**GROUPE NUTRI**

# POLITIQUE RELATIVE À LA CYBERSÉCURITÉ

**JANVIER 2024**

# TABLE DES MATIÈRES



*L'emploi du genre masculin comprend et inclut le féminin, et le singulier comprend le pluriel et vice-versa, cette présentation ayant pour objet de faciliter la lecture du texte.*

## I. INTRODUCTION

Le risque de vol de données, de fraudes et de failles de sécurité peut avoir un impact négatif sur les systèmes, l'infrastructure technologique et la réputation d'une entreprise. Par conséquent, Groupe Nutri Inc. et ses unités d'affaires, ci-après nommées **Groupe Nutri**, adoptent cette politique pour aider à décrire les mesures de sécurité mises en place pour faire en sorte que les informations restent sécurisées et protégées.

## II. OBJECTIFS

L'objectif de cette politique est de :

- Protéger les données confidentielles et l'infrastructure technologique de Groupe Nutri;
- Décrire les protocoles et les directives qui régissent les mesures de cybersécurité;
- Définir les règles d'utilisation professionnelle et personnelle des outils informatiques, et;
- Rappeler le processus disciplinaire pour les violations de la politique.

## III. CHAMP D'APPLICATION

Cette politique s'applique à tous les membres du conseil d'administration, employés permanents et à temps partiel, sous-traitants, bénévoles, fournisseurs, stagiaires ainsi qu'à toute personne ayant accès aux systèmes électroniques, informations, logiciels ou outils informatiques de Groupe Nutri.

## IV. DÉFINITIONS

Pour les fins de la présente politique, les expressions suivantes signifient :

– « *données confidentielles* »

- Les renseignements personnels;
- Les Informations financières non publiées;
- Les informations sur les clients, les fournisseurs et les actionnaires;
- Les clients potentiels et les données relatives aux ventes;
- Les brevets, processus commerciaux et nouvelles technologies;
- Les mots de passe, affectations et informations personnelles des employés;
- Les contrats d'entreprise et documents juridiques.

– « *incident de confidentialité* »

- L’accès non autorisé à des données confidentielles ;
- L’utilisation non autorisée de données confidentielles;
- La communication non autorisée de données confidentielles;
- La perte de données confidentielles ou toute autre atteinte à la protection d’un tel renseignement.

## V. SÉCURITÉ DE L’ÉQUIPEMENT

Pour assurer la sécurité de tous les appareils et informations fournis par l’entreprise, les employés de Groupe Nutri sont tenus de :

- Garder tous les appareils fournis par l’entreprise, y compris les tablettes, les ordinateurs et les appareils mobiles, protégés par un mot de passe (minimum de 8 caractères);
- Sécuriser tous les appareils fournis avant de quitter leur bureau;
- Obtenir l’autorisation de la direction ou de leur supérieur immédiat avant de retirer les appareils des locaux de l’entreprise;
- S’abstenir de partager des mots de passe privés avec des collègues, des connaissances personnelles ou quiconque;
- Effectuer régulièrement la mise à jour de sécurité des logiciels utilisés;
- Se conformer aux directives du service informatique.

## VI. SÉCURITÉ DU COURRIER ÉLECTRONIQUE

La protection des systèmes de messagerie est une priorité élevée, car les courriels peuvent entraîner des vols de données, des fraudes et introduire des logiciels malveillants. Par conséquent, Groupe Nutri exige que tous les employés :

- Vérifient la légitimité de chaque courriel avant de l’ouvrir, y compris l’adresse courriel et le nom de l’expéditeur;
- Évitent d’ouvrir des courriels et des pièces jointes suspects et de cliquer sur des liens qu’ils contiennent;
- Vérifient les courriels pour des erreurs grammaticales importantes;
- Contactent le service informatique en cas de courriels suspects.

## VII. TRANSFERT DE DONNÉES

Groupe Nutri reconnait les risques de sécurité liés au transfert de données confidentielles, que ce soit à l'interne ou à l'extérieur de l'entreprise. Pour minimiser les risques de vol de données, tous les employés doivent :

- Obtenir l'autorisation nécessaire de la direction ou de leur supérieur immédiat avant de transférer des données confidentielles;
- S'abstenir de transférer des données confidentielles aux employés et à des tiers qui n'y ont pas accès dans le cadre de leurs fonctions;
- Ne transférer des données confidentielles que sur les réseaux approuvés par Groupe Nutri;
- Vérifier le destinataire autorisé des données confidentielles et s'assurer qu'il a mis en place les mesures de sécurité appropriées;
- Alerter immédiatement le service informatique de toute activité suspecte, incluant tout incident de confidentialité.

## VIII. MESURES DISCIPLINAIRES

La violation de cette politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement. Les sanctions seront basées sur la gravité de la violation. Les violations non intentionnelles peuvent justifier un avertissement verbal, les violations fréquentes de même nature peuvent conduire à un avertissement écrit, et les violations intentionnelles peuvent entraîner une suspension ou un licenciement, selon les circonstances.

## IX. ADMINISTRATION DE LA POLITIQUE

| | |
|---|---|
| Instance responsable : | Conseil d'administration |
| Responsable de l'application de la politique : | Vice-président, Ressources humaines |
| Date de l'approbation : | Janvier 2024 |
| Date de révision : | s.o. |
| Date d'entrée en vigueur de la politique : | Janvier 2024 |
| Fréquence de la mise à jour de la politique : | Cette politique est révisée à la demande du Vice-président, ressources humaines ou au besoin |