CÔTÉ-RECO INC.
DESCHAILLONS, QC

Politiques – Sécurité informatique

Les politiques de sécurité informatique établies par Côté-Reco visent à garantir la confidentialité, l'intégrité et la disponibilité des données sensibles et des systèmes d'information. Cette politique définit les directives et les mesures nécessaires pour protéger nos actifs informationnels contre les menaces internes et externes. Elle s'applique à toute personne ayant accès aux informations de l'entreprise.

Cette politique sera régulièrement révisée et mise à jour pour prendre en compte les évolutions technologiques et les nouvelles menaces en matière de sécurité. Chaque personne qui accepte cette politique est tenue de se conformer à celle-ci ainsi qu'à se tenir au courant de ses mises à jour, et de contribuer activement à la protection des informations confidentielles de l'entreprise

Responsabilités

La responsabilité de la mise en œuvre et du respect de cette politique incombe à tous les niveaux de l'organisation.

- La direction générale doit approuver la politique et les procédures associées et s'assurer que les ressources nécessaires sont allouées pour la mise en œuvre de cette politique.
- Les responsables de la sécurité Informatique doivent mettre en œuvre et maintenir la politique.
- Chaque personne est individuellement responsable de connaître et comprendre cette politique, d'appliquer les principes dans ses activités quotidiennes et de signaler toute violation ou anomalie à l'équipe de Côté-Reco.

Ce document regroupe quatre politiques distinctes :

- La politique de sécurité de l'information
- La politique de gestion des accès
- La politique relative aux mots de passe
- La politique de gestion documentaire

---

1. Politique – Sécurité de l'information

1.1 Gestion des données

Chaque personne est tenue de protéger les informations de l'entreprise en mettant en œuvre des mesures de sécurité appropriées, notamment en ce qui concerne l'accès, la manipulation et le stockage des données sensibles.

1.2 Transmission des données par courriel

La transmission des données par courriel est une pratique courante, mais elle doit être soumise à un cadre strict pour garantir la sécurité et la confidentialité des informations échangées. Les personnes ayant accès aux données sensibles et confidentielles de Côté-Reco doivent veiller à supprimer toutes les copies ou traces de ces données sur leur système informatique pour éviter tout accès non autorisé ultérieur.

1.3 Accès

L'accès aux systèmes et aux données de l'entreprise est un privilège accordé sous réserve du respect de règles strictes visant à assurer la sécurité et la confidentialité des informations. Les utilisateurs doivent se déconnecter de manière sécurisée après avoir terminé leurs activités à distance, afin de prévenir tout accès non autorisé à leurs comptes ou aux systèmes de l'entreprise. Les appareils utilisés pour accéder aux sites de Côté-Reco doivent être verrouillés avec un mot de passe ou une méthode d'authentification biométrique pour empêcher l'accès non autorisé en cas de perte ou de vol.

1.5 Formation et sensibilisation

Un cadre rigoureux de formation et de sensibilisation est essentiel pour garantir que tous les employés comprennent et mettent en œuvre les meilleures pratiques en matière de sécurité de l'information. De cette façon, chaque personne utilisant les systèmes de Côté-Reco est tenu de transmettre l'information de cette politique à ses employés ou collaborateur à qui il aura donné l'accès et de s'assurer qu'elles soient suivies. Tous sont invités à signaler toute activité suspecte ou toute violation potentielle de la sécurité de l'information à l'équipe responsable de la sécurité de Côté-Reco.

1.6 Protection de la vie privée

Les informations collectées sont traitées de manière confidentielle. Seuls les membres autorisés de l'équipe de sécurité de l'information ont accès aux données collectées.

1.7 Durée de conservation des données

Les données collectées sont conservées uniquement pendant la durée nécessaire pour atteindre les objectifs de sécurité de l'information. Une fois cette période expirée, les données sont effacées de manière sécurisée.

