditaire ou superviseur) de l'entreprise à approuver la demande de billet du service d'assistance pour l'accès de tout tiers doivent être enregistrés et affichés dans Active Directory dans un champ approprié, comme partie intégrante des détails de compte de ce tiers.

DIRECTIVES POUR LES ADMINISTRATEURS INFORMATIQUES LIÉES AUX COMPTES TIERS

- Les identifiants d'accès aux systèmes tiers ou les comptes émis par McWane sont également soumis aux limitations suivantes :

    - ces comptes créés pour être utilisés sur les systèmes McWane ne sont pas valides au-delà de 120 jours à compter de la date de création et, par défaut, expirent et deviennent désactivés, sauf demande de prolongation du superviseur au-delà de 120 jours; Les demandes de prolongation de ces comptes par le superviseur ne doivent pas être accordées pour plus de 120 jours consécutifs.
    - ces comptes ne peuvent pas être partagés par plusieurs individus ou par des tiers.

- ces comptes doivent utiliser le VEN. PRÉNOM. NOM de famille @divisionname.com convention de nommage.
- ces comptes ne seront autorisés que jusqu'à la licence Microsoft Office 365 F3, sauf indication contraire de la part du membre superviseur de l'équipe tierce concernée.
- ces comptes seront obligés de respecter les exigences de mot de passe corporatif, de phrase secrète, d'accès à distance, VPN et/ou d'authentification multifacteur (MFA) de McWane, lors de leur création; et,
- ces comptes ne peuvent être utilisés que par des connexions distantes sécurisées, si nécessaire, en utilisant un logiciel approuvé par McWane qui a été installé et configuré sur l'ordinateur des tiers.

- Lorsqu'un tiers ayant accès aux systèmes McWane est résilié et/ou termine son travail avant le délai initialement prévu, le membre autorisé de l'équipe (commanditaire ou superviseur) doit informer le personnel informatique approprié de désactiver et/ou retirer l'identifiant ou le compte assigné à ce tiers, en temps opportun.

- Tous les ordinateurs, ordinateurs portables, tablettes ou autres appareils tiers utilisés pour accéder aux systèmes de McWane peuvent être soumis à une inspection et à une approbation par le personnel informatique de McWane ou de ses divisions, avant d'être autorisés à se connecter aux systèmes de McWane ou de ses divisions.

Section 6 : Sauvegarde des données

Toutes les applications, données et informations contenues dans les systèmes informatiques de l'entreprise doivent être sauvegardées et/ou archivées afin de garantir que les capacités fondamentales de données et/ou de reprise après sinistre sont en place. Lorsque possible, des systèmes informatiques centralisés d'entreprise devraient être utilisés par les divisions pour les sauvegardes, afin d'assurer un accès cohérent et facile en cas de besoin de récupération. Toutes les mesures de sauvegarde des données et de reprise en cas de sinistre informatique entreprises par la Société et par ses divisions doivent fournir un soutien satisfaisant aux besoins internes ou externes, y compris le respect de toute loi et réglementation fédérale, étatique ou locale applicable. Les divisions devraient également tenir des dossiers adéquats qui documentent les sauvegardes de routine réussies de toutes les données, postes de travail et serveurs maintenus localement, et à ce titre, fournir les documents nécessaires de temps à autre pour répondre à toute exigence d'audit interne ou externe ou d'autres exigences de conformité. Les TI corporatifs travailleront avec les divisions pour assurer la cohérence dans leurs pratiques de sauvegarde des données et/ou du matériel, au besoin.

Section 7 : Réponse aux incidents et préparation à la reprise après sinistre

McWane a élaboré et maintient un plan distinct **de réponse aux incidents TI (« IRP »),** qui peut être mis à jour de temps à autre, et qui est mis en place pour fournir à la direction et au personnel TI des principes,

des lignes directrices et des procédures afin d'identifier et de gérer correctement les incidents informatiques susceptibles d'affecter la sécurité et/ou la sécurité de l'information des ressources informatiques globales de McWane's et/ou de ses divisions.

