Rapport

Audit d’optimisation des ressources – Protection des renseignements personnels

15 novembre 2022

Présenté à :

Raymond Chabot Grant Thornton

VILLE DE DEUX-MONTAGNES

Raymond Chabot
Grant Thornton

Raymond Chabot
Grant Thornton S.E.N.C.R.L.
Bureau 2000
Tour de la Banque Nationale
600, rue De La Gauchetière Ouest
Montréal (Québec)
H3B 4L8

T 514 878-2691

Le 15 novembre 2022

Aux membres du conseil municipal
Ville de Deux-Montagnes
803, chemin d'Oka
Deux-Montagnes (Québec) J7R 1L8

Objet : Rapport – Audit d'optimisation des ressources – Protection des renseignements personnels

Mesdames, Messieurs,

Nous avons le plaisir de vous présenter notre rapport portant sur l'information relative à la protection des renseignements personnels par la Ville de Deux-Montagnes (ci-après la « Ville »).

Ce mandat a été réalisé en vertu des dispositions de la Loi sur les cités et villes, et le présent rapport doit être déposé à la première séance du conseil municipal qui suit sa réception par la direction de la Ville. Celui-ci doit également être publié sur le site Web de la Commission municipale du Québec.

Nous tenons à souligner l'excellente collaboration de toutes les personnes rencontrées au cours de la réalisation du mandat.

Nous vous prions de recevoir, Mesdames, Messieurs, nos salutations les plus distinguées.

Raymond Chabot Grant Thornton S.E.N.C.R.L.[1]

[1] CPA auditeur, permis de comptabilité publique nº A129112

Table des matières

1. Contexte et objectif

1.1. CONTEXTE

La Ville de Deux-Montagnes (ci-après la « Ville ») collecte et traite des renseignements personnels afférents à la vie privée de ses employés et des citoyens. La Ville compte plus de 17 500 citoyens et plus de 200 employés permanents, temporaires et saisonniers. Les informations détenues par la Ville sont nécessaires afin de servir adéquatement les citoyens et consistent en ce qui suit :

- Dossiers d'employés, leurs dossiers médicaux ainsi que leurs coordonnées bancaires;
- Candidatures aux fins de recrutement;
- Informations personnelles des citoyens pour utilisation des services en ligne, comme les demandes de permis et la taxation.

La Ville de Deux-Montagnes étant un organisme municipal, il est donc assujetti à la loi pour le secteur public, soit la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Cette loi s'applique à tous les documents, peu importe leur format : écrit, graphique, sonore, visuel, informatisé ou autre.

Les renseignements personnels sont définis par les renseignements qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

Des exemples de renseignements personnels :

- Nom, prénom, pseudonyme, date de naissance, NAS;
- Photos, enregistrements sonores de voix;
- Numéro de téléphone fixe ou portable, adresse postale, adresse courriel;
- Adresse IP, identifiant de connexion informatique ou identifiant de *cookie*;
- Numéro de plaque d'immatriculation, numéro d'une pièce d'identité, coordonnées bancaires;
- Les données relatives à la santé des individus;
- Les données concernant la vie sexuelle ou l'orientation sexuelle;
- Les données qui révèlent une prétendue origine raciale ou ethnique.

Certaines données sont de nature publique, comme le rôle d'évaluation et de taxation, où on trouve les informations des propriétaires (nom, prénom, adresse), et le rôle d'évaluation du terrain et bâtiment.

Les conséquences d'une mauvaise protection des renseignements personnels, en plus de ne pas être conforme à la loi, peuvent être de permettre la divulgation non autorisée des renseignements personnels, qu'une personne malintentionnée utilise l'information des renseignements personnels aux fins d'usurpation d'identité, d'atteinte à la réputation de la Ville, une perte de confiance des citoyens envers la Ville ainsi que des poursuites judiciaires.

2. Objectif de l’audit et portée des travaux

2.1. OBJECTIF DE L’AUDIT

En vertu des dispositions de la Loi sur les cités et villes, nous avons réalisé une mission d’audit de l’optimisation des ressources portant sur la protection des renseignements personnels.

Cet audit avait pour objectif de s’assurer que les renseignements personnels détenus par la Ville faisaient l’objet d’une protection adéquate afin de mitiger les risques de bris de confidentialité, de vol ou d’accès non autorisé aux renseignements personnels.

Responsabilité de la direction

La direction de la Ville est responsable de la protection des renseignements personnels qu’elle détient. Elle est également responsable de la mise en place des systèmes, des procédures et des contrôles lui permettant d’identifier, de gérer et de protéger les renseignements personnels, et ce, conformément aux règles en vigueur et aux saines pratiques en matière de protection des renseignements personnels.

Responsabilité de l’auditeur

Notre responsabilité consiste à fournir une conclusion sur l’objectif de l’audit. Pour ce faire, nous estimons que nous avons recueilli les éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d’assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés à la section 5.2.

Nous avons planifié et réalisé notre mission d’assurance raisonnable conformément à la norme canadienne de missions de certification (NCMC) 3001, « Missions d’appréciation directe », du *Manuel de CPA Canada – Certification.* Cette norme requiert que nous planifiions et réalisions la mission de façon à obtenir une assurance raisonnable à l’égard de notre conclusion sur l’objectif de l’audit.

L’assurance raisonnable correspond à un niveau élevé d’assurance, qui ne garantit toutefois pas qu’une mission réalisée conformément à cette norme permettra toujours de détecter tout cas important de non-conformité ou les déficiences significatives qui pourraient exister. Les cas de non-conformité ou déficiences significatives aux critères peuvent résulter de fraudes ou d’erreurs et ils sont considérés comme significatifs lorsqu’il est raisonnable de s’attendre à ce que, individuellement ou collectivement, ils puissent influer sur les décisions des utilisateurs de notre rapport. Une mission d’assurance raisonnable visant la délivrance d’un rapport de l’auditeur implique la mise en œuvre de procédures en vue d’obtenir des éléments probants suffisants et appropriés pour fonder raisonnablement une conclusion et obtenir un niveau d’assurance élevé. La nature, le calendrier et l’étendue des procédures d’audit choisies relèvent de notre jugement professionnel, et notamment

de notre évaluation des risques de non-conformité ou de déficiences significatives, que celles-ci résultent de fraudes ou d'erreurs.

