MÉRIEUX NUTRISCIENCES

POLITIQUE DE CONFORMITÉ

SÉCURITÉ DES DONNÉES

(Octobre 2020 - V.1)

1. OBJECTIFS

Cette politique vise à préciser les obligations et responsabilités des Utilisateurs pour assurer une utilisation appropriée des Ressources Informatiques ainsi que la protection des Données Professionnelles et Personnelles au sein de chacune des entités du groupe.

Cette politique s'applique à l'utilisation des Ressources Informatiques dans le cadre des activités de la Société ou pour interagir avec les réseaux internes ou les systèmes d'entreprises, que ces derniers soient détenus ou loués par la Société, l'Utilisateur ou un tiers.

Cette Politique sur la Sécurité des Données s'applique à tous les employés, administrateurs et dirigeants de la Société. Il est de la responsabilité des managers de partager ces directives et recommandations avec tous les employés de la Société.

2. DÉFINITIONS

Données Personnelles s'entend de toute information identifiant, directement ou indirectement, une personne physique.

Données Professionnelles s'entend de toute information confidentielle traitée pour le compte de la Société ou de l'un de ses partenaires ou clients.

Législation sur la Protection des Données s'entend du Règlement Européen (UE) 2016/679 relatif à la protection des Données Personnelles et toute autre législation nationale relative à la protection des Données Personnelles applicable à la présente politique.

Ressources Informatiques s'entend de l'ensemble du/des:

- Matériel informatique fourni ou permettant l'accès à: serveurs, ordinateurs, imprimantes, tablettes, smartphones, réseaux, canaux et autres équipements informatiques;
- Logiciels stockés sur l'ordinateur de l'Utilisateur ou accessibles à distance sur les serveurs de la Société (Intranet) ou sur des serveurs externes (Internet).

Utilisateur s'entend de toute personne, quel que soit son statut, utilisant les Ressources Informatiques de la Société.

3. PRINCIPE GÉNÉRAL

L'ensemble des Ressources Informatiques appartiennent à la Société et sont fournies aux Utilisateurs dans le seul but d'être utilisées à des fins commerciales légitimes et conformément aux politiques, procédures, directives et instructions de la Société.

L'utilisation personnelle des Ressources Informatiques, y compris l'accès aux réseaux (Internet ou locaux), est autorisée dans la mesure où elle reste appropriée, limitée, légale, ne perturbe pas le fonctionnement de la Société et ne nuit pas à sa réputation.

4. CONFIDENTIALITÉ ET PROTECTION

Protection des informations

Il est de la responsabilité de chaque Utilisateur de gérer, maintenir et protéger de façon appropriée la sécurité des Ressources Informatiques et des Données Professionnelles de la Société auxquelles il a accès ou qu'il contrôle conformément aux directives de la Société en matière de sécurité de l'information au niveau global disponibles sur MXNS Connect.

Les informations et procédés utilisés pour transmettre, stocker et accéder aux Ressources Informatiques ainsi qu'aux Données Professionnelles de la Société peuvent être confidentiels, commercialement sensibles ou soumis à des droits de propriété intellectuelle.

Chaque Utilisateur doit également protéger les informations appartenant à des tiers, tels que les clients, partenaires et fournisseurs, contre toute divulgation non autorisée ou tout autre dommage.

Paramètres d'accès

Les comptes, identifiants, mots de passe, licences ou tout autre dispositif informatique propre à chaque Utilisateur sont des informations personnelles.

Les mots de passe sont associés à un identifiant spécifique à chaque Utilisateur et, lorsqu'ils sont utilisés correctement, empêchent tout accès non autorisé. Les mots de passe doivent rester strictement confidentiels et ne doivent jamais être divulgués, y compris à son manager ou au Support Informatique. Les mots de passe ne doivent pas être évidents et doivent contenir des lettres, des chiffres et/ou des signes de ponctuation.

Pour garantir un bon niveau de sécurité, la Société recommande vivement à chaque Utilisateur de changer ses mots de passe tous les 120 jours.

Chaque Utilisateur doit modifier ou demander le renouvellement de ses moyens d'authentification dès lors qu'il soupçonne leur divulgation.

Chaque Utilisateur doit utiliser ses droits d'accès uniquement pour accéder aux informations ou services nécessaires à l'exécution des tâches qui lui sont confiées et pour lesquelles il est autorisé.

Chaque Utilisateur doit assurer la confidentialité de son poste informatique en verrouillant son écran pendant son absence. Chaque Utilisateur s'engage également à assurer son bon fonctionnement et notamment à redémarrer son ordinateur relié au réseau interne au minimum

une fois par semaine, pour permettre l'installation des mises à jour de sécurité de la Société. Un redémarrage régulier est également requis pour les tablettes et les téléphones.

