Politique de sécurité des renseignements
Détenteurs de carte de crédit

Loisirs Renaud-Coursol
320 Rue Richard, Laval, QC H7M 1T8
450-933-5574
www.renaudcoursol.com

2025-01-30
Mise à jour 2025-02-14

Loisirs
Renaud·Coursol

Table des matières

Introduction **2**
Politique de sécurité des renseignements **2**
1. Sécurité des réseaux **3**
2. Politique d'utilisation acceptable **3**
3. Protection des données stockées **4**
4. Classification des renseignements **4**
5. Accès aux données de titulaire de carte de paiement **5**
6. Sécurité physique **5**
7. Protection des données en transit **6**
8. Élimination des données stockées **7**
9. Sensibilisation à la sécurité et procédures **7**
10. Plan de Réaction aux Incidents de Sécurité liés aux Cartes de Crédit (PCI) **8**
11. Politique de Transfert des Informations Sensibles **12**
12. Gestion de l'accès utilisateur **12**
13. Politique relative au contrôle d'accès **13**
LEXIQUE **14**
Annexe B : Liste des dispositifs **16**
Annexe C -Autres Prestataires de Services de Paiement **16**
Annexe D - Politique de Gestion des POI autonomes et P2PE **16**
Annexe E - Politique de Configuration et de Renforcement du eCommerce **17**

Introduction

Le présent document de politique englobe tous les aspects de la sécurité entourant les renseignements confidentiels de Loisirs Renaud-Coursol et doit être distribué à l'équipe utilisant le système d'inscription de Loisirs Renaud-Coursol. Les employés et bénévoles doivent lire ce document dans son intégralité et signer le formulaire confirmant qu'ils ont entièrement lu et compris cette politique. Ce document sera révisé et mis à jour par la direction sur une base annuelle ou lorsque jugé pertinent pour comprendre les normes de sécurité nouvellement élaborées et ajoutées à la politique et distribuées à l'ensemble des employés, bénévoles et ses agents contractuels, le cas échéant.

Politique de sécurité des renseignements

Loisirs Renaud-Coursol traite quotidiennement des informations sensibles. Les informations sensibles doivent faire l'objet de mesures de protection adéquates afin de protéger les données du compte, y compris les données du titulaire de la carte de paiement, la vie privée du titulaire de la carte de paiement, et d'assurer la conformité avec les diverses réglementations, tout en préservant l'avenir de l'organisation.

Loisirs Renaud-Coursol s'engage à respecter la vie privée de tous ses clients et à protéger les données des clients contre les tiers. À cette fin, la direction s'engage à maintenir un environnement sécurisé pour le traitement des informations relatives aux titulaires de cartes de paiement, afin que nous puissions tenir nos promesses.

- Traiter les informations relatives à l'entreprise et au compte d'une manière qui corresponde à leur sensibilité et à leur classification ;
- Restreindre l'usage des renseignements de Loisirs Renaud-Coursol et les systèmes de télécommunication et assurer qu'il n'interfère avec votre rendement au travail;
- Loisirs Renaud-Coursol se réserve le droit de surveiller, d'accéder, de réviser, de vérifier, de copier, de stocker ou de supprimer toute communication électronique, tout équipement, système et trafic réseau à toute fin;
- N'utilisez pas le courriel, Internet et les autres ressources de Loisirs Renaud-Coursol pour vous engager dans une action offensive, menaçante, discriminatoire, diffamatoire, pornographique, obscène, harcelante ou illégale;
- Ne divulguez jamais de renseignements personnels, à moins d'y être autorisé;
- Protéger les données sensibles des cartes de paiement et renseignements personnels des comptes, y compris les informations relatives aux titulaires de cartes de paiement;
- Conservez les mots de passe et les comptes en toute sécurité;
- Demandez l'approbation de la direction avant d'établir tout nouveau matériel informatique ou logiciel, des connexions avec des tiers, etc.;
- N'installez pas de logiciel ou de matériel informatique non autorisé, notamment des modems ou un accès sans fil, à moins d'avoir expressément été autorisé par la direction;
- Laissez toujours les bureaux libres de données de titulaire de carte de paiement et verrouillez les écrans d'ordinateur lorsqu'ils sont sans surveillance;
- Les incidents liés à la sécurité des renseignements doivent être signalés, sans délai, à la personne responsable de la réponse aux incidents à l'échelle locale. Assurez-vous de savoir de qui il s'agit;
- Participer à une formation de sensibilisation à la sécurité sur une base annuelle.

Nous avons tous la responsabilité de nous assurer que les systèmes et les données de notre entreprise sont protégés de tout accès non autorisé et d'usage inapproprié. Si vous avez des doutes concernant n'importe quelle des politiques détaillées aux présentes, demandez des conseils et des directives à

votre gestionnaire hiérarchique.

1. Sécurité des réseaux

Un diagramme de haut niveau du réseau est tenu à jour et revu chaque année. Le diagramme de réseau fournit une vue d'ensemble de l'environnement des données du titulaire de la carte (CDE), qui montre au minimum les connexions entrantes et sortantes du CDE. Les composants essentiels du système au sein du CDE, tels que les dispositifs POI/POS, les bases de données, les serveurs web de commerce électronique, les serveurs de réorientation/iFrame, etc. et tout autre composant de paiement nécessaire, le cas échéant, doivent également être illustrés.

En outre, l'ASV doit être effectué et complété par un fournisseur de services d'analyse approuvé par le PCI SSC sur une base trimestrielle (tous les 90-92 jours), le cas échéant. Les preuves de ces scans doivent être conservées pendant une période de 18 mois. Pour le eCommerce, les analyses doivent inclure au minimum les serveurs de redirection/iFrame.