Notre indépendance et notre contrôle qualité

Nous nous sommes conformés aux règles ou au code de déontologie pertinents applicables à l'exercice de l'expertise comptable et se rapportant aux missions de certification, qui sont publiés par les différents organismes professionnels comptables, lesquels reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Le cabinet applique la Norme canadienne de contrôle qualité (NCCQ) 1, *Contrôle qualité des cabinets réalisant des missions d'audit ou d'examen d'états financiers et d'autres missions de certification,* et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables.

2.2. PORTÉE DES TRAVAUX

Nos travaux d'audit ont porté sur la période du 7 octobre 2021 au 20 décembre 2021. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en avril 2022.

Nos travaux se sont limités et ont été réalisés sur un échantillon de systèmes contenant des renseignements personnels jugés critiques par la Ville. Les systèmes sélectionnés sont les suivants :

- ACCEO Municipal – système financier, de taxation et de paie/RH (hébergé par la Ville);
- ACCEO Territoire – système utilisé pour la gestion du territoire et des demandes diverses et de paiement de permis en ligne (hébergé par la Ville);
- Loisirs Sport-Plus – système de réservation en ligne pour les citoyens (géré et hébergé par un fournisseur externe);
- Serveur de fichiers et contrôleur de domaine – systèmes gérant les fichiers et les utilisateurs sur le réseau (hébergé par la Ville).

Bien qu'il s'agisse d'un audit, notre mission ne constitue pas en soi un exercice de conformité à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ni aux autres lois et normes auxquelles la Ville pourrait se référer en ce qui concerne les renseignements personnels.

À la fin de nos travaux, un rapport préliminaire comprenant nos constats a été présenté aux instances concernées de la Ville, et ce, aux fins de discussions. Par la suite, le rapport final a été transmis aux mêmes instances pour l'obtention d'un plan d'action et d'un échéancier pour la mise en œuvre des recommandations les concernant.

3. Résultats de l'audit

3.1. GOUVERNANCE

La gouvernance est un élément important pour la Ville, car elle vient établir et officialiser les orientations prises par la direction et le conseil municipal. Elle jette les bases des attentes de la Ville envers ses employés, les consultants ainsi que les fournisseurs avec qui elle collabore. Une bonne gouvernance permet de venir encadrer les principes et les standards souhaités par la Ville et cette notion s'applique à l'ensemble des sphères d'une Ville, incluant le respect des renseignements personnels.

Plus précisément, la gouvernance à l'égard des technologies de l'information (TI) s'entend de la gestion et du contrôle de l'environnement TI, notamment les données utiles à une organisation et à ses parties prenantes. La gouvernance des TI exige un leadership, des structures organisationnelles, des politiques, des processus et des contrôles internes afin que les TI respectent la stratégie et les objectifs de la Ville et de ses parties prenantes. Elle englobe les efforts des employés et les processus qui soutiennent la prise de décisions relatives aux initiatives technologiques. Lorsqu'elle est mise en œuvre avec efficacité, cette gouvernance permet d'atteindre un équilibre entre la création de valeur et l'atténuation des risques pour la Ville.

3.1.1. Politiques

La mise en place de politiques des TI permet de venir encadrer la gouvernance. Celles-ci établissent les attentes et les comportements attendus en matière de sécurité de l'information et de protection des renseignements personnels.

Ces politiques doivent être officiellement autorisées par la direction, revues périodiquement et diffusées à l'ensemble des employés, consultants et fournisseurs.

Dans le cadre de notre audit, nous avons constaté qu'il n'y a aucune politique de sécurité. La Ville a une *Politique d'utilisation des systèmes informatiques* qui a été révisée pour la dernière fois en 2007. Cette politique adresse des éléments tels que la propriété du matériel, l'utilisation du système informatique et des sites Web, les activités prohibées, etc. Cependant, cette politique n'aborde pas la sécurité ainsi que la protection des renseignements personnels. De plus, bien que cette politique soit accessible sur le réseau interne de la Ville, celle-ci n'est pas signée à l'embauche par les nouveaux employés ou consultants.

Recommandations

- Nous recommandons à la Ville de mettre en place une politique à l'égard de la sécurité des TI et de la protection des renseignements personnels et de procéder à une mise à jour (révision) de sa politique d'utilisation des systèmes informatiques. Des procédures devront par la suite être élaborées afin d'opérationnaliser ces politiques. De plus, l'ensemble de ces politiques et procédures devront être revues périodiquement.
- Nous recommandons à la Ville que les politiques soient entérinées par la direction et le conseil municipal et par la suite diffusées à l'ensemble des employés, consultants et fournisseurs. Les nouveaux employés et consultants devront quant à eux en prendre connaissance lors de leur embauche.
- Nous recommandons à la Ville de définir, par l'entremise de la politique à l'égard de la sécurité des TI et de la protection des renseignements personnels, les rôles et responsabilités en matière de protection des renseignements personnels.

3.1.2. Classification et inventaire des renseignements personnels

Les organismes publics se doivent d'établir et de maintenir à jour un inventaire des fichiers contenant des renseignements personnels. Cela est requis par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. L'article 76 de cette loi indique ce que doit contenir l'inventaire :

- La désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier;
- La provenance des renseignements versés à chaque fichier;
- Les catégories de personnes concernées par les renseignements versés à chaque fichier;
- Les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions;
- Les mesures de sécurité prises pour assurer la protection des renseignements personnels.

Une classification et un inventaire des renseignements personnels permettent de mieux maîtriser les actifs informationnels de l'organisation pour ainsi déployer les mesures nécessaires pour la protection de ceux-ci. Cela permet de bien déterminer les objectifs en matière de sécurité de l'information et de protection des renseignements personnels.

