Groupe CIS

Mesures de Protection des Données

1.Introduction

Groupe CIS est un important fournisseur nord-américain de solutions logicielles d'affaires, spécialisé dans la livraison directe en magasin (Direct Store Delivery – DSD), l'automatisation de la force de vente (Sales Force Automation – SFA) et la gestion du transport de personnes et de marchandises. Fort d'un héritage remontant à 1977, ***Groupe CIS*** s'est bâti une réputation de fournisseur de solutions numériques innovantes, sécurisées et évolutives qui permettent aux organisations d'optimiser leurs opérations et d'améliorer leur productivité.
En tant que partenaire technologique de confiance pour de nombreuses industries, ***Groupe CIS*** reconnaît l'importance essentielle de protéger les données de ses clients et de maintenir les plus hauts standards en matière de sécurité de l'information.
Ce document présente les mesures complètes de protection des données mises en place au sein de l'organisation afin d'assurer la confidentialité, l'intégrité et la disponibilité des actifs informationnels. Ces contrôles s'alignent sur les meilleures pratiques de l'industrie et les exigences réglementaires, notamment ISO 27001 et la Loi 25 du Québec. Ils sont continuellement révisés et améliorés afin de répondre aux menaces en évolution et aux besoins d'affaires.

2.Contrôles Organisationnels

Pour assurer une posture de sécurité robuste et résiliente, ***Groupe CIS*** a mis en place un ensemble complet de contrôles organisationnels. Ces contrôles visent à établir une gouvernance claire, renforcer les responsabilités et aligner les pratiques de sécurité aux objectifs d'affaires et aux exigences réglementaires.
Ci-dessous se trouvent les principales catégories et mesures qui composent la structure de sécurité, la gestion des politiques et la stratégie de protection des données de ***Groupe CIS***.

Catégorie	Contrôles
Organisation de la Sécurité	***Structure de sécurité*** • Une structure de sécurité de l'information est établie avec des rôles et responsabilités clairement définis, alignés avec le principe de séparation des tâches. Des réunions régulières du Comité de pilotage de la sécurité de l'information sont tenues. • La direction exige que tous les employés et consultants reconnaissent et signent les politiques et normes de sécurité du ***Groupe CIS***.
Gestion des Politiques et Procédures	***Politiques, normes et procédures de sécurité*** • Une documentation complète en sécurité de l'information est en place et opérationnelle (politiques, normes, plans, guides, procédures d'exploitation, etc.). • Un processus de gestion documentaire (création, maintenance, révision, retrait) est en place.
Protection des Actifs et des Données	***Gestion des actifs*** • Un outil de gestion des actifs est utilisé pour maintenir un inventaire du matériel et des logiciels. • Un processus défini existe pour la restitution et la mise hors service sécurisée des équipements (incluant la désinfection des données et la destruction physique). • Les politiques d'utilisation acceptable et de classification de l'information assurent la manipulation adéquate des informations et des actifs. • Seuls les ordinateurs portables des employés sont autorisés à quitter les bureaux. • Les documents physiques ne sont plus utilisés, soutenant ainsi un environnement de travail entièrement numérique et sécurisé. ***Sécurité des données*** • Tous les postes de travail sont protégés par un chiffrement complet du disque. • Les données en transit entre l'environnement de ***Groupe CIS*** et tous les appareils et ressources autorisés (ordinateurs, appareils mobiles, serveurs, applications, etc.) sont chiffrées.