Pour les terminaux de type standalone-dialup : Non utilisé

Pour les solutions P2PE : Non utilisé

Pour le commerce électronique qui utilise la redirection/iFrame vers une page de paiement hébergée : voir l'Annexe D.

2. Politique d'utilisation acceptable

Les intentions de la direction de publier une politique d'utilisation acceptable consistent à ne pas imposer de restrictions contraires à la culture d'ouverture, de confiance et d'intégrité établie de Loisirs Renaud-Coursol . La direction s'est engagée à protéger les employés, bénévoles, partenaires et Loisirs Renaud-Coursol de toutes les actions illégales ou dommageables prises par des personnes, que ce soit sciemment ou non. Loisirs Renaud-Coursol tiendra à jour une liste approuvée des technologies et dispositifs et du personnel et des bénévoles ayant accès à de tels dispositifs, tel que détaillé à l'Annexe B.

- Il incombe aux employés et bénévoles d'exercer un bon jugement en regard du caractère raisonnable de l'usage personnel.
- Les employés doivent prendre toutes les mesures nécessaires pour prévenir l'accès non autorisé aux données confidentielles, notamment les données de titulaire de carte de paiement.
- Veuillez garder les mots de passe sécurisés et ne partagez pas de comptes.
- Les utilisateurs autorisés sont responsables de la sécurité de leurs mots de passe et de leurs comptes.
- Tous les ordinateurs de bureau, ordinateurs portatifs et postes de travail doivent être sécurisés avec un économiseur d'écran doté d'une fonctionnalité d'activation automatique.
- Tous les PDV et les dispositifs de saisie de PIN doivent être adéquatement protégés et sécurisés de manière à ne pas pouvoir être trafiqués ni modifiés.
- Les employés et bénévoles doivent prendre toutes les mesures nécessaires pour empêcher l'accès non autorisé aux données confidentielles, y compris les données relatives aux comptes et aux titulaires de cartes de paiement.

- La liste des dispositifs figurant à l'Annexe B sera régulièrement mise à jour en cas de modification, d'ajout ou de mise hors service de dispositifs. Un inventaire des dispositifs sera régulièrement effectué et les dispositifs seront inspectés afin d'identifier toute altération ou substitution potentielle des dispositifs.
- Puisque les renseignements contenus dans les ordinateurs portatifs sont particulièrement vulnérables, une attention particulière est nécessaire.
- Les affichages que font les employés à partir d'une adresse de courriel de Loisirs Renaud-Coursol vers des groupes de discussion doivent contenir une dénégation de responsabilité indiquant que les opinions exprimées leur sont propres et qu'elles ne sont pas nécessairement celles de Loisirs Renaud-Coursol , à moins que l'affichage n'ait été fait dans le cadre d'activités professionnelles.
- Les employés et bénévoles doivent faire preuve d'une extrême prudence lorsqu'ils ouvrent des pièces jointes reçues d'expéditeurs inconnus, qui peuvent contenir des virus, des bombes logiques, des chevaux de Troie ou des attaques par hameçonnage.

3. Protection des données stockées

- Loisirs Renaud-Coursol et ses employés et bénévoles ne doivent en aucun cas stocker les données du titulaire de la carte de paiement sous forme de PAN ou de données d'authentification sensibles sous forme électronique.
- Toutes les données sensibles relatives aux comptes, y compris les données relatives aux titulaires de cartes de paiement, stockées et traitées sur papier par Loisirs Renaud-Coursol et ses employés, et bénévoles doivent être protégées en permanence contre toute utilisation non autorisée. Toutes les données sensibles relatives aux cartes de paiement qui ne sont plus nécessaires à Loisirs Renaud-Coursol pour des raisons commerciales doivent être éliminées de manière sûre et irrécupérable.
- S'il n'y a pas de besoin spécifique de voir le PAN (Primary Account Number) complet, il doit être masqué lorsqu'il est affiché et les six premiers et quatre derniers chiffres du PAN doivent être affichés au maximum.
- Les PAN qui ne sont pas protégés comme indiqué ci-dessus ne doivent pas être envoyés au réseau extérieur via les technologies de messagerie de l'utilisateur final telles que le courrier électronique, les chats, ICQ messenger, etc,

Il est strictement interdit de stocker :

1. **Le contenu de la bande magnétique de la carte de paiement (données de piste) ou les données de piste équivalentes à celles de la puce, sur quelque support que ce soit.**
2. **Le CVV2/CVC2/CAV2/CID (le numéro à 3 ou 4 chiffres figurant dans le champ de signature au verso de la carte de paiement) sur quelque support que ce soit.**
3. **Le PIN ou le bloc PIN encodé, en aucune circonstance.**

4. Classification des renseignements

Les données et les supports qui contiennent des données doivent toujours être étiquetés de manière à indiquer leur niveau de sensibilité

- **Les données confidentielles** peuvent comprendre des fonds de renseignements pour lesquels il existe des exigences juridiques visant à prévenir la divulgation, ou des sanctions financières

pour toute divulgation, ou de données qui entraîneraient de sérieux préjudices à Loisirs Renaud-Coursol si elles étaient divulguées ou modifiées. **Les données confidentielles comprennent les données de titulaire de carte**.

- **Les données pour usage interne** peuvent comprendre des renseignements que le titulaire des données considère comme devant être protégées pour en éviter toute divulgation non autorisée;
- **Les données publiques** sont des renseignements qui peuvent être diffusés librement.

5. Accès aux données de titulaire de carte de paiement

Tous les accès aux titulaires de cartes de paiement doivent être contrôlés et autorisés. Toute fonction nécessitant l'accès aux données du titulaire de la carte doit être clairement définie.