1.8 Nettoyage des bureaux

Le nettoyage des bureaux, dans le but de respecter la confidentialité des informations de Côté-Reco, doit être observer de ces façons :

1. Avant de quitter votre poste de travail, assurez-vous que votre bureau est débarrassé de tout papier, documents, post-it, et autres objets renfermant des informations confidentielles de Côté-Reco.
2. Verrouillez votre ordinateur ou déconnectez-vous lorsque vous quittez votre bureau du site sécurisé.
3. Ne laissez pas d'informations sensibles affichées à l'écran.
4. Tous les documents contenant des informations sensibles doivent être rangés dans des classeurs verrouillés ou des armoires.
5. Ne laissez jamais de documents confidentiels sur votre bureau pendant la nuit et ne laissez pas de documents imprimés contenant des informations sensibles sur votre bureau.
6. Signalez tout incident de sécurité.

2. Politique – Gestion d'accès

2.1 Principes de gestion d'accès

Chaque utilisateur (et son équipe à qui il donne accès) doit être identifié de manière unique avant d'accéder aux systèmes, afin de permettre le suivi de ses activités et d'assurer la responsabilité. L'authentification doit reposer sur des méthodes sécurisées, telles que des mots de passe forts, l'authentification à deux facteurs (2FA) ou l'utilisation de certificats.

2.2 Gestion des comptes utilisateurs

La création, la modification et la suppression des comptes utilisateurs doivent être documentées et approuvées par les responsables concernés. Les comptes inactifs doivent être désactivés ou supprimés régulièrement afin de maintenir un niveau de sécurité optimal. **Si vous faites un licenciement d'employé et qu'il avait accès à la plateforme, vous vous devez d'aller changer votre mot de passe car cet employé pourra continuer à y aller sans problème.**

2.3 Partage des accès

Chaque utilisateur est personnellement responsable de la confidentialité de ses identifiants et doit s'assurer de ne jamais les communiquer à d'autres personnes et d'assurer le suivi des personnes à qui il donne le privilège de son accès en la partageant.

2.6 Révocation des privilèges

Les privilèges d'accès peuvent être révoqués en tout temps lorsque la situation l'exige, notamment en cas de fin d'emploi, d'arrêt de travail, de changement de rôle, ou de non-respect des politiques de

sécurité. La procédure de révocation doit être clairement définie, documentée et suivie rigoureusement. Elle comprend les étapes nécessaires pour désactiver les comptes, retirer les droits d'accès et informer les utilisateurs concernés. Les responsables de la sécurité informatique doivent être avisés rapidement et sont responsables de l'exécution de cette procédure.

3. Politique – Mots de passe

Une politique de mot de passe est essentielle car elle contribue à la sécurité des données et à la protection contre les cybermenaces.

3.1 Directive pour les mots de passe

- Un accès de type privilégiés est toute combinaison d'un nom d'utilisateur/mot de passe disposant de permissions supplémentaires / particulières / administratifs.
- Ils doivent être stockés dans une voute de mot de passe encryptée (utilisation d'un gestionnaire de mot de passe).
- Ils ne doivent pas être réutilisés à plus d'un endroit.
- Utiliser des mots de passe différents de ceux de votre vie personnelle.

3.3 Définition d'un mot de passe fort

Le mot de passe de passe ne doit pas contenir le nom de l'usager ou une partie de son nom.

3.3.1 Consignes générales

- Privilégier les mots de passe longs
- Ne pas utiliser d'anciens mot de passe
- N'utiliser aucun mot du dictionnaire (peu importe la langue : français, anglais ...) à l'endroit comme à l'envers.
- N'utiliser pas des mots/prénoms/noms faciles à deviner :
    - Nom, nom de famille, ami, nom d'animaux de compagnie, nom de vos enfants, nom de votre conjoint(e), partie d'un nom, ...
    - Nom de la compagnie, numéros de téléphone, adresses, ...
    - Date de fête
    - Modèles tels que : 1234, abcd, qwerty, password123, Juin2023, Automne2022, ...
- Utiliser des mots de passe différents pour chaque accès.
- Utiliser des mots de passe que vous n'utilisez pas dans votre vie personnelle
- Ne partagez pas vos mots de passe. En cas d'absence nécessitant l'échange de mot de passe, celui-ci devra être changé au retour de la personne.
- Ne stockez pas vos mots de passe dans des fichiers « standards » (Word, Excel, texte...).
- Aucun mot de passe ne doit être écrit (post-it sur l'écran ou en arrière du clavier ...).
- Utiliser une voûte encryptée (gestionnaire de mot de passe).
- Ne pas utiliser la fonction « Enregistrer mot de passe » d'une application ou de vos navigateurs internet (Chrome, Opera, Firefox, Edge...).