Dans le cadre de notre audit, nous avons observé que la Ville s'est dotée d'un plan de classification des documents municipaux, d'un calendrier de conservation et d'une politique relative à la gestion des documents et des archives. Cependant, selon les informations recueillies, le plan de classification n'a pas été mis en application par les différents services de la Ville, à l'exception du Service du greffe. De plus, le plan de classification et le calendrier de conservation ne traitent pas des données électroniques.

Finalement, nous avons constaté qu'il n'y avait pas d'inventaire à jour des renseignements personnels conservés pour les archives papier ni d'inventaire des données électroniques.

Notons qu'une démarche est en cours d'implantation pour changer le logiciel d'archivage. Ce changement permettra d'inclure les données électroniques dans la classification des renseignements personnels et d'uniformiser les façons de faire à l'ensemble des services.

Recommandations

- Nous recommandons à la Ville de bonifier le plan de classification et le calendrier de conservation des documents municipaux afin d'y intégrer les données électroniques ainsi que les renseignements personnels.
- Nous recommandons à la Ville de mettre en place un inventaire des renseignements personnels collectés et conservés, autant sous format papier qu'électronique, et de procéder à la classification de ses données, et ce, afin de se conformer à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Cet inventaire devrait permettre d'identifier les renseignements personnels détenus par la Ville.
- Nous recommandons à la Ville de mettre en place un processus afin d'assurer le maintien et la mise à jour de l'inventaire et de la classification des renseignements, incluant les renseignements personnels.
- Nous recommandons à la Ville de communiquer les politiques et les attentes à la direction des différents services afin qu'ils soient impliqués dans le maintien de l'inventaire et la classification des renseignements, incluant les renseignements personnels.

3.1.3. Programme de sensibilisation

La sensibilisation à la sécurité des TI est indispensable afin de protéger une organisation de personnes malveillantes et de prévenir les cyberattaques potentielles. En effet, les techniques utilisées sont de plus en plus sophistiquées et les employés et consultants sont souvent les premiers visés par ces cyberattaques, et ce, par leur manque de connaissances au sujet de celles-ci.

Ceux-ci ont donc tous un rôle important à jouer à l'égard de la sécurité de l'information. Il est primordial de mettre en place un programme de sensibilisation. Un tel programme permet de transmettre aux utilisateurs les connaissances nécessaires afin de protéger l'organisation et ses renseignements personnels. Un programme de sensibilisation performant contient des formations sur la sécurité des TI et sur la protection des renseignements personnels, des simulations d'hameçonnage et d'autres exercices afin d'informer les utilisateurs des façons pour se prémunir de menaces comme l'hameçonnage, le harponnage, les rançongiciels, l'ingénierie sociale, etc.

Dans le cadre de notre audit, nous avons constaté qu'il n'y a pas eu de campagne de sensibilisation officielle ni de formation sur la sécurité de l'information et des renseignements personnels auprès de l'ensemble des employés de la Ville.

Recommandations

- Nous recommandons à la Ville de mettre en place un programme de sensibilisation officiel à l'égard de la sécurité de l'information et de la protection des renseignements personnels. Le programme devrait être revu annuellement et diffusé auprès de l'ensemble des employés et consultants de la Ville. Un tel programme peut prendre diverses formes telles que des courriels de rappel de sécurité, de la formation continue sur des sujets d'actualité ainsi que des simulations et exercices afin de tester le niveau de connaissances et de conscience en matière de sécurité et de protection des renseignements personnels.
- Nous recommandons à la Ville de mettre en place des mesures afin de suivre les employés et consultants ayant participé ou ayant exécuté les activités reliées au programme de sensibilisation pour s'assurer que tous les employés suivent les formations.

3.2. CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

La Ville doit prendre les mesures de sécurité nécessaires afin d'assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits, tel qu'il est exigé par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels à l'article 63.1.

Une organisation doit s'assurer de définir des règles et procédures à l'égard de la conservation et de la destruction des données, dont les renseignements personnels, et ce, autant en ce qui concerne les données sur support papier que sur support électronique. En effet, la capacité et le désir de conserver d'importantes quantités de renseignements personnels augmentent les risques relatifs à la protection des renseignements personnels. De ce fait, les durées de conservation doivent être clairement établies et tenir compte des exigences réglementaires applicables et de l'objectif initial ayant mené à la collecte de ces données.

En ce qui concerne la destruction de ces données lorsque la durée de conservation a été atteinte, une organisation doit définir les procédures visant à détruire irrémédiablement le support sur lequel sont stockées les données, de sorte qu'il soit impossible de reconstituer celles-ci de quelque façon que ce soit. De plus, ces procédures doivent également tenir compte de la destruction de toutes les copies ainsi que de tous les fichiers de sauvegarde.

Dans le cadre de notre audit, nous avons pris en considération les renseignements personnels conservés ou détruits. Pour conserver et par la suite détruire les renseignements personnels au bon moment, un calendrier de conservation doit être instauré. La Ville a un plan de classification qui contient le recueil des délais de conservation des données. Cependant, le plan de classification ne tient pas compte des données électroniques, puisqu'il n'y a pas de recueil pour les données électroniques ni de délai de conservation défini.

Les archives sur support papier sont quant à elles conservées au Service du greffe, et ce, dans des classeurs anti-feu verrouillés et derrière une porte verrouillée. Cependant, il n'y a pas de processus officiel de gestion des accès physiques. La gestion des clés s'effectue par l'entremise de la directrice générale adjointe et trésorière. Il n'y a pas de liste officielle d'utilisateurs des clés.

De plus, la gestion par clés est plus complexe comparativement à une gestion par des cartes d'accès magnétiques. En effet, l'inventaire des cartes magnétiques, ainsi que les détenteurs de ces cartes, peut être facilement analysé et validé sur une base périodique, et ce, par l'entremise de rapports du système de gestion des cartes d'accès. La gestion par cartes permet également une imputabilité des actions qui n'est pas présente avec les accès par clé.