Chaque Utilisateur doit prendre soin du matériel portable de la Société et assurer sa protection, au sein de la Société comme en dehors de celle-ci. Si, en dehors des heures de travail, l'Utilisateur laisse le matériel portable sur site, il s'engage à le stocker dans une boîte ou un meuble verrouillé. Si l'Utilisateur emporte le matériel portable avec lui, il s'engage à ne pas le laisser dans un endroit sans surveillance.

5. CONTRÔLE DES ACTIVITÉS

Contrôles automatisés

L'ensemble des actions effectuées à partir des Ressources Informatiques de la Société peuvent faire l'objet d'une surveillance. Chaque Utilisateur est considéré comme responsable des actions effectuées sous son identité informatique.

Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le Département Informatique, un contrôle manuel ainsi qu'une vérification de toute opération effectuée par un ou plusieurs Utilisateurs pourront être mis en oeuvre.

Si une Ressource Informatique présente des anomalies, l'Utilisateur doit en informer immédiatement le Département Informatique via ssp.mxns.com.

6. EMAIL

La messagerie électronique (nominative ou non) est mise à disposition des Utilisateurs à des fins Commerciales et sous la responsabilité de chaque Utilisateur.

Utilisation Personnelle de la Messagerie électronique

L'Utilisateur a le droit d'utiliser occasionnellement sa messagerie électronique à des fins personnelles. Cependant, ces messages doivent être clairement identifiés comme des messages privés et personnels (en ajoutant le mot «PERSONNEL» ou «PRIVÉ» dans la ligne d'objet ou en créant un répertoire spécifique dédié à ce contenu). Tous les messages non identifiés comme personnels sont présumés être des messages professionnels.

Les Droits de la Société

Bien que la Société s'engage à toujours protéger les données des employés, la Société conserve néanmoins le droit de consulter les e-mails d'un Utilisateur dans des circonstances spécifiques et critiques et à des fins légitimes telles que la continuité des activités, la sécurisation des Ressources Informatiques ou en cas d'enquêtes policières ou administratives.

Dans de telles situations exceptionnelles, l'accès à la messagerie électronique de l'Utilisateur ne sera donné qu'à un nombre très restreint de managers de la Société ou à des experts externes qui auront un réel besoin d'être impliqués pour la résolution de cette situation critique. Les droits de consultation de la messagerie électronique d'un Utilisateur étendus à un tiers ne

permettront jamais à la Société d'utiliser autrement l'adresse e-mail de l'Utilisateur. La Société doit, dans la mesure du possible, informer l'Utilisateur avant de donner tout droit d'accès à sa messagerie électronique à un tiers. Si de telles informations ne peuvent être communiquées au préalable pour des raisons confidentielles ou pratiques, l'Utilisateur sera informé dans les plus brefs délais. En accédant aux e-mails des Utilisateurs, la Société s'engage à ne pas consulter les messages clairement identifiés comme « personnels » tels que décrits dans la sous-rubrique précédente.

Départ d'un Utilisateur

Avant de quitter la Société, il appartient à chaque Utilisateur de supprimer tous ses messages personnels et de mettre en place un message d'absence indiquant son départ de la Société. L'accès à la messagerie électronique de l'Utilisateur sera résilié à la fin de son contrat de travail.

Après le départ de l'Utilisateur, la Société pourra accéder à ses e-mails pendant une durée limitée si cela est nécessaire dans le cadre des activités de la Société. La Société ne pourra pas utiliser l'adresse e-mail de l'Utilisateur et y accédera uniquement en mode consultation. La Société s'engage à ne pas consulter les messages clairement identifiés comme personnels.

7. PROTECTION DES RÉSEAUX ET DES ÉCHANGES

Utilisation des Réseaux

Chaque Utilisateur s'engage à ne pas télécharger ou utiliser à des fins commerciales, des logiciels ou progiciels dont les frais de licence n'auraient pas été acquittés, provenant de sites suspects, ou interdits par la Société. Les Utilisateurs s'engagent à ne pas perturber délibérément le bon fonctionnement des Ressources Informatiques et des réseaux. Si les Utilisateurs souhaitent installer un logiciel ou un progiciel ou toute application sur les Ressources informatiques disponibles, ces derniers acceptent de faire une demande au Support Informatique via ssp.mxns.com.

Il est interdit de connecter des Ressources Informatiques autres que celles de la Société sur le réseau filaire des sites de la Société. Si nécessaire, des connexions Wifi «Invité» doivent être utilisées pour des équipements personnels ou tiers. Le Support Informatique est autorisé à interrompre la connexion en cas de risque pour la Société ou d'abus.

