



CODE DE CONDUITE



MÉRIEUX NUTRISCIENCES

POLITIQUE DE CONFORMITÉ

CONFIDENTIALITÉ

(Octobre 2020 - V.1)

1. OBJECTIFS

La confidentialité des informations est essentielle pour notre entreprise, nos clients et partenaires. La divulgation non autorisée d'informations confidentielles peut être très préjudiciable à la Société, à ses employés, ses clients et plus généralement, à l'ensemble de ses partenaires.

Des raisons commerciales légitimes peuvent cependant justifier le partage d'informations confidentielles avec un tiers.

L'objectif de cette Politique est de fournir un cadre pour assurer la confidentialité des informations sensibles et protéger la Société contre le risque de divulgation non autorisée.

Cette politique de confidentialité 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. INFORMATIONS CONFIDENTIELLES

Les informations confidentielles sont des informations exclusives non publiques, qui peuvent prendre une forme visuelle, orale, papier ou électronique. Il peut s'agir de secrets commerciaux, de savoir-faire, de documents et / ou de données liés soit à la Société, soit à un tiers en relation d'affaires avec la Société (clients, fournisseurs, partenaires commerciaux et cibles potentielles pour une acquisition).

Les informations confidentielles comprennent notamment :

- les listes de clients, prix, appels d'offre, contrats et autres données confidentielles concernant nos clients ;
- les mémorandums, résumés, notes, enregistrements, rapports, analyses et autres données techniques confidentielles ;
- les croquis, spécifications de produits, plans (y compris les plans stratégiques et les plans marketing), dessins, codes logiciels et autres données confidentielles liées à la recherche et au développement ;

- le savoir-faire, les méthodes, modes opératoires normalisés, documents de traçabilité des tests, résultats d'essais ainsi que résultats de projets de recherche et développement scientifiques ;
- les procédures opérationnelles et qualité ;
- les plans des laboratoires et configurations des espace de travail et des équipements ;
- les procédures informatiques et technologiques, les protocoles de sécurité, les identifiants et mots de passe ;
- les données confidentielles des employés (y compris celles relatives à la paie) ainsi que les dossiers du personnel ;
- les données personnelles de tous nos contacts externes y compris celles des volontaires participant à des études cliniques ou sensorielles ;
- le nom des fournisseurs, les grilles tarifaires, les pratiques commerciales ainsi que les réseaux de distribution ;
- les rapports d'audit, les données financières, les pratiques comptables, financières et technologiques de nos partenaires ou cibles d'acquisition ;
- toute information concernant le contenu des accords avec les prêteurs et les assureurs de la Société ;
- les informations confidentielles concernant les sociétés du groupe Institut Mérieux, notamment celles cotées en bourse ;
- toute information concernant les actionnaires de la Société ; et
- toute autre information qui n'est pas de notoriété publique ainsi que toute information liée en tout ou en partie à des informations confidentielles.

Si vous souhaitez en savoir plus sur les règles de confidentialité applicables aux données personnelles, veuillez vous référer à la Politique de confidentialité de la Société ([disponible sur MXNS Connect / Legal Affairs&compliance / Personal data protection](#)).

3. RÈGLES GÉNÉRALES

Contrairement aux marques, brevets ou noms de domaine légalement protégés par un enregistrement officiel, les informations et savoir-faire confidentiels ne peuvent pas être enregistrés. Ces droits ne sont protégés que dans la mesure où ils restent confidentiels.

Les principes généraux suivants doivent ainsi être respectés :

- **Lorsque vous avez un doute, supposez que les informations sont confidentielles!**

Consultez le Département juridique & compliance lorsque vous avez un doute et ce, avant d'utiliser des informations sensibles (compliance@mxns.com).

- **Protégez les informations confidentielles et les logos de nos clients et fournisseurs**

Les informations fournies par nos clients et fournisseurs dans le cadre d'une relation commerciale spécifique ne peuvent être utilisées à d'autres fins, sauf si vous obtenez au préalable leur consentement écrit.

La même règle s'applique avant toute utilisation des marques et logos de nos clients et fournisseurs dans toute communication marketing.

- **Soyez prudent au cours de vos conversations informelles!**

De nombreuses Informations confidentielles sont partagées lors de réunions internes qui se tiennent dans les locaux de la Société (salles de réunion, bureaux des salariés) ou dans des espaces partagés ou publics (open space, restaurant, train, avion, rue, etc.). Il est déconseillé de discuter d'informations confidentielles dans des espaces partagés ou publics.

Ne partagez les informations confidentielles reçues qu'avec vos collègues impliqués sur le projet et ayant donc un intérêt direct à connaître ces informations.

Soyez également prudent lorsque vous discutez avec vos amis et membres de votre famille de sujets liés à votre activité professionnelle.

- **Soyez prudent avec les documents que vous entreposez, imprimez ou envoyez!**

Lorsque vous quittez une salle de réunion (privée ou publique), aucun dossier contenant des informations confidentielles ne doit être oublié (veillez notamment à effacer les mentions écrites sur les tableaux ainsi qu'aux documents jetés dans la poubelle de la salle). Ne laissez aucune information confidentielle visible sans surveillance sur votre bureau, imprimante ou poste de travail et verrouillez votre ordinateur lorsque vous n'êtes pas à votre bureau. Soyez prudents avec les documents que vous apportez en salles de conférence ou que vous imprimez sur les imprimantes partagées.

Comme indiqué dans la Politique de sécurité des données, le transfert d'informations confidentielles par des moyens numériques doit être effectué uniquement via les outils de la Société tels que le Drive.