Concernant la conservation des données électroniques à la Ville, nous avons audité les sauvegardes informatiques. Un outil est utilisé pour sauvegarder les serveurs, dont le serveur de fichiers. Cependant, nous avons noté que les sauvegardes ne sont pas chiffrées bien qu'elles ne soient pas entreposées à l'extérieur du réseau de la Ville. De plus, celles-ci ne sont pas testées périodiquement. Il est recommandé de chiffrer les sauvegardes afin de s'assurer que les données sauvegardées ne sont pas accédées par des personnes non autorisées. Il est aussi recommandé de tester périodiquement les restaures complètes de sauvegarde pour s'assurer qu'elles sont fonctionnelles.

Concernant la destruction des archives, elle se fait par une entreprise spécialisée dans le domaine, qui détruit les archives qui sont arrivées au terme de leur délai de conservation. L'organisme émet un certificat de destruction des informations. De plus, relativement aux données électroniques, il n'y a aucune politique de disposition à l'égard des disques durs qui doivent être disposés ou effacés.

La Ville a également mis en place des boîtes sécurisées pour la destruction des documents confidentiels. Une entreprise est responsable de la destruction des documents qui se retrouvent dans ces boîtes, et ce, mensuellement.

Finalement, pour les données gérées par les tiers, les contrats ne spécifient pas les paramètres quant à la conservation et à la destruction des données.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus officiel afin de gérer les accès aux divers sites d'archives et de restreindre l'accès au personnel approprié uniquement.
- Nous recommandons à la Ville d'inclure, pour les contrats avec les fournisseurs hébergeant des renseignements personnels, des clauses sur les durées de conservation et la destruction des données, et ce, en ligne avec le plan de classification de la Ville.
- Nous recommandons à la Ville de procéder au chiffrement des sauvegardes des données électroniques conservées à l'externe et de s'assurer que la période de rétention des sauvegardes répond aux besoins de la Ville.
- Nous recommandons à la Ville de procéder à des tests de restauration des sauvegardes périodiquement pour s'assurer que les sauvegardes sont fonctionnelles.
- Nous recommandons à la Ville de mettre en place un mécanisme de suivi des délais de conservation des données électroniques afin de s'assurer que le calendrier de destruction des documents est respecté.
- Nous recommandons à la Ville de rédiger et de formaliser le processus de destruction des données électroniques (par exemple, les disques durs ou autres supports électroniques) et de documenter le processus chaque fois que des données sont effacées. Cela implique de documenter le détail des médias détruits, la procédure de destruction et la mise au rebut ainsi que de conserver une confirmation que les données ont été effacées et qu'elles ne sont plus lisibles.

3.3. MESURES DE PROTECTION

Comme indiqué précédemment et selon l'article 63.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, l'organisme public doit prendre les mesures propres à assurer la protection des renseignements personnels. Les mesures de protection sont les procédures et contrôles mis en place par la Ville afin de protéger contre l'accès non autorisé aux renseignements personnels. Nous avons évalué les procédures et contrôles en lien avec les activités suivantes :

- Gestion des accès logiques et physiques;
- Gestion des vulnérabilités;
- Gestion des incidents et de la surveillance;
- Gestion de la relève informatique;
- Gestion des fournisseurs.

3.3.1. Gestion des accès logiques et physiques

Accès logiques

La gestion des accès logiques vise à assurer que les accès aux systèmes contenant des renseignements personnels ou aux renseignements personnels directement sont restreints au personnel approprié en fonction de leurs rôles et responsabilités. La mise en place de contrôles d'accès vise à :

- Gérer et contrôler les accès logiques aux systèmes et aux données;
- Détecter des accès non autorisés;
- Définir les règles en matière d'identification, d'authentification et d'autorisation d'accès.

Nous avons évalué les mesures en place afin de contrôler et restreindre l'accès aux renseignements personnels pour les systèmes inclus dans la portée de nos travaux, soit les systèmes ACCEO Municipal, ACCEO Territoire, Loisirs Sport-Plus ainsi que le serveur de fichiers et le contrôleur de domaine.

Gestion des octrois, modifications et retraits d'accès

La mise en place de mesures de contrôle relatives à l'octroi, à la modification et au retrait d'accès vise à assurer que les accès octroyés à un employé sont officiellement autorisés et restreints en fonction des rôles et responsabilités de celui-ci. De plus, ces mesures visent à assurer que lors du départ d'un employé ou lors d'un changement de fonction, les accès de l'employé sont retirés ou modifiés, et ce, en temps opportun.

Octroi et modification des accès

Nous avons noté que le processus en place dans le cadre de la création ou modification de comptes n'était pas formalisé. Le Service des TI est avisé directement par le gestionnaire pour créer les accès réseau. Les accès pour les applications passent par la directrice générale adjointe et trésorière. Le processus est similaire pour les départs d'un employé, qui se font par courriel ou verbalement.

En ce qui concerne les arrivées, un compte réseau est créé et les accès sont octroyés selon le titre du nouvel employé. Les accès aux applications sont gérés par une ou des personnes du service responsable de l'application (désigné comme responsable des accès à l'application). Par exemple, pour l'application ACCEO Municipal pour les finances, la personne qui gère les accès est la directrice générale adjointe et trésorière. À l'arrivée de l'employé, le Service des TI crée le compte réseau, alors qu'en ce qui concerne les applications, le responsable de chaque application va octroyer les accès en fonction du rôle de l'employé au sein de la Ville. Ce processus n'est pas officiellement documenté. Cependant, pour ACCEO Municipal, il n'y a pas eu d'arrivée de nouveaux employés depuis quelques années, réduisant le risque d'accès non autorisé aux systèmes.

De plus, les responsables des applications peuvent recevoir des demandes d'accès en provenance des directeurs des autres services. Cela est également informel et non documenté, puisque ce sont les responsables des accès qui vont généralement déterminer le type d'accès requis pour la personne.