- L'affichage des données du compte ou du titulaire de la carte doit être limité au minimum aux 6 premiers et aux 4 derniers chiffres du numéro de compte primaire (PAN).
- L'accès aux informations sensibles relatives aux titulaires de cartes de paiement, telles que les PAN, les informations personnelles et les données commerciales, est limité aux employés et bénévoles qui ont un besoin légitime de consulter ces informations.
- Aucun autre employé ou bénévole ne doit avoir accès à ces données confidentielles, à moins qu'il n'en ait véritablement besoin pour des raisons professionnelles ou dans le cadre de ses fonctions.
- Si les données relatives aux titulaires de cartes de paiement sont partagées avec un prestataire de services (tiers), une liste de ces prestataires de services sera tenue à jour, comme indiqué à l'Annexe C.
- Loisirs Renaud-Coursol veillera à ce qu'un accord écrit comprenant une reconnaissance soit en place, selon lequel le prestataire de services sera responsable des données du titulaire de la carte de paiement que le prestataire de services tiers (TPSP) possède.
- Loisirs Renaud-Coursol s'assurera de l'existence d'un processus établi, comprenant une diligence raisonnable, avant de s'engager avec un TPSP.
- L'entreprise disposera d'un processus permettant de contrôler la conformité à la norme PCI DSS du TPSP.
- L'Entreprise doit veiller à ce que les responsabilités en matière de sécurité des données relatives aux comptes et aux titulaires de cartes de paiement soient définies entre l'entreprise et le TPSP. Ces éléments doivent être consignés dans une matrice des responsabilités.

6. Sécurité physique

L'accès aux renseignements personnels et confidentiels, tant au format sur support papier ou souple doit être physiquement restreint pour prévenir toutes les personnes non autorisées d'obtenir des données sensibles.

- Un support se définit comme tout document papier imprimé ou rédigé à la main, télécopie reçue, bande de sauvegarde, disque dur d'ordinateur, etc.
- Un support contenant des renseignements de titulaires de carte de paiement doit être manipulé et distribué de manière sécurisée par des personnes de confiance.
- Les visiteurs doivent toujours être accompagnés par un employé de confiance dans des zones où se trouvent des renseignements de titulaires de carte de paiement.
- Des procédures doivent être mises en place pour aider l'ensemble du personnel à distinguer facilement les employés des visiteurs, particulièrement dans les zones où des données de

titulaire de carte de paiement sont accessibles. Le terme « employé » fait référence aux employés et au personnel à temps plein et à temps partiel ainsi qu'aux consultants qui sont « résidents » sur les lieux de Loisirs Renaud-Coursol . Un « visiteur » se définit comme un fournisseur, l'invité d'un employé, du personnel de service, ou quiconque qui doit pénétrer sur les lieux pour une courte durée, habituellement pas plus d'une journée.

- Les connecteurs réseau situés dans les espaces publics et accessibles aux visiteurs doivent être désactivés et activés lorsque l'accès au réseau est explicitement autorisé.
- Il convient de tenir à jour une liste des dispositifs, y compris les terminaux des points d'interaction (POI), qui acceptent les données des cartes de paiement.
- La liste doit inclure la marque, le modèle et l'emplacement du dispositif (POI).
- La liste doit comporter le numéro de série ou un identifiant unique du dispositif (POI).
- La liste doit être mise à jour lorsque des dispositifs (POI) sont ajoutés, supprimés ou déplacés.
- Les surfaces des dispositifs POS sont périodiquement inspectées afin de détecter toute altération ou substitution.
- Le personnel qui utilise les dispositifs doit être formé et conscient de la nécessité de manipuler les dispositifs POI.
- Le personnel utilisant les dispositifs doit vérifier l'identité de tout tiers prétendant réparer ou effectuer des tâches de maintenance sur les dispositifs (POI), installer de nouveaux dispositifs (POI) ou remplacer des dispositifs (POI).
- Le personnel qui utilise les dispositifs doit être formé à signaler tout comportement suspect et toute indication de falsification des dispositifs (POI) au personnel approprié des sites de Loisirs Renaud-Coursol. Un « visiteur » est défini comme un vendeur, l'invité d'un employé, le personnel de service ou toute personne qui doit entrer dans les locaux pour une courte durée, généralement pas plus d'une journée.
- Un contrôle rigoureux doit être exercé quant à la distribution à l'externe ou à l'interne de tout support contenant des données de titulaire de carte et ce contrôle doit être approuvé par la direction.
- Un contrôle rigoureux doit également être exercé quant au stockage et à l'accessibilité du support.
- Tous les ordinateurs dans lesquels sont stockées des données de titulaire de carte doivent être munis d'un économiseur d'écran protégé par mot de passe activé pour en prévenir l'utilisation non autorisée.

7. Protection des données en transit

Toutes les données de titulaire de carte doivent être protégées de manière sécurisée lorsqu'elles doivent être transportées de manière physique ou électronique.

- Les données de titulaire de carte (NCP, données de suivi, etc.) ne doivent jamais être envoyées par courriel sur Internet, par clavardage instantané ou au moyen de toute autre technologie destinée à un utilisateur final.
- S'il y a un motif commercial d'envoyer des données de titulaire de carte par courriel, par Internet ou par tout autre moyen, cela doit alors se faire après en avoir obtenu l'autorisation et au moyen d'un mécanisme de cryptage puissant (c.à-d., cryptage AES, PGP, IPSEC, etc.).
- Le transport de supports contenant des données de titulaires de carte de paiement à un autre endroit doit être autorisé par la direction, consigné dans un journal et inventorié avant de quitter les lieux. Seuls les services de messagerie sécurisés peuvent être utilisés pour le transport de tels supports. L'état de l'expédition doit être surveillé jusqu'à la livraison au nouvel emplacement.

