Cybersécurité : Politique de gouvernance et confidentialité des données

1. INFORMATION SUR LA POLITIQUE

Nom de l'organisation : **Solutions Biotonix Inc.**
Date d'entrée en vigueur de la politique : **1 août 2023**
Date de révision : **4 février 2025** *(prochaine révision prévue pour août 2025)*

1.1 Portée de la politique

La politique de sécurité des données de Solutions Biotonix, s'applique à toutes les entités relevant de la responsabilité de l'entreprise. Les mesures décrites ci-dessus s'appliquent uniformément à l'ensemble de l'organisation, afin d'assurer une protection et une conformité cohérentes.

En ce qui concerne les sous-traitants de données, la société collabore avec Solulan (certifié SOC 2) en tant que partenaire de confiance, pour renforcer leurs efforts en matière de cybersécurité et garantir la sécurité de leur environnement Office 365. Leur système de sauvegarde avancé et de prévention des pertes de données (DLP) contribue significativement à améliorer les mesures de protection des données de Solutions Biotonix. L'utilisation de produits premium de Microsoft, optimisés par leur partenaire, assure un niveau de sécurité supérieur.

Biotonix s'engage à appliquer une gouvernance rigoureuse en matière de cybersécurité et de confidentialité des données. Sous la supervision du Vice-Président des Technologies, Sébastien Lacoste, l'organisation applique les meilleures pratiques en matière de protection des données et respecte les exigences de la Loi 25 du Québec.

1.2 Énoncés de la politique

1.2.1 Solutions Biotonix possède des données personnelles et sensibles.

1.2.2 L'approche de l'organisation en matière de sécurité des données, repose sur un engagement solide :

1.2.3 Respect des lois et meilleures pratiques : La société se conforme aux normes légales et a les meilleures pratiques pour assurer une conformité proactive.

1.2.4 Préservation des droits individuels : Les droits des individus sont au centre des préoccupations de Solutions Biotonix, conformément aux normes légales et éthiques.

1.2.5 Transparence et communication : L'entreprise entretient une relation transparente et honnête avec les détenteurs de données, respectant la confidentialité tout en fournissant des informations nécessaires.

1.2.6 Formation et soutien du personnel : Solutions Biotonix forme et soutient son équipe, pour garantir une gestion cohérente et avisée des données personnelles.

© Cybersécurité Biotonix 2025

1.2.7 Notification volontaire au Commissaire à l'Information : La société signale volontairement les incidents, démontrant leur engagement envers la responsabilité et la transparence.

1.2.8 En somme, ces piliers guident l'engagement de Solutions Biotonix à protéger les données de manière proactive, éthique et conforme à la réglementation.

1.3 Risques clés

- La perte des données des utilisateurs.
- Une fuite de données venant d'un environnement de travail non sécurisé.

2. RESPONSABILITÉS

2.1 La direction

La direction de Solutions Biotonix a la responsabilité générale de veiller à ce que l'organisation se conforme à ses obligations légales.

2.2 Responsable de la protection des données

Ce rôle est parfaitement assumé par le Vice-Président des Technologies, Sébastien Lacoste, ingénieur en informatique. Ce rôle central garantit la mise en œuvre des meilleures pratiques en matière de sécurité. Ses responsabilités comprennent :

- Informer le Conseil d'administration des responsabilités en matière de protection des données
- Revoir les politiques de protection des données et les politiques connexes
- Conseiller les autres membres du personnel sur les questions complexes liées à la protection des données
- Veiller à ce que l'intégration et la formation en matière de protection des données soient effectuées
- Traiter les demandes d'accès aux données des sujets
- Approuver les divulgations inhabituelles ou controversées de données personnelles
- Approuver les contrats avec les sous-traitants de données

2.3 Employé(e)s de Biotonix

Tous les membres du personnel sont tenus de lire, de comprendre et d'accepter toutes les politiques et procédures liées aux données personnelles qu'ils pourraient traiter dans le cadre de leurs activités.

© Cybersécurité Biotonix 2025

3. SÉCURITÉ

3.1 Mesures de sécurités

Pour garantir une protection renforcée, tous les employés doivent se déconnecter de leurs sessions à la fin de leur période de travail. En complément, l'authentification multifactorielle (MFA) est obligatoire pour tous les accès aux comptes Office 365, limitant ainsi les risques d'accès non autorisés. La responsabilité des sauvegardes est confiée à Solulan conformément à l'accord fait entre ceux-ci et Solutions Biotonix.