En ce qui concerne les accès à distance, tous les utilisateurs ont désormais la possibilité d'accéder au réseau de la Ville à distance, en ce, considérant le contexte pandémique et l'augmentation du télétravail. La Ville utilise un VPN qui est lié aux comptes du contrôleur de domaine et, par conséquent, les accès en VPN restent les mêmes que si la personne était physiquement dans les locaux de la Ville.

Retrait des accès

Nous avons noté que le processus en place de retrait des accès n'était pas formalisé. Le Service des TI est informé par la directrice générale adjointe et trésorière du départ d'un employé, et le Service des TI procède au retrait des accès au réseau de l'employé en question. Cependant, le Service des TI ne reçoit pas toujours l'information, donc, dans certaines situations, le Service des TI ne peut pas retirer les droits d'accès en temps opportun. Ce constat est également applicable aux applications, les responsables n'étant pas toujours avisés des départs en temps opportun. Notons que, pour l'application ACCEO Municipal, il n'y a pas eu de départ dans les dernières années, ce qui réduit le risque d'accès non autorisé par d'anciens employés.

Comptes génériques à hauts privilèges

Un compte générique est un compte n'appartenant pas à un utilisateur en particulier et pouvant être utilisé par plusieurs utilisateurs. Un tel compte possède généralement des accès privilégiés et ne permet pas l'imputabilité des actions commises. Dans le contexte des renseignements personnels, il peut aussi y avoir des comptes génériques avec de moindres privilèges, mais possédant des accès en lecture ou écriture aux renseignements personnels, ce qui peut rendre difficile l'imputation des actions en cas de bris de confidentialité avec ces comptes génériques.

Dans le cadre de notre audit, nous avons relevé l'existence d'un compte générique dans l'application AccèsCité Loisirs, celui-ci possédant plusieurs accès et qui n'est pas attribué à une seule personne.

Gestion des rôles des utilisateurs

Une bonne pratique dans la gestion des droits d'accès est d'utiliser des groupes bien définis et d'octroyer aux utilisateurs des groupes spécifiques en fonction de leurs responsabilités. Ce processus de gestion par groupes permet de plus facilement gérer les accès autant lors de l'octroi que de la modification ou de la révision des accès. Les accès sont gérés par groupes pour les applications et pour le réseau. Nous avons cependant constaté que, pour ACCEO Municipal, il y avait neuf utilisateurs qui sont administrateurs de l'application, alors que ce rôle devrait être limité à

un nombre restreint d'utilisateurs. Nous avons également constaté que les droits administrateur pour le réseau ne sont pas réservés qu'au Service des TI, puisque la direction générale possède également ces droits.

Accès aux bases de données

Les accès aux bases de données sont réservés au Service des TI ou aux fournisseurs des applications auditées.

Recommandations

- Nous recommandons à la Ville de formaliser le processus d'octroi d'accès et de modification d'accès pour les applications et les serveurs de fichiers. Le processus doit comprendre une autorisation du propriétaire des données avant d'octroyer un accès. Ce processus doit être documenté et appliqué à toutes les applications aussi bien qu'au niveau du réseau.
- Nous recommandons à la Ville de mettre en place un processus officiel afin d'aviser le Service des TI et les responsables applicatifs afin de retirer les accès en temps opportun lors du départ des employés. Le processus pourrait être automatisé par l'entremise du logiciel ACCEO Municipal.
- Nous recommandons à la Ville d'éviter l'utilisation de comptes génériques afin d'assurer l'imputabilité des actions commises. Dans les situations où l'utilisation de tels comptes est nécessaire, la Ville devra mettre en place des mesures afin d'assurer l'imputabilité des actions, comme l'instauration d'une voûte de mots de passe qui permet de journaliser les accès aux mots de passe et le moment de l'utilisation par un utilisateur.
- Nous recommandons à la Ville, pour l'application ACCEO Municipal et pour le réseau, de limiter les utilisateurs ayant les droits administrateur à un nombre restreint d'utilisateurs autorisés.

Révision périodique des accès

Une révision périodique des accès permet au responsable d'un système de confirmer que seuls les accès autorisés sont actifs, que les accès sont conformes aux rôles et responsabilités des utilisateurs et que les accès aux renseignements personnels sont restreints au personnel approprié.

Nous avons noté qu'il n'y a présentement pas de processus défini à la Ville en ce qui concerne la révision périodique des accès. Il n'y a aucune révision des accès aux applications, incluant la juste séparation des tâches et l'accès aux renseignements personnels, en lecture ou écriture, de leurs bases de données et des serveurs de fichiers et du contrôleur de domaine.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus officiel de révision périodique des accès. Ce processus doit comprendre la revue complète des utilisateurs et de leurs rôles pour s'assurer de la juste séparation des tâches et que l'accès aux renseignements personnels, autant en lecture qu'en écriture, est restreint au personnel approprié. Le processus devrait être appliqué pour l'ensemble des applications, incluant celles avec peu d'utilisateurs, ainsi qu'aux bases de données et au réseau.

Authentification et gestion des mots de passe

L'authentification, soit la combinaison d'un code d'utilisateur et d'un mot de passe, doit être assez robuste afin de limiter les risques d'accès non autorisés. Dans le cadre de nos travaux, nous avons évalué les paramètres de mots de passe des systèmes dans notre portée.

Nous avons relevé que l'ensemble des logiciels, à l'exception de Loisirs Sport-Plus pour les loisirs, sont liés au contrôleur de domaine de la Ville. Nous avons cependant constaté que les paramètres de mots de passe ne respectent pas les bonnes pratiques (longueur et complexité des mots de passe, verrouillage automatique après un nombre de tentatives infructueuses et verrouillage automatique après une période d'inactivité).

Concernant l'application Loisirs Sport-Plus, celle-ci est accessible par les employés de la Ville *via* un accès administrateur ou par les citoyens directement. Bien que les paramètres de mot de passe respectent les bonnes pratiques en ce qui concerne l'authentification des citoyens, il n'y a aucun paramètre exigé par le système pour l'authentification des administrateurs de l'application.