8. Élimination des données stockées

- Toutes les données doivent être éliminées de manière sécurisée lorsque Loisirs Renaud-Coursol n'en a plus besoin, peu importe le support ou le type d'application sur lequel elles sont stockées.
- Un processus automatique doit être mis en place pour supprimer de manière permanente les données en ligne qui ne servent plus.
- Toutes les copies papier de données de titulaire de carte doivent être détruites manuellement lorsqu'elles ne sont plus utiles pour des motifs commerciaux valides et justifiés. Un processus trimestriel doit être mis en place pour confirmer que les données de titulaire de carte sous une autre forme électronique ont été éliminées de manière appropriée et en temps opportun.
- Loisirs Renaud-Coursol devra avoir prévu des procédures de destruction pour le matériel au format papier. Ces procédures permettront de veiller à ce que le matériel au format papier soit coupé en travers, déchiqueté, incinéré ou désintégré de manière à ne pas pouvoir être reconstitué.
- Loisirs Renaud-Coursol devra avoir des procédures documentées pour la destruction des supports électroniques. Ces procédures comprendront :
    - Toutes les données de titulaire de carte sur support électronique doivent être rendues irrécupérables lorsque supprimées, p. ex., par la démagnétisation le nettoyage électronique au moyen de procédés de suppression sécurisés de grade militaire ou par la destruction matérielle du support;
    - Si des programmes de nettoyage sécurisés sont utilisés, la procédure doit être définie selon les normes acceptées dans l'industrie, suivies d'une suppression sécurisée.
- Tous les renseignements de titulaire de carte en attente de destruction doivent être conservés dans des récipients de stockage clairement identifiés « Pour déchiquetage » et l'accès à ces récipients doit être restreint.

9. Sensibilisation à la sécurité et procédures

Les politiques et procédures décrites ci-dessous doivent être comprises dans les pratiques de Loisirs Renaud-Coursol pour maintenir un niveau élevé de sensibilisation à la sécurité. La protection des données sensibles nécessite une formation régulière de l'ensemble des employés et entrepreneurs.

- Veuillez effectuer une révision des procédures de manutention des renseignements personnels et confidentiels et organiser des réunions périodiques sur la sensibilisation à la sécurité pour inclure ces procédures dans les pratiques quotidiennes de Loisirs Renaud-Coursol .
- Distribuez ce document de politique de sécurité à tous les employés de Loisirs Renaud-Coursol pour qu'ils le lisent. Il incombe à tous les employés de confirmer qu'ils comprennent le contenu de ce document de politique de sécurité en signant un formulaire d'attestation (voir l'Annexe A).
- Tous les employés qui manipulent des renseignements sensibles seront soumis à des vérifications des antécédents (comme des vérifications de casier judiciaire et de dossier de crédit, dans des limites permises par la loi locale) avant d'entrer en poste à Loisirs Renaud-Coursol .
- Tous les tiers ayant accès à des numéros de compte de carte de paiement sont tenus par contrat de se conformer à la norme de sécurité liée aux cartes (PCI/DSS).
- Les politiques de sécurité de Loisirs Renaud-Coursol doivent être révisées tous les ans et mises à jour au besoin.
- La sensibilisation à la sécurité doit inclure la sensibilisation à l'hameçonnage.

10.Plan de Réaction aux Incidents de Sécurité liés aux Cartes de Crédit (PCI)

Le plan de réponse aux incidents PCI de Loisirs Renaud-Coursol est comme suit :

1. Chaque division doit signaler un incident à l'officier de sécurité des renseignements (préférablement) ou à un autre membre de l'équipe de réponse PCI.
2. Ce membre de l'équipe qui reçoit le rapport avisera l'équipe de réponse PCI de l'incident.
3. L'équipe de réponse PCI mènera une enquête concernant l'incident et assistera la division potentiellement compromise en limitant l'exposition des données de titulaire de carte et en atténuant les risques liés à l'incident.
4. L'équipe de réponse PCI résoudra le problème à la satisfaction de toutes les parties en cause, notamment en signalant l'incident et les conclusions aux parties concernées (associations de cartes de crédit, organismes responsables du traitement de cartes, etc.) au besoin.
5. L'équipe de réponse PCI déterminera si les politiques et les processus en place doivent être mis à jour pour éviter tout incident semblable dans l'avenir et si des mesures de protection supplémentaires sont requises dans l'environnement où l'incident s'est produit, ou pour l'institution.

Équipe de Réaction aux Incidents de Sécurité PCI de Loisirs Renaud-Coursol :

Responsable de l'Information, de la conformité et des risques	Lucie Lanthier

Procédures de Réaction aux Incidents de Sécurité de l'Information PCI :

Une division qui a des motifs raisonnables de croire avoir été victime d'une brèche de compte, ou d'une brèche d'information de titulaire de carte ou de systèmes liés à l'environnement PCI en général, doit informer l'équipe de réponse aux incidents PCI de Loisirs Renaud-Coursol . Après avoir été avisée d'une compromission, l'équipe de réponse PCI de pair avec tout autre personnel désigné, procéderont à la mise en œuvre du plan de réponse aux incidents PCI pour aider et bonifier les plans de réponse de la division.