3.2 Stockage des données

Les données sensibles issues des applications Biotonix sont stockées de manière sécurisée dans Microsoft Azure, sur des serveurs au Canada, bénéficiant ainsi des protections avancées de cette plateforme. De plus, notre partenariat avec Solulan (certifié SOC 2) garantit un renforcement de la cybersécurité, notamment dans l'environnement Office 365, avec des solutions avancées de prévention des pertes de données (DLP) et de sauvegarde automatisée.

3.3 Rétention des données

En raison des lois en vigueur et de l'approche transparente de Solutions Biotonix, les utilisateurs sont les propriétaires de leurs données et peuvent les supprimer de manière permanente à tout moment via l'option disponible directement dans l'application mobile.
Solutions Biotonix applique également une politique de rétention des données afin d'assurer la conformité aux réglementations applicables et aux besoins opérationnels :

- **Données des utilisateurs actifs** : conservées tant que le compte est actif.
- **Données des utilisateurs inactifs** : supprimées après **24 mois** d'inactivité, sauf en cas d'obligation légale de conservation.
- **Données transactionnelles** (paiements, factures, historiques de connexion, etc.) : conservées pour une durée minimale de **7 ans** à des fins de conformité réglementaire et d'audit.
- **Données anonymisées** : certaines données peuvent être conservées de façon anonymisée à des fins statistiques et d'amélioration des services, sans possibilité d'identification de l'utilisateur.

Les utilisateurs peuvent demander la suppression immédiate de leurs données personnelles via l'application mobile ou, en cas de besoin, par une demande écrite auprès du Responsable de la protection des données. En cas d'incident de cybersécurité nécessitant une enquête, certaines données peuvent être conservées temporairement au-delà de ces périodes jusqu'à la clôture de l'enquête.

3.4 Droit d'accès

Les rôles et permissions sont attribués avec une approche stricte du principe de moindre privilège, garantissant que chaque employé dispose uniquement des accès nécessaires à ses tâches.

© Cybersécurité Biotonix 2025

4. PLAN DE GESTION DES INCIDENTS DE CYBERSÉCURITÉ

4.1 Définition d'un incident

Un incident peut inclure :

- Accès non autorisé aux systèmes ou aux données.
- Fuite ou perte de données sensibles.
- Infection par un malware ou ransomware.
- Attaque par hameçonnage (phishing).
- Défaillance d'un système critique exposant des données.

4.2 Processus de réponse aux incidents

4.2.1 Détection et alerte

- Surveiller et détecter les menaces via des outils de cybersécurité (ex : antivirus, SIEM, logs d'accès).
- Définir un canal d'alerte interne (courriel dédié, Teams) pour rapporter un incident.
- Prioriser l'incident selon sa gravité (mineur, modéré, critique).

4.2.2 Contention de l'incident

- Isoler immédiatement les systèmes ou comptes compromis (ex : désactiver un compte, bloquer un accès).
- Mettre en œuvre des contre-mesures (ex : activer un pare-feu temporaire).
- Informer les parties concernées (direction, responsable de la protection des données, partenaires techniques Solulan).

4.2.3 Analyse et remédiation

- Identifier l'origine de l'incident (ex : faille humaine, attaque externe, vulnérabilité logicielle).
- Vérifier les dommages subis et les données affectées.
- Appliquer des correctifs de sécurité (ex : mises à jour, changement des accès, révisions des procédures).

4.2.4 Communication et notification

- Notifier la Commission d'Accès à l'Information (CAI) si nécessaire (selon la Loi 25).
- Informer les utilisateurs concernés en cas de risque pour leurs données.
- Communiquer avec les sous-traitants et partenaires si l'incident les impacte.

4.2.5 Apprentissage et prévention

- Rédiger un rapport d'incident (ce qui s'est passé, actions prises, leçons apprises).
- Adapter les procédures et la formation du personnel pour éviter la répétition de l'incident.
- Mettre en place un plan d'amélioration continue.

© Cybersécurité Biotonix 2025