Recommandations

- Nous recommandons à la Ville de revoir ses paramètres de mots de passe au contrôleur de domaine et à l'application Loisirs Sport-Plus afin de répondre aux bonnes pratiques en matière d'authentification. La Ville devrait également envisager la mise en place d'une authentification multifacteur afin de renforcer le processus d'authentification, et ce, en complément de la mise en place de paramètres de mots de passe plus robustes.

Accès physiques

La gestion des accès physiques vise à assurer que les accès aux salles des serveurs hébergeant les systèmes contenant des renseignements personnels sont restreints au personnel approprié en fonction de leurs rôles et responsabilités. Il est à noter que la gestion des accès aux salles d'archives a été abordée à la section 3.2 – Conservation et destruction des renseignements personnels.

En ce qui concerne les salles des serveurs (salles principale et secondaire), l'accès aux salles est protégé par une porte verrouillée à clé et est restreint à seulement 2 personnes.

3.3.2. Gestion des vulnérabilités

La gestion des vulnérabilités est un processus qui vise la découverte proactive de menaces, la surveillance en continu des actifs informationnels d'une organisation ainsi que la mise en place de mesures afin de prévenir et détecter les menaces, incluant celles reliées aux renseignements personnels.

La gestion des vulnérabilités comprend la mise en place de contrôles relatifs à l'évaluation des vulnérabilités de sécurité, la mise à jour des correctifs *(patches)* sur les serveurs et les applications, la mise en place d'antivirus et l'exécution de tests d'intrusion.

Mise à jour des correctifs *(patches)*

Nous avons évalué le processus de mise à jour des serveurs et des applications dans la portée de nos travaux. L'équipe du Service des TI fait les mises à jour des serveurs au besoin seulement. Il n'y a pas de processus officiel de mise à jour. Les postes de travail des employés sont quant à eux mis à jour automatiquement. Lors de notre audit, nous avons constaté que les serveurs n'étaient pas mis à jour automatiquement et que les correctifs de sécurité n'étaient pas tous installés.

Antivirus

Les postes de travail et les serveurs sont tous protégés par un antivirus qui est mis à jour automatiquement. De plus, le Service des TI fait une revue mensuelle des postes de travail et des serveurs pour s'assurer que les mises à jour ont été effectuées sur l'ensemble du parc informatique.

L'administrateur gère les antivirus *via* une console qui contient entre autres un tableau de bord lui permettant de voir rapidement les versions des antivirus déployés sur les serveurs et les postes de travail. Le Service des TI est avisé par courriel ou par téléphone par les utilisateurs lorsqu'une anomalie survient et celui-ci applique les correctifs nécessaires de façon réactive.

Coupe-feu

Nous avons observé l'existence de coupe-feu aux différents points d'entrée du réseau de la Ville qui sont munis d'un IPS *(Intrusion Prevention System).* Les coupe-feu ne sont pas maintenus à jour et les règles ne sont pas révisées périodiquement. Cependant, les serveurs Web sont installés dans une zone séparée du réseau interne. De plus, il n'y a pas de diagramme de réseau permettant de visualiser la façon dont les divers équipements communiquent entre eux. Le diagramme de réseau permettrait à la Ville de documenter son environnement réseau et de faciliter la compréhension de celui-ci par les différents intervenants amenés à intervenir en cas de problème, de changement à l'infrastructure, afin de renforcer la sécurité ou aux fins de conformité.

Tests d'intrusion

Nous avons constaté qu'aucun test d'intrusion n'a été effectué depuis de nombreuses années à la Ville.

Recommandations

- Nous recommandons à la Ville de mettre à jour son infrastructure réseau avec des versions de systèmes d'exploitation supportées par les fournisseurs pour réduire le risque d'attaque sur le réseau.
- Nous recommandons à la Ville de valider périodiquement les règles de coupe-feu pour s'assurer qu'elles sont toujours à jour et utiles et qu'elles protègent adéquatement le réseau.
- Nous recommandons à la Ville de réaliser des tests d'intrusion sur le réseau interne et d'effectuer annuellement des tests d'intrusion par l'entremise d'une firme de sécurité externe. Les vulnérabilités à corriger doivent être suivies et priorisées en fonction de leur criticité.
- Nous recommandons à la Ville de documenter et de maintenir à jour un diagramme de réseau.

3.3.3. Gestion des incidents et de la surveillance

Un processus de gestion des incidents vise à identifier les incidents de sécurité, incluant les incidents afférents aux renseignements personnels, et permet de s'assurer que des mesures de mitigation appropriées sont mises en place afin d'éviter qu'un incident se reproduise.

La gestion des incidents de sécurité se fait par le Service des TI.

Nous avons constaté que la Ville n'a aucun processus formalisé concernant la gestion des incidents. Lorsqu'il y a un problème ou un incident, les employés de la Ville contactent le Service des TI qui journalise les demandes dans un outil de billetterie. Les techniciens TI vont eux-mêmes prioriser les demandes.

De plus, il n'y a pas de processus officiel de détection et d'escalade en cas d'incident de sécurité et de bris de confidentialité de renseignements personnels. Un tel processus permettrait une intervention en temps opportun dans l'éventualité d'un incident de sécurité ou d'un bris de confidentialité de renseignements personnels et une réponse rapide suite à l'identification de l'incident, incluant les étapes critiques à suivre afin de résoudre celui-ci dans les meilleurs délais, le cas échéant.

Finalement, les actions sur l'infrastructure du réseau, les coupe-feu ainsi que le VPN sont journalisées et celles-ci peuvent être consultées en cas d'incident. Cependant, les journaux *(logs)* ne sont pas officiellement analysés et révisés périodiquement par le Service des TI.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus de gestion des incidents de sécurité et bris de confidentialité de renseignements personnels ainsi qu'un processus d'escalade.
- Nous recommandons à la Ville de mettre en place un processus visant à analyser les journaux afin d'identifier et d'intervenir en temps opportun s'il y a des tentatives d'accès ou des incidents de sécurité.