Notification de réponse aux incidents

Membres de Cordée :

Escalade - Premier niveau
Directeur de Loisirs Renaud-Coursol

Escalade - Deuxième niveau
Président de Loisirs Renaud-Coursol

Personnes-ressources externes (au besoin)
Fournisseurs de cartes aux marchands
Marques
Fournisseur de services Internet (le cas échéant)
Fournisseur de services Internet de l'intrus (le cas échéant)
Supports de communication (locaux et longue distance)
Partenaires commerciaux

Société d'assurance
Équipe de réponse externe le cas échéant (Centre de coordination CERT 1, etc.)
Organismes d'application de la loi, le cas échéant, dans la juridiction locale

En réponse à une compromission des systèmes, l'équipe de réponse PCI et ses délégués :

1. S'assureront que le(s) système(s) compromis est/sont isolé(s) sur/du réseau.
2. Rassembleront, examineront et analyseront les listes de contrôle et l'information connexe de diverses mesures de protection et contrôles de sécurité locaux.
3. Mèneront une analyse judiciaire appropriée du système compromis.
4. Communiqueront avec des divisions et des entités externes au besoin.
5. Mettront l'analyse judiciaire et les listes de contrôle à la disposition des organismes responsables de l'application de la loi ou du personnel de sécurité de l'industrie des cartes au besoin.
6. Aideront le personnel responsable de l'application de la loi et de la sécurité des cartes de l'industrie dans les processus d'enquête, notamment les poursuites.

Les compagnies de cartes ont des exigences individuelles précises que l'équipe de réponse doit observer dans le signalement de brèches soupçonnées ou confirmées de données de titulaire de carte.

Notifications de réponse aux incidents selon divers systèmes de carte

1. Dans l'éventualité d'un soupçon de brèche de sécurité, veuillez aviser le responsable de la sécurité des renseignements, ou votre gestionnaire hiérarchique, dans les plus brefs délais.
2. Le responsable de la sécurité mènera une enquête initiale de la brèche de sécurité soupçonnée.
3. Sur confirmation de l'occurrence d'une brèche de sécurité, le responsable de la sécurité avisera la direction et commencera à en informer toutes les parties concernées qui pourraient être touchées par une telle compromission.

Étapes VISA

Si la compromission de la sécurité des données met en cause des numéros de compte de carte de crédit, vous devez mettre la procédure suivante en œuvre :

- Éteindre tous les systèmes et les procédés impliqués dans la brèche pour en limiter l'étendue et prévenir toute autre exposition.
- Alerter les parties touchées et les autorités comme la banque du commerçant (votre banque), le contrôle des fraudes Visa et la police.
- Fournir des détails concernant l'ensemble des numéros de carte compromis ou potentiellement compromis au Contrôle des fraudes Visa dans un délai de 24 heures.
- Pour obtenir de plus amples renseignements, visitez le : http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

Modèle de rapport d'incident Visa

Ce rapport doit être remis à VISA dans un délai de 14 jours suivant le signalement initial de l'incident à VISA. Le contenu du rapport et les normes suivantes doivent être respectées lors de la rédaction du rapport d'incident. Le rapport d'incident doit être distribué de manière sécurisée à

VISA et à la banque du marchand. Visa classera le rapport avec la mention « Secret Visa »*.

I. Sommaire exécutif
    a. Comprend un aperçu de l'incident
    b. Comprend le niveau de RISQUE (élevé, moyen, faible)
    c. Détermine si la compromission a été contenue
II. Contexte
III. Analyse initiale
IV. Procédures d'enquête
    a. Comprend les outils judiciaires utilisés durant l'enquête
V. Conclusions
    a. Nombre de comptes à risque, identifie ces commerces et compromissions
    b. Type de renseignements de compte à risque
    c. Identifie TOUS les systèmes analysés. Comprend ce qui suit :
        - Noms du système de nom de domaine (DNS)
        - Adresses de protocole Internet (IP)
        - Version du système d'exploitation (OS)
        - Fonction du/des système(s)
    d. Identifie TOUS les systèmes compromis.Comprend ce qui suit :
        - Noms DNS
        - Adresses IP
        - Version du système d'exploitation (OS)
        - Fonction du/des système(s)
    e. Délai de la compromission
    f. Toutes les données exportées par l'intrus
    g. Établit la manière et la source de la compromission
    h. Vérifie tous les emplacement éventuels de bases de données pour assurer qu'aucune donnée CVV1, Données de suivi 1 ou Données de suivi 2 ne sont stockées nulle part, qu'elles soient chiffrées ou non (p. ex., tables dupliquées ou de sauvegarde ou bases de données, bases de données utilisées dans le développement, environnements d'étape ou de mise à l'essai, données sur le logiciel des machines des ingénieurs, etc.)
    i. Au besoin, revoir la sécurité au point final de VisaNet et déterminer le risque
VI. Action de l'entité compromise
VII. Recommandations
VIII. Personne(s)-ressource de l'entité et de l'évaluateur de la sécurité qui procèdent à l'enquête

*Cette classification s'applique aux renseignements commerciaux les plus sensibles et doit être utilisée pour VISA. Sa divulgation non autorisée pourrait avoir une incidence grave et nuisible pour VISA, ses employés, banques membres, partenaires commerciaux et/ou la marque.

Étapes MasterCard :

1. Dans un délai de 24 heures d'un événement de compromission de compte, aviser l'équipe des comptes compromis MasterCard en téléphonant au 1-636-722-4100.
2. Fournir un énoncé détaillé par écrit du fait concernant la compromission du compte (y compris les circonstances concourantes) par courriel sécurisé à compromised_account_team@mastercard.com.
3. Fournir au service du contrôle des fraudes aux marchands MasterCard une liste complète de tous les numéros de compte compromis connus.
4. Dans un délai de 72 heures de la connaissance d'un compte soupçonné compromis, faire appel

aux services d'une compagnie de sécurité des données acceptable pour MasterCard pour évaluer la vulnérabilité des données compromises et des systèmes connexes (comme une évaluation judiciaire détaillée).