En général, les objectifs pour gérer les incidents informatiques dans l'environnement McWane incluent :

- Déterminer ce qui s'est passé.
- Déterminer comment cela s'est produit.
- Évaluer tout impact et/ou dommage résultant d'un incident informatique.
- Éviter une escalade, une propagation ou un impact supplémentaire pouvant résulter d'un incident informatique.
- En train de se remettre d'un incident informatique.
- Poursuivre une remédiation prudente et permanente des menaces afin de permettre d'éviter d'autres incidents informatiques qui pourraient autrement se reproduire à partir des mêmes vulnérabilités système ou similaires.
- Déterminer l'identité des acteurs malveillants impliqués dans tout incident informatique et poursuivre tout recours juridique disponible pour la Société, si approprié et possible; et,
- Déterminer toute action (conforme à la législation fédérale, provinciale ou locale en vigueur) nécessaire pour McWane ou ses divisions, qui atténuerait et résoudrait de manière appropriée toute violation d'information ou de données, ou de violation de la vie privée, qui aurait pu résulter d'un incident informatique.

Le plan de réponse aux incidents TI de McWane fournit des directives et prend en compte les principes suivants :

- Des lignes directrices établies pour aider à prioriser, caractériser et/ou classer les incidents.
- Définitions précises des rôles et responsabilités des intervenants en incident, des procédures de gestion des incidents et des plans de communication.
- Des lignes directrices établies qui mèneront à la préservation appropriée de toute documentation pertinente liée aux incidents signalables, selon l'exigence de la loi applicable ou selon les directives du département juridique de McWane.
- Des processus établis permettant de réviser et de modifier le plan périodiquement; et,
- Des processus établis qui prévoient que l'IRP soit évalué, selon la nécessité par la direction de McWane, afin de s'assurer que McWane et/ou ses divisions sont en mesure de mener une réponse approfondie à tout incident informatique réel.

Section 8 : Articles généraux

Enjeux et rétroaction : Pour informer et améliorer les pratiques de l'entreprise en matière de gestion des technologies de l'information, les membres de l'équipe sont encouragés à fournir des commentaires sur l'efficacité, les limites ou tout aspect problématique rencontré lors de l'application des principes inclus dans cette politique.

Les technologies modernes évoluent rapidement. Ainsi, McWane se réserve le droit de modifier, modifier, compléter ou remplacer cette politique à tout moment, avec ou sans préavis, et tous les membres de l'équipe doivent rester informés de la dernière version de cette politique.

Avertissement : Rien dans cette politique n'est conçu ou destiné à interférer, restreindre ou empêcher les communications des membres de l'équipe concernant les salaires, les heures, autres modalités d'emploi ou tout autre droit protégé par les lois du travail applicables.

Conformité aux politiques et ententes connexes : Cette politique vise à ajouter, et non contredire, limiter ou remplacer toute autre politique et exigence légale applicable, qui demeurent toutes pleinement en vigueur.

Reconnaissance et conformité : LE RESPECT *DE CETTE POLITIQUE EST UNE CONDITION D'EMPLOI AUPRÈS DE L'ENTREPRISE*. Tous les membres actifs de l'équipe sont encouragés à lire et signer cette politique, soit dans le cadre de leur processus d'intégration, soit lors d'interactions régulières avec le personnel informatique de la division, de l'entreprise ou d'autres gestionnaires. Les copies des pages de signature retournées doivent être conservées par la Compagnie, soit localement, soit dans un dossier de stockage désigné situé sur le réseau McWane.

En signant ci-dessous, je reconnais avoir lu et compris les exigences énoncées dans cette politique. J'accepte d'utiliser les réseaux, systèmes et/ou équipements informatiques McWane conformément aux meilleures pratiques de sécurité décrites ci-dessus et de signaler tout incident ou préoccupation de sécurité à mon superviseur ou gestionnaire RH.

Signature d'un membre de l'équipe : _____

Date : _____