3.3.4. Gestion de la relève informatique

La relève informatique permet de ramener la situation à la normale rapidement en cas d'incident majeur dans les salles de serveurs. La Ville n'a pas élaboré un plan de relève informatique couvrant l'ensemble des applications et des infrastructures.

Recommandations

- Nous recommandons à la Ville d'élaborer un plan de relève TI. Par la suite, la Ville devra établir un calendrier de tests pour couvrir la stratégie de recouvrement du plan de relève, effectuer les tests périodiquement et maintenir son plan de relève TI à jour.

3.3.5. Gestion des fournisseurs

La Ville collabore avec des fournisseurs qui peuvent héberger des renseignements personnels, et ce, collectés pour le bénéfice de la Ville. Dans le cas de Loisirs Sport-Plus, les renseignements personnels se trouvent chez le fournisseur.

Loisirs Sport-Plus

Les renseignements personnels suivants se retrouvent sur l'application :

- Ouverture du compte citoyen : adresse de courriel, nom, prénom, téléphone et sexe sont obligatoires. La date de naissance, le rôle familial, l'adresse complète sont optionnels;
- Mise à jour du profil de chaque membre de la famille : nom, prénom, adresse, code postal, téléphone. Les informations suivantes sont facultatives : numéro d'assurance maladie et NAS;
- De plus, pour les enfants, les renseignements suivants sont facultatifs : allergies, médicaments et troubles de comportement.

Dans les documents d'appels d'offres, la Ville inclut une clause générale sur la confidentialité, mais celle-ci n'adresse pas spécifiquement la gestion et la protection des renseignements personnels par le fournisseur.

Considérant que des renseignements personnels collectés pour la Ville sont hébergés chez un fournisseur et que des données peuvent être accessibles par celui-ci, il est important pour la Ville de mettre en place un processus officiel de gestion des fournisseurs afin de s'assurer que les fournisseurs avec qui la Ville collabore répondent aux standards établis par celle-ci en matière de sécurité et de protection des renseignements personnels. De plus, la Ville doit mettre en place des mesures de surveillance afin d'évaluer la conformité de ces fournisseurs aux standards établis.

Nous avons noté que la Ville n'a pas élaboré de processus officiel de gestion des fournisseurs permettant de s'assurer que les bonnes pratiques de sécurité sont prises en compte dans les contrats.

De plus, la Ville ne procède pas à une évaluation périodique de ses fournisseurs afin d'identifier les fournisseurs les plus à risque, et ce, en fonction des données hébergées ou des services rendus, afin d'évaluer la sécurité par l'entremise d'un questionnaire ou l'obtention d'une attestation externe démontrant leur conformité à un cadre de référence reconnu en matière de sécurité de l'information.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus officiel de gestion des fournisseurs afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement la performance et la conformité de celui-ci aux standards de sécurité établis et attendus. L'évaluation périodique doit être effectuée en fonction du risque associé au fournisseur afin de s'assurer qu'il respecte les clauses contractuelles et les standards établis en matière de sécurité et de protection des renseignements personnels.
- Nous recommandons à la Ville d'intégrer des clauses au contrat de service auprès des fournisseurs relativement aux attentes en matière de sécurité et de protection des renseignements personnels ainsi qu'aux divulgations nécessaires en cas de bris de confidentialité. Voici une liste non exhaustive de clauses à considérer :
    - Accès aux renseignements personnels restreint au personnel autorisé du fournisseur;
    - Confidentialité des renseignements personnels hébergés;
    - Sous-traitants du fournisseur (si applicable) devant se conformer aux mêmes standards de sécurité que le fournisseur selon le contrat;
    - Durée de conservation des renseignements personnels et méthodes de destruction;
    - Etc.

4. Conclusion

La Ville possède plusieurs renseignements personnels autant sur ses employés que sur ses citoyens. La Ville doit donc s'assurer de mettre en place un environnement de contrôle adéquat permettant de maintenir la confidentialité des renseignements personnels et de protéger ceux-ci.

En conclusion, bien que la Ville ait mis en place certaines mesures visant la protection des renseignements personnels, celles-ci pourraient, à notre avis, faire l'objet d'améliorations significatives et d'optimisation des ressources de la Ville.

Gouvernance

La Ville ne s'est pas dotée d'une politique de sécurité des TI ni d'une politique de la protection de l'information qui viennent établir la gouvernance et qui décrivent les lignes directrices de la sécurité des TI et de la protection des renseignements personnels au sein de la Ville. La politique d'utilisation des systèmes informatiques doit être revue. Ces politiques devraient être officiellement approuvées par la direction et par le conseil municipal.

Tel qu'il est requis dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, la Ville se doit d'établir et de maintenir à jour un inventaire de ses fichiers contenant des renseignements personnels. Nos travaux nous ont permis de constater qu'un plan de classification des documents municipaux, un calendrier de conservation et une politique relative à la gestion des documents et des archives sont en place. Cependant, ceux-ci ne sont pas suivis par les différents services.

En date du présent rapport, le registre d'inventaire n'était pas à jour pour les documents sur support papier et il n'y a pas de registre en place pour les données électroniques. De plus, il n'y a pas de classification des fichiers permettant d'identifier les renseignements personnels. La Ville se devra d'établir leur classification et de mettre à jour son registre d'inventaire, et ce, périodiquement.

En ce qui concerne la sensibilisation des employés, il n'y a pas eu de campagne de sensibilisation officielle ou de formation sur la sécurité de l'information et des renseignements personnels auprès de l'ensemble des employés de la Ville. Les employés sont un point névralgique de la sécurité de l'information et ils doivent être sensibilisés et formés afin de détecter les menaces éventuelles.

Conservation et destruction des renseignements personnels

La Ville a un plan de classification des documents municipaux qui contient le recueil des délais de conservation des données. Cependant, nous avons noté que ce plan de classification ne tient pas compte des renseignements personnels et des données sur support électronique.

En ce qui concerne les archives papier, elles sont conservées au Service du greffe dans des classeurs anti-feu derrière une porte verrouillée à clé. Il est donc difficile pour la Ville d'identifier les employés ayant accès à ces salles et ainsi d'assurer une imputabilité des actions.