5. Fournir des rapports d'état écrits hebdomadaires à MasterCard, traitant les questions ouvertes et les problèmes jusqu'à ce que l'audit soit terminé à la satisfaction de MasterCard.
6. Fournir sans tarder des listes à jour de numéros de compte compromis connus, de la documentation supplémentaire et toute autre information que MasterCard pourrait demander.
7. Fournir les conclusions de tous les audits et de toutes les enquêtes au service de contrôle des fraudes aux marchands de MasterCard dans les délais prescrits et continuer de traiter toute exposition ou recommandation en suspens jusqu'à ce qu'elles soient résolues à la satisfaction de MasterCard.

Une fois que MasterCard obtient les détails des données de comptes compromis et la liste des numéros de compte compromis, MasterCard :

1. Identifiera les émetteurs des comptes qui ont été soupçonnés avoir été compromis et regroupera tous les comptes connus sous leur ID respectif de membre parent.

2. Distribuera les données de numéros de compte à leurs émetteurs respectifs.

Les employés de Loisirs Renaud-Coursol doivent signaler tous les problèmes de sécurité à l'officier de la sécurité. Le rôle de l'officier de la sécurité consiste à communiquer efficacement l'ensemble des politiques et procédures liées à la sécurité aux employés de Loisirs Renaud-Coursol et aux entrepreneurs. En outre, cet officier de la sécurité doit superviser les horaires des séances de formation en sécurité, contrôler et faire appliquer les politiques de sécurité décrites dans ce document et lors des séances de formation et enfin, superviser la mise en œuvre du plan de réponse aux incidents dans l'éventualité où des données sensibles seraient compromises.

Étapes Discover

I. Dans un délai de 24 heures d'un événement de compromission de compte, aviser le service de la prévention des fraudes de Discover.
II. Préparer un énoncé détaillé par écrit du fait concernant la compromission du compte, y compris les circonstances concourantes.
III. Préparer une liste de tous les numéros de compte compromis connus.
IV. Obtenir des exigences supplémentaires précises de la part de Discover.

Étapes American Express

I. Dans un délai de 24 heures d'un événement de compromission de compte, aviser les services aux marchands American Express.
II. Préparer un énoncé détaillé par écrit du fait concernant la compromission du compte, y compris les circonstances concourantes.
III. Préparer une liste de tous les numéros de compte compromis connus. Obtenir des exigences supplémentaires précises de la part d'American Express.

11.Politique de Transfert des Informations Sensibles

- Toutes les entreprises de tierce partie prodiguant des services essentiels à Loisirs Renaud-Coursol doivent fournir une entente convenue sur les niveaux de service.
- Toutes les entreprises de tierce partie fournissant des services d'hébergement doivent se conformer à la politique sur la sécurité physique et le contrôle de l'accès de Loisirs Renaud-Coursol .
- Toutes les entreprises tierces susceptibles d'affecter la sécurité des informations relatives au titulaire de la carte doivent :

    1. respecter les exigences PCI DSS en matière de sécurité.
    2. reconnaître leur responsabilité quant à la sécurité des données des titulaires de carte de paiement.
    3. reconnaître que les données de titulaire de carte de paiement doivent uniquement être utilisées pour aider à conclure une transaction, appuyer un programme de fidélité, fournir un service de contrôle de la fraude ou pour des usages spécifiquement requis par la loi.
    4. avoir des dispositions appropriées pour la continuité des affaires dans l'éventualité d'une interruption, d'un désastre ou d'une majeure.
    5. fournir leur entière collaboration et accès pour mener un examen approfondi de la sécurité à la suite d'une intrusion à un représentant de l'industrie des cartes de paiement, ou à un tiers approuvé par l'industrie des cartes de paiement.

12.Gestion de l'accès utilisateur

- L'accès à Loisirs Renaud-Coursol est contrôlé au moyen d'un processus d'enregistrement de l'utilisateur formel commençant par un avis formel des RH ou d'un gestionnaire hiérarchique.
- Chaque utilisateur est identifié par un ID utilisateur unique de manière à ce que les utilisateurs puissent être liés à leurs actes et tenus responsables de ceux-ci. L'utilisation d'un groupe d'ID est uniquement permis lorsque convenable pour les travaux menés.
- Il y existe un niveau d'accès standard; d'autres services peuvent être accédés lorsque les RH ou des cadres hiérarchiques l'ont spécifiquement autorisé.
- La fonction professionnelle de l'utilisateur permet de décider le niveau d'accès que l'employé a aux données de titulaire de carte.
- Une demande de service peut être faite par écrit (par courriel ou copie papier) par le gestionnaire hiérarchique du nouvel employé ou par les RH. La demande est au format libre, mais elle doit indiquer :

    Le nom de la personne qui présente la demande :
    Le titre de poste des nouveaux employés et leur groupe de travail :
    La date d'entrée en fonction :
    Les services requis (les services par défaut sont : MS Outlook, MS Office et l'accès Internet) :

- Chaque utilisateur se verra remettre une copie de son formulaire de nouvel utilisateur pour fournir une attestation écrite de ses droits d'accès, signée par un représentant des TI après la procédure d'induction. L'utilisateur signe le formulaire, indiquant qu'il comprend les conditions d'accès.
- L'accès à l'ensemble des systèmes de Loisirs Renaud-Coursol est fourni par les TI et peut uniquement commencer une fois les procédures appropriées complétées.

- Dès qu'une personne quitte son emploi au sein de Loisirs Renaud-Coursol , toutes ses connexions au système doivent être immédiatement révoquées et son compte doit être désactivé et supprimé.
- Dans le cadre du processus de fin d'emploi de l'employé (des cadres hiérarchiques dans le cas d'entrepreneurs), les RH informeront les opérations des TI de toutes les personnes qui quittent leur emploi ainsi que de leur date de départ.