L'utilisation de plates-formes accessibles au public telles que Dropbox, Wetransfer ou équivalent est strictement interdite. Les sauvegardes des fichiers de la Société doivent être réalisées uniquement via Google Drive. Les sauvegardes sur un cloud personnel, des disques durs externes, des clés USB ou équivalents ne sont pas autorisées.

- **Soyez prudent avec vos ordinateurs et téléphones !**

Des écrans de sécurité doivent être utilisés dans l'espace public. Votre équipe locale Support informatique peut vous en fournir un. Renouvelez votre mot de passe régulièrement. Consultez la politique de sécurité des données pour plus d'informations sur l'utilisation des appareils informatiques.

L'enregistrement des réunions par vidéo ou microphone n'est pas autorisé sauf accord préalable de tous les participants.

- **Soyez prudent avec les vidéos et photos prises au cours des visites de laboratoire !**

Nous devons rester attentifs à ce qui est partagé publiquement ou qui peut être perçu par nos clients et fournisseurs lors des visites de laboratoire. Par principe, les photos ou vidéos sont interdites lors des visites de laboratoire. En outre, les visites des salles du laboratoire où des méthodes très spécifiques sont utilisées doivent toujours être d'abord autorisées par le directeur général du pays et précédées de la signature d'un accord de confidentialité. De plus, tout visiteur externe doit être inscrit sur le registre des visiteurs avant toute visite.

- **Vos obligations de confidentialité survivent après la fin de votre contrat de travail !**

Les employés sont soumis à une obligation de confidentialité portant sur toutes les informations confidentielles auxquelles ils auront eu accès au cours de leur activité professionnelle et cette obligation survit à la cessation de leur contrat de travail, qu'importe la cause.

4. RECOMMANDATIONS CONCERNANT LA DIVULGATION D'INFORMATIONS CONFIDENTIELLES

La divulgation d'informations confidentielles à des parties tierces peut être nécessaire en soutien de propositions commerciales, de présentations clients ou fournisseurs, d'appels d'offres ou dans le cadre plus général d'échanges commerciaux.

Il est rappelé qu'il est strictement interdit de partager des informations confidentielles avec tout concurrent de la Société.

- **Limitez la divulgation à ceux qui ont vraiment besoin d'en avoir connaissance**

L'accès, la possession ou toute autre utilisation d'informations confidentielles doivent être limités aux seules personnes qui ont un besoin réel d'en avoir connaissance pour accomplir leur travail.

- **Vérifiez les accords existants signés avec votre partenaire**

Avant toute divulgation d'informations confidentielles à un partenaire, vérifiez si la Société a déjà conclu un accord de confidentialité avec lui.

- **Signez un accord de confidentialité**

Lorsqu'il est nécessaire de divulguer des informations confidentielles, assurez-vous qu'un accord de confidentialité a bien été signé par les deux parties avant de partager des informations.

L'accord de confidentialité ne dispense cependant pas les employés de leur responsabilité quant à la pertinence des informations confidentielles qu'ils entendent divulguer.

Un modèle d'accord de confidentialité est disponible sur [MXNS Connect/ Affaires juridiques et conformité](#) ainsi qu'un guide d'accompagnement sur l'utilisation de ce modèle. N'hésitez pas à utiliser ces supports par vous-mêmes. Si vous avez des questions sur la manière de le remplir, vous pouvez contacter le Département juridique.

- **Contactez le service Communication avant tout échange avec les médias**

Aucun échange verbal ou écrit avec la presse ne doit être réalisé sans l'autorisation expresse et préalable du service Communication.

La divulgation d'informations aux médias, en particulier au cours d'une situation de crise potentielle ou déjà existante, doit être gérée avec le plus grand soin. Veuillez consulter la politique de gestion de crise pour plus d'informations sur les directives de la Société dans de telles hypothèses.

- **Contactez le Département juridique & Compliance dans l'hypothèse d'une divulgation requise par les autorités publiques**

La Société peut être sollicitée ou contrainte de divulguer certaines informations confidentielles par les autorités publiques et le non-respect de la Société pourrait être puni par la loi. Une telle obligation peut se produire dans le cadre d'une assignation à comparaître, d'enquêtes policières, d'audits ou de contrôles effectués par des organismes d'accréditation ou d'autres agences gouvernementales.

Lorsque la Société reçoit une demande d'informations, une analyse précise doit être réalisée pour s'assurer de ne pas effectuer une divulgation excessive ou insuffisante. De nombreuses demandes de documents émanant d'agences gouvernementales ou d'autorités publiques peuvent sembler contraignantes alors que la Société est en réalité en droit de refuser de divulguer les informations demandées. Il est important ainsi que vous soyez accompagnés par le Département juridique & Compliance (compliance@mxns.com) pour répondre à ces demandes.

Même contrainte par la loi, la Société conserve un devoir de confidentialité envers ses employés, clients, etc. Elle peut avoir une obligation contractuelle d'informer son client dans l'hypothèse d'une divulgation imposée. Elle se doit aussi de veiller à la préservation du caractère confidentiel des documents qu'elle aura divulgués aux agences gouvernementales et autorités publiques.

- **Contactez le Département juridique & Compliance en cas de divulgation non autorisée d'obligations confidentielles**

Une violation d'informations confidentielles ne doit jamais être sous-estimée. La divulgation non autorisée d'informations confidentielles peut en effet entraîner des risques juridiques et porter atteinte à la réputation de la Société.

Ainsi, sans crainte de représailles, les employés sont encouragés à signaler toute violation d'informations confidentielles :

- au service informatique, dans l'hypothèse où la violation serait liée à la perte de données électroniques ou de matériel informatique ;
- au délégué à la protection des données (dpo@mxns.com) en cas de violation de données personnelles
- au Département Juridique & Compliance dans tous les cas.

5. 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.

6. 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.

7. 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.

* *
*