Échanges en Réseaux

Chaque Utilisateur devra faire preuve de vigilance à l'égard des informations envoyées et reçues (désinformation, virus informatique, tentative de fraude, chaînes, phishing, ...) et des sites Internet sur lesquels il se connecte. Tout soupçon ou toute information reçu(e) concernant un problème de sécurité informatique doit être signalé au Support Informatique via ssp.mxns.com. Il est interdit d'envoyer, transmettre, télécharger, importer, créer ou afficher des e-mails, des pièces jointes ou des éléments trouvés sur Internet inappropriés et pouvant constituer une violation ou une atteinte aux valeurs politiques, procédures, directives ou instructions de la Société.

Les informations échangées électroniquement avec des tiers peuvent, en termes juridiques, former un contrat dans certaines conditions ou être utilisées comme des preuves légales. Chaque Utilisateur doit donc prêter une attention particulière au type d'informations qu'il

échange par voie électronique ainsi que par le biais du courrier traditionnel. Chaque Utilisateur est informé que l'e-mail est un document administratif accepté comme preuve en cas de litige.

Utilisation de l'Espace de Stockage

L'espace de stockage de la Société est Google Drive. La Société s'engage uniquement à récupérer les données stockées sur Google Drive.

Tout stockage de données de la Société sur des serveurs ou d'autres applications que Google Drive doit être discuté et approuvé en amont par le Département Informatique.

Les périphériques de stockage (par exemple: clé USB, disque dur externe) d'origine inconnue ne doivent pas être connectés aux ordinateurs et équipements de la Société. L'utilisation des périphériques de stockage doit être temporaire afin de limiter tout risque de perte de données. Les fichiers stockés sur ces appareils doivent être supprimés après utilisation.

Le transfert de fichiers entre les Utilisateurs de la Société se fait via des liens dynamiques vers Google Drive dont les partages doivent être gérés avec soin et non comme des pièces jointes attachées à des e-mails.

Stockage de fichiers et informations privées

Toutes les données sont considérées comme Professionnelles à l'exception des données clairement marquées par l'utilisateur comme privées (en ajoutant le mot «PERSONNEL» ou «PRIVÉ»). Le stockage privé des fichiers et des informations est toléré sur l'ordinateur et sur Google Drive tant dans la mesure où il reste limité. Il ne doit pas occuper les serveurs et autres applications.

Procédure de Contrôle en cas de Perte ou de Vol

En cas de perte, de vol de matériel ou d'utilisation frauduleuse, chaque Utilisateur doit en informer immédiatement le Département Informatique via ssp.mxns.com et faire un rapport au Data Champion/DPO via le lien Data Breach disponible sur MXNS Connect. Le Data Champion déterminera la nécessité ou non de signaler la faille de sécurité aux autorités locales compétentes.

Le Département Informatique peut supprimer à distance toutes les données de la Société présentes sur l'appareil et, à tout moment, procéder à la suppression des données de la Société en cas d'utilisation suspecte d'un appareil mobile.

8. TÉLÉPHONIE

Utilisation Personnelle du Téléphone au cours de Voyages d'Affaires

L'utilisation personnelles du téléphone portable est tolérée lors de voyages d'affaires, à condition qu'elle soit justifiée par les besoins ordinaires de la vie familiale et réalisée dans la limite du raisonnable. L'Utilisateur est informé que la Société peut avoir accès à l'historique d'activité de l'employé, tant sur les appareils fixes que mobiles, uniquement pour une raison légitime comme précisé ci-dessus. Cet historique sera utilisé à des fins statistiques, de contrôle interne et de vérification dans les limites prévues par la loi.

9. RÉGLEMENTATION LOCALE FOURNISSANT DES RÈGLES DIFFÉRENTES DE CETTE POLITIQUE

Cette Politique vise à fournir une norme minimale commune. Dans l'hypothèse où une législation locale prévoirait des standards plus élevés ou une norme additionnelle, ces normes devraient être suivies en plus de la présente Politique. Cependant, si le respect de cette

Politique entre en conflit avec une loi applicable, vous devez respecter la loi et informer le Département Juridique et Compliance de l'existence d'un tel conflit.

10. DÉCLARATION DE SANCTION

Le non-respect des exigences de la présente Politique ou des procédures qu'elle édicte entraînera des mesures disciplinaires pouvant aller jusqu'au licenciement.

11. SOULEVER DES QUESTIONS OU SIGNALER DES RISQUES IDENTIFIÉS

Cette Politique ne traite pas de toutes les situations que vous pourriez rencontrer professionnellement. Si vous êtes confrontés à une situation pouvant présenter un risque et que vous ne savez pas comment y faire face, vous devez demander conseil. Une assistance est à votre disposition auprès de votre manager et / ou de votre département juridique.

Vous pouvez contacter le Département juridique & Compliance par e-mail compliance@mxns.com. Vos questions ou préoccupations resteront confidentielles dans toute la mesure du possible et feront l'objet d'un suivi rapide et approprié.

* *

*