13. Politique relative au contrôle d'accès

- Des systèmes de contrôle d'accès sont en place pour protéger les intérêts de l'ensemble des utilisateurs des systèmes informatiques de Loisirs Renaud-Coursol en fournissant un environnement sûr, sécurisé et facilement accessible dans lequel travailler.
- Loisirs Renaud-Coursol fournira à tous les employés et aux autres utilisateurs l'information dont ils ont besoin pour s'acquitter de leurs responsabilités de la manière la plus efficace et efficiente possible.
- Les ID génériques ou de groupe ne doivent habituellement pas être permis, mais ils peuvent être accordés dans des circonstances exceptionnelles si d'autres contrôles d'accès suffisants sont en place.
- L'affectation de droits de privilège (p. ex., administrateur local, administrateur de domaine, super-utilisateur, accès racine) doit être limitée et contrôlée, et l'autorisation doit être fournie conjointement par le propriétaire du système et les services de TI. Les équipes techniques doivent se protéger contre l'émission de droits de privilège de toutes les équipes pour prévenir la perte de confidentialité.
- Les droits d'accès seront accordés suivant les principes du moindre privilège et du besoin de savoir.
- Chaque utilisateur doit tenter de maintenir la sécurité des données à leur niveau de classification, même si les mécanismes de sécurité techniques échouent ou sont absents.
- Les utilisateurs qui choisissent de placer de l'information sur un support numérique ou des dispositifs de stockage ou de maintenir une base de données distincte doivent uniquement le faire lorsqu'une telle démarche est conforme à la classification des données.
- Il incombe aux utilisateurs de signaler les instances de non-conformité à l'officier général de la sécurité des renseignements.
- L'accès aux ressources et aux services de TI de Loisirs Renaud-Coursol sera accordé selon la disposition d'un compte Active Directory unique et d'un mot de passe complexe.
- Aucun accès aux ressources et services en TI de Loisirs Renaud-Coursol ne sera fourni sans authentification et autorisation préalable du compte Active Directory Windows d'un utilisateur de Loisirs Renaud-Coursol .
- L'émission d'un mot de passe, les exigences en matière de puissance, le changement et le contrôle seront gérés au moyen de processus formels. La longueur du mot de passe, sa complexité et ses délais d'expiration seront contrôlés au moyen des objets de la politique de groupe d'Active Directory Windows.
    - Mot de passe : 8 caractères, complexe, unique et à modifier à la première utilisation, non réutilisable, à modifier tous les 90 jours.
- L'accès à l'information confidentielle, restreinte et protégée sera limité aux personnes autorisées dont les responsabilités professionnelles l'exigent, comme déterminé par le propriétaire des

données ou son représentant désigné. Les demandes de permission d'accès qui doivent être accordées, changées ou révoquées doivent se faire par écrit.

- On s'attend à ce que les utilisateurs se familiarisent avec et respectent les politiques, normes et lignes directrices de Loisirs Renaud-Coursol pour l'usage acceptable des réseaux et des systèmes.
- L'accès aux utilisateurs distants doit être assujetti à l'autorisation des services de TI et accordé conformément à la politique d'accès à distance et à la politique de sécurité des renseignements. Aucun accès externe non contrôlé à un dispositif réseau ou à un système en réseau ne doit être permis.
- L'accès aux données est contrôlé de diverses manières et de façon appropriée selon les niveaux de classification décrits dans la politique de gestion de la sécurité des renseignements.
- Les méthodes de contrôle d'accès comprennent les droits d'accès de connexion, les permissions de Windows share et NTFS, les privilèges de compte utilisateur, les droits d'accès au serveur et aux postes de travail, les permissions de pare-feu, les droits d'authentification IIS intranet/extranet, les droits de base de données SQL, les réseaux isolés et d'autres méthodes au besoin.
- Un processus formel doit être mené à des intervalles réguliers par les propriétaires de système et de données, de pair avec les Services de TI pour réviser les droits d'accès des utilisateurs. La révision doit être consignée en journal et les services de TI doivent signer la révision pour donner le pouvoir aux utilisateurs de droits d'accès continus.

LEXIQUE

Données sensibles: représente les chiffres d'une carte de crédit ou débit, le chiffre CVV ou la date d'expiration.

Entériné par le conseil d'administration de Loisirs Renaud-Coursol en date du 18 février 2025 par résolution 20250218-001.

Annexe A – Formulaire d'acceptation de conformité avec les politiques de sécurité

_____
Nom de l'employé ou du bénévole (en caractères d'imprimerie)

_____
Service

J'accepte de prendre toutes les précautions raisonnables pour assurer que les renseignements internes de Loisirs Renaud-Coursol , ou les renseignements qui ont été confiés à Loisirs Renaud-Coursol par des tiers comme des clients, ne seront pas divulgués à des personnes non autorisées.

À la fin de mon emploi ou de mon contrat avec Loisirs Renaud-Coursol , je consens à retourner tous les renseignements auxquels j'ai eu accès dans le cadre de mes fonctions. Je comprends que je ne suis pas autorisé à utiliser de renseignements sensibles à mes propres fins, ni n'avoir la liberté de fournir ces renseignements à des tiers sans le consentement exprès du directeur interne désigné comme étant le propriétaire des renseignements.

J'ai accès à une copie des politiques relatives à la sécurité des renseignements, j'ai lu et j'ai compris ces politiques et je comprends comment elles influent sur mon travail. En tant que condition de mon emploi continu, je consens à respecter les politiques et les autres exigences trouvées dans la politique relative à la sécurité de Loisirs Renaud-Coursol .

Je comprends que la non-conformité sera un motif de mesures disciplinaires pouvant mener jusqu'au renvoi, et à d'éventuelles sanctions pénales et/ou civiles.

Je consens également à signaler dans les plus brefs délais, toutes les violations ou violations soupçonnées des politiques relatives à la sécurité des renseignements au responsable de la sécurité désigné.