Concernant les sauvegardes informatiques, celles-ci sont mises sur cassette à l'extérieur de la salle des serveurs principale. Cependant, nous avons noté qu'il n'existe pas de politique de rétention des sauvegardes ni de tests périodiques de restaure. De plus, celles-ci ne sont pas chiffrées, ce qui augmente le risque que des sauvegardes contenant des renseignements personnels soient lues par des personnes non autorisées.

Finalement, en ce qui concerne les données gérées par les tiers, les ententes auprès de ces tiers devraient spécifier les exigences quant à la conservation et à la destruction des données.

Mesures de protection

Nous avons noté dans le cadre de nos travaux que le processus de gestion des accès logiques était généralement informel et non documenté, et ce, tant au niveau de l'octroi des accès aux applications qu'au retrait de ceux-ci à la suite du départ d'un employé. Ce constat augmente le risque que des accès non autorisés soient octroyés, que les accès octroyés ne soient pas en fonction des responsabilités de l'employé ou qu'un employé ne se voie pas retirer ses accès en temps opportun. De plus, nous avons noté l'existence de comptes génériques, ce qui ne permet pas d'assurer l'imputabilité des actions commises, principalement en ce qui concerne les accès aux renseignements personnels. Finalement, il n'y a aucun processus de révision périodique des accès en place, ce qui permettrait au responsable d'un système de confirmer que seuls les accès autorisés sont effectifs, que les accès sont conformes aux rôles et responsabilités des utilisateurs et que les accès aux renseignements personnels sont restreints au personnel approprié.

Il est important de mettre en place des mots de passe robustes pour accéder aux applications qui contiennent des renseignements personnels. Nous avons remarqué que bien que les applications soient synchronisées avec le contrôleur de domaine, celui-ci n'exige pas les paramètres de mot de passe robustes. Cela permettrait de réduire le risque d'usurpation de compte et d'accès non autorisé aux renseignements personnels.

En ce qui concerne la gestion des vulnérabilités, nous avons constaté que le processus de mise à jour des serveurs est manuel. Il se peut que des rustines de sécurité ne soient pas installées en temps opportun et qu'une personne mal intentionnée utilise cette faille. Nous avons noté que les serveurs et postes de travail étaient protégés par un antivirus. De plus, le réseau de la Ville est protégé par des coupe-feu aux différents points d'entrée du réseau de la Ville et ceux-ci sont munis d'un IPS *(Intrusion Prevention System).* Cependant, les coupe-feu ne sont pas mis à jour régulièrement et les règles de ceux-ci ne sont pas révisées périodiquement. Par ailleurs, la Ville n'a pas réalisé de tests d'intrusion dans les dernières années autant pour le périmètre externe qu'interne.

Pour ce qui concerne la gestion des incidents, il n'y a pas de processus officiel de détection et d'escalade en cas d'incident de sécurité et de bris de confidentialité de renseignements personnels. Aussi, la révision des journaux des équipements de sécurité comme les coupe-feu n'est effectuée que lorsqu'il y a un incident. Il n'y a pas de processus permettant de détecter les menaces en temps opportun avant que le risque se matérialise.

Enfin, en ce qui concerne la gestion des fournisseurs, nous avons noté qu'ils peuvent héberger des renseignements personnels, ceux-ci étant collectés pour le bénéfice de la Ville. Il est donc primordial de mettre en place un processus officiel de gestion des fournisseurs afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement la performance et la conformité de celui-ci aux standards de sécurité établis et attendus. De plus, nous avons noté qu'il n'y avait pas systématiquement de clauses au contrat de service auprès des fournisseurs relativement aux attentes en matière de sécurité et de protection des renseignements personnels ainsi qu'aux divulgations nécessaires en cas de bris de confidentialité.

5. Objectif et critères d'audit

5.1. OBJECTIF

S'assurer que les renseignements personnels détenus par la Ville faisaient l'objet d'une protection adéquate afin de mitiger les risques de bris de confidentialité, de vol ou d'accès non autorisés aux renseignements personnels.

5.2. CRITÈRES D'AUDIT

- Gouvernance :
  - La Ville dispose de politiques définissant les exigences quant à la gestion des renseignements personnels, et ce, pour l'ensemble des services de la Ville;
  - La Ville maintient un inventaire des renseignements personnels, permettant à celle-ci d'avoir un portrait global des renseignements à protéger;
  - Les employés de la Ville sont sensibilisés quant aux enjeux et risques liés à la gestion des renseignements personnels afin que ceux-ci respectent les politiques ou mesures visant la sécurité de ces renseignements;
- Conservation et destruction des renseignements personnels :
  - Les renseignements personnels sont conservés selon un calendrier préétabli et lorsque ceux-ci ne sont plus requis, ils sont détruits de manière à ce qu'ils ne puissent plus être reconstitués;
- Mesures de protection à l'égard des renseignements personnels :
  - Les accès sont accordés de manière à ce que les accès aux renseignements personnels soient limités aux personnes autorisées uniquement, de par leurs rôles et responsabilités. De plus, les paramètres de sécurité sont assez robustes pour prévenir des accès non autorisés aux renseignements personnels;
  - La Ville a mis en place des mesures de surveillance afin de prévenir et détecter des attaques ou des vulnérabilités potentielles. De plus, la Ville procède à des tests d'intrusion qui permettent de mesurer les vulnérabilités des systèmes contenant des renseignements personnels face aux cyberattaques;
  - La Ville a mis en place un processus de gestion des incidents lui permettant de réagir en temps opportun en cas d'incident majeur visant des renseignements personnels afin de minimiser les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de résoudre celui-ci;
  - Les renseignements personnels transmis, gérés ou hébergés par des tierces parties (fournisseurs) sont protégés afin de préserver la confidentialité de ceux-ci.

rcgt.com

Raymond Chabot Grant Thornton

Certification | Fiscalité | Conseil