- Ne jamais transmettre de mot de passe par courriel.

3.3.1 Mot de passe

	Minimum requis	Commentaires
Nombres de caractères minimales	12	Pas de répétition ou de suite de caractère Ex : aaaaaa111111
Lettres minuscules	1	a à z
Lettres majuscules	1	A à Z
Nombre	1	0 à 9
Caractères spéciaux	1	#!()&%$...

Si vous avez un doute sur l'intégrité d'un mot de passe (mot de passe potentiellement compromis), veuillez en aviser notre équipe rapidement et en faire le changement.

4. Politique – Gestion documentaire

4.1 Objectifs de la politique

Cette politique s'applique à tous les documents contenant vos renseignements, qu'ils soient sous forme physique ou électronique, produits ou reçus, ainsi qu'à toutes les personnes qui interagissent avec ces documents dans le cadre de leurs fonctions professionnelles.

4.1.1 Stockage sécurisé

Les documents physiques seront conservés dans des espaces dédiés, tels que des armoires verrouillées ou des salles d'archives sécurisées. L'accès à ces espaces sera restreint aux personnes autorisées uniquement.

Les documents électroniques seront stockés dans des systèmes de gestion de documents électroniques (GED) sécurisés. Des mesures de sécurité telles que l'authentification multi-facteurs, le chiffrement des données et les autorisations d'accès seront mises en place pour protéger ces documents contre tout accès non autorisé.

Des mesures de sécurité appropriées doivent être mises en place pour protéger les documents contre tout accès non autorisé, altération ou perte. Les documents sensibles doivent être traités avec un niveau de confidentialité approprié et protégés en conséquence.

4.2 Conservation

Les périodes de conservation doivent être déterminées en fonction des exigences légales, réglementaires et opérationnelles. Les documents doivent être conservés pendant la durée nécessaire, puis éliminés de manière sécurisée conformément aux politiques de destruction des documents.

4.3 Révision et mise à jour

Les documents doivent être régulièrement révisés et mis à jour pour refléter les changements organisationnels, législatifs ou technologiques pertinents. Les versions obsolètes doivent être archivées ou éliminées de manière appropriée.

---

5. Cas de non-respect des politiques

Pour assurer le respect des politiques de sécurité de l'information et maintenir un environnement de travail sûr et sécurisé, un cadre de sanctions clair est établi pour traiter les cas de non-respect des règles et des procédures établies. Les sanctions applicables sont définies en fonction de la gravité de l'infraction et peuvent inclure les mesures suivantes :

5.1 Réduction des privilèges d’accès

En cas de violation grave ou répétée des politiques de sécurité, l'employé peut se voir temporairement ou définitivement retirer certains privilèges d'accès aux systèmes ou aux données de l'entreprise. Cette mesure vise à limiter les risques liés au comportement de l’utilisateur et à protéger les actifs informationnels de l'entreprise.

Cette politique entre en vigueur dès sa publication et est contraignante pour tous les employés de l’entreprise et ses filiales. Cette politique a été approuvée par la direction générale de Côté-Reco et sera révisée périodiquement pour assurer sa pertinence et son efficacité.

En acceptant, vous confirmez avoir lu et compris la politique de sécurité informatique de l’entreprise et vous acceptez de respecter toutes les règles et procédures décrites dans ce document.