_____
Signature de l'employé

_____
Date

Annexe B : Liste des dispositifs

2024

Nom du bien/dispositif	Description	Propriétaire/Utilisateur approuvé	Emplacement
Vostro 7500	Portable	Lucie Lanthier	CCSL - Maison
Inspirion 5570	Vieux Portable	Myriam Landry	Maison
Inspirion 7640	Portable	Myriam Landry	CCSL - CCRF
Vostro 7500	Portable	Ana Rodriguez	CCSL
HP	Portable	non utilisé	
Inspirion 3000	Portable	Ken Tourangeau	Maison
Vostro AN-517	Portable	Alicia Negro	CCSL - PRC
Vostro AN-517	Portable	non utilisé	
Aspire	Portable	non utilisé	

Annexe C -Autres Prestataires de Services de Paiement

Nom du fournisseur de services	Coordonnées	Services prodigués	Conforme à la norme PCIN DSS	Date de validation de la PCI DSS
Les entreprises Amilia inc.	1751 rue Richardson, Suite 3.105 Montréal, Québec, H3K 1G6 Facture	Plateforme de gestion d'inscription et de paiement	https://trust.amilia.com/resources?s=ecdsrs46kmpq0yyvjnjbu&name=amilia-pci-dss-service-provider-level-1-|-attestation-of-compliance-(aoc)-2024	à recevoir

Annexe D - Politique de Gestion des POI autonomes et P2PE

Lorsque Loisirs Renaud-Coursol utilise des POI autonomes ou P2PE, les politiques suivantes sont applicables :

Inventaire et Gestion du dispositif POI :

- Tenir à jour un inventaire de tous les dispositifs POI, en indiquant la marque, le modèle, l'emplacement et le numéro de série.
- Établir des procédures pour ajouter, déplacer et mettre hors service des dispositifs POI en toute sécurité.

Mesures de sécurité physique :

- Sécuriser les dispositifs de la POI afin d'éviter toute falsification ou substitution. Cela inclut l'utilisation de scellés ou de boîtiers inviolables.
- Inspecter régulièrement les dispositifs pour détecter tout signe de falsification ou de substitution.
- Mettre en place un stockage sécurisé pour les dispositifs non utilisés.

Inspection et maintenance du dispositif :

- Procéder régulièrement à l'inspection et à l'entretien des dispositifs d'identification des points d'intérêt afin de s'assurer qu'ils fonctionnent correctement et qu'ils n'ont pas été compromis.
- Documenter et tenir un registre de toutes les inspections et activités de maintenance.

Gestion sécurisée des configurations et des logiciels :

- Veiller à ce que les dispositifs POI soient configurés de manière sécurisée et en conformité avec les exigences de la norme PCI DSS.
- Mettre en œuvre des mesures visant à empêcher toute modification non autorisée des logiciels et des paramètres de configuration.
- Mettre régulièrement à jour le logiciel du dispositif POI, y compris les correctifs pour les vulnérabilités connues.

Contrôles d'Accès :

- Restreindre l'accès aux dispositifs POI au seul personnel autorisé.
- Utiliser des méthodes d'authentification forte pour l'accès administratif aux dispositifs POI.
- Mettre en place des contrôles d'accès basés sur les rôles et séparer les tâches afin de minimiser le risque d'accès ou de changements non autorisés.

Annexe E - Politique de Configuration et de Renforcement du eCommerce

Lorsque Loisirs Renaud-Coursol utilise des solutions re-direct et iFrame pour effectuer des paiements dans le cadre du eCommerce, elle doit configurer et renforcer ces systèmes comme suit :

Établir une Configuration Standard du Serveur de eCommerce :

- Définir une configuration standard pour les serveurs qui inclut les services, les protocoles et les paramètres nécessaires.
- Veiller à ce que les comptes par défaut des fournisseurs soient modifiés, supprimés ou désactivés.
- Désactiver les services et les protocoles inutiles afin de réduire les vulnérabilités.
- Veiller à ce que tous les paramètres de sécurité soient conformes aux meilleures pratiques du secteur.

Mettre en œuvre des Procédures de Renforcement :

- Mettre en œuvre des mécanismes d'authentification et d'autorisation solides.
- Utiliser des outils de contrôle de l'intégrité des fichiers pour détecter les modifications non autorisées.
- Renforcer l'utilisation de solutions antivirus et anti logiciels malveillants.

Contrôler l'Accès Administratif :

- Limiter l'accès aux configurations du serveur au seul personnel autorisé.
- Utiliser l'authentification à plusieurs facteurs pour l'accès administratif.
- Conserver une piste d'audit de tous les accès et de toutes les modifications apportées aux configurations des serveurs.

Réviser et mettre à jour régulièrement les configurations :

- Examiner périodiquement la configuration des serveurs par rapport à la norme établie.
- Mettre à jour les configurations en fonction des nouvelles menaces, des vulnérabilités ou de l'évolution des besoins de l'organisation.

Maintenir un programme de gestion des vulnérabilités :

- Rechercher régulièrement les vulnérabilités et remédier aux faiblesses identifiées.
- Inclure les composants logiciels et physiques dans les évaluations de vulnérabilité.
- Établir un processus de vérification des nouvelles vulnérabilités en matière de sécurité et inclure les éléments suivants :
    - Sources reconnues par l'industrie
    - Processus de classement des risques basé sur les meilleures pratiques de l'industrie et identification des vulnérabilités à haut risque.
- Mettre à jour et corriger régulièrement les systèmes d'exploitation et les logiciels afin d'éliminer les vulnérabilités.
- Veiller à appliquer les correctifs de sécurité applicables dans un délai d'un mois à compter de la publication.