Catégorie	Contrôles
Gestion des Risques, de la Conformité et des Fournisseurs	***Gestion des risques*** • Un processus de gestion des risques en sécurité de l'information est implanté et opérationnel. • Les risques sont évalués, traités, communiqués et suivis régulièrement. ***Gestion de la conformité*** • Un Responsable de la protection des renseignements personnels (DPO) est désigné pour assurer la conformité avec la Loi 25 et autres réglementations. • L'accès aux ressources contenant des informations sensibles ou des renseignements personnels (PII) est restreint. ***Gestion des fournisseurs et tiers*** • Les risques liés aux fournisseurs et tiers sont intégrés au processus de gestion des risques de sécurité. Une diligence raisonnable est effectuée pour les services nouveaux ou modifiés. Les contrats incluent toujours des clauses et exigences spécifiques en matière de sécurité de l'information. • Une Norme de sécurité infonuagique est en place pour encadrer la sécurité des environnements cloud. ***Audits indépendants*** • Des tests d'intrusion (pentests) sont effectués régulièrement sur l'environnement et les applications du ***Groupe CIS***. • ***Groupe CIS*** est certifié ISO 27001.
Gestion du Personnel et Sensibilisation à la Sécurité	***Gestion du Personnel et Sensibilisation à la Sécurité*** • Des vérifications liées à la sécurité sont intégrées au processus RH tout au long du cycle d'emploi, incluant les mesures disciplinaires liées à la conformité. • Tous les utilisateurs doivent suivre annuellement une formation de sécurité et signer les politiques clés, telles que l'Utilisation acceptable et la Norme de sécurité en télétravail. La conformité est suivie et appliquée.
Gestion des Accès	***Gestion des Accès (Logiques et Physiques)*** • L'accès aux données dans l'environnement du ***Groupe CIS*** est accordé en fonction des rôles (RBAC) et du principe du besoin de savoir. • Une politique de mot de passe robuste est appliquée; l'authentification multifacteur et l'authentification unique sont activées lorsque possible. • Des contrôles physiques stricts sont en place au siège social. • Les procédures d'intégration, de gestion, de révision et de retrait des accès sont en place et auditées régulièrement.
Opérations de Sécurité	***Contrôles des postes de travail*** • Une solution de détection et réponse sur les endpoints (EDR) est déployée sur tous les terminaux. • Les postes de travail utilisent le chiffrement complet du disque (FDE). • Les connexions à distance doivent passer par le VPN corporatif. ***Gestion des vulnérabilités*** • Un processus de gestion des vulnérabilités est en place pour évaluer les menaces et niveaux de sévérité et appliquer les correctifs requis. ***Surveillance et SOC*** • Les événements de sécurité des utilisateurs et administrateurs sont consignés. • Un SOC surveille et analyse les événements, et alerte l'équipe de sécurité en cas d'incident potentiel.

Catégorie	Contrôles
Sécurité des Communications	***Sécurité des Communications*** • Le réseau est segmenté adéquatement et le périmètre est protégé par des technologies de dernière génération (protection avancée des courriels, passerelle web sécurisée, VPN, MFA, etc.). • Un filtrage web est en place.
Gestion des Systèmes d'Information	***Gestion des changements*** • Tous les changements dans l'environnement sont documentés, approuvés et contrôlés par un processus formel. ***Gestion de la capacité*** • La capacité est surveillée et des mesures sont prises pour assurer des ressources suffisantes. ***Développement logiciel*** • L'accès au code source est séparé selon les unités d'affaires. • Des standards de développement sécurisé sont suivis. • Les tests sont effectués dans des environnements isolés avant la mise en production. • L'accès aux données de test est restreint.
Gestion des Incidents de Sécurité	***Gestion des Incidents de Sécurité*** • ***Groupe CIS*** dispose d'un plan de réponse aux incidents documenté et opérationnel, avec des rôles et responsabilités définis ainsi qu'un processus de notification de brèche. • Le plan est testé régulièrement.
Gestion de la Continuité des TIC	***Gestion de la Continuité des TIC*** • Les environnements clients sont sauvegardés dans Azure. Les serveurs corporatifs sont sauvegardés sur site, avec réplication hors site. • Des contrôles et mécanismes de surveillance assurent la continuité en cas d'événement perturbateur. Les procédures de reprise sont identifiées et documentées.