Rapport

Audit d’optimisation des ressources – Protection des renseignements personnels

Le 22 novembre 2023

Présenté à :

Raymond Chabot Grant Thornton

VILLE DE SAINT-GEORGES

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 22 novembre 2023

Aux membres du conseil municipal
Ville de Saint-Georges
11700, boulevard Lacroix
Saint-Georges (Québec) G5Y 1L3

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

Mesdames, Messieurs,

Nous avons le plaisir de vous présenter notre rapport portant sur la protection des renseignements personnels par la Ville de Saint-Georges (ci-après la « Ville »).

Ce mandat a été réalisé en vertu des dispositions de la Loi sur la Commission municipale, 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 objectifs

1.1. CONTEXTE

La Ville de Saint-Georges (ci-après la « Ville ») collecte et traite des renseignements personnels (« RP ») afférents à la vie privée de ses employés et des citoyens. La Ville compte plus de 33 000 citoyens et plus de 400 employés. Les informations détenues par la Ville sont nécessaires afin de servir adéquatement les citoyens et consistent en des :

- dossiers d'employés, leurs dossiers médicaux ainsi que leurs coordonnées bancaires;
- candidatures aux fins de recrutement;
- informations personnelles des citoyens pour l'utilisation des services en ligne, comme les demandes de permis, le paiement de stationnement et la taxation.

La Ville étant un organisme municipal, elle est assujettie à la loi pour le secteur public *:* 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.

De plus, la Ville est également assujettie à la nouvelle Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (ci-après la « loi 25 »), dont certaines dispositions sont entrées en vigueur le 22 septembre 2022 et d'autres dispositions entreront progressivement en vigueur jusqu'en 2024. Les nouvelles obligations relatives à cette loi exigent, entre autres[1] :

- de désigner une personne responsable de la protection des renseignements personnels et de publier son titre et ses coordonnées sur le site Internet de la Ville;
- de tenir un registre de tous les incidents de confidentialité, de prendre rapidement des mesures afin de diminuer le risque qu'un préjudice soit causé aux personnes concernées et d'aviser la Commission d'accès à l'information du Québec pour les incidents présentant un risque sérieux de préjudice;
- de former un comité sur l'accès à l'information et la protection des renseignements personnels;
- de mettre en œuvre des politiques et des pratiques encadrant la gouvernance des renseignements personnels;
- de publier une politique de confidentialité si des renseignements personnels sont recueillis par un moyen technologique;

[1] : Extrait de l'aide-mémoire : Résumé des nouvelles obligations des entreprises – Commission d'accès à l'information du Québec.

- de respecter les nouvelles règles de consentement définies;
- de détruire les renseignements personnels lorsque la finalité de leur collecte est accomplie, ou les anonymiser pour les utiliser à des fins sérieuses et légitimes, sous réserve des conditions et d'un délai de conservation prévus par une loi;
- de respecter les nouvelles règles d'utilisation des renseignements personnels;
- de prévoir, par défaut, les paramètres assurant le plus haut niveau de confidentialité du produit ou du service technologique offert au public;
- etc.

Les renseignements personnels sont définis par les RP, 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 RP :

- 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;
- Données relatives à la santé des individus;
- Données concernant la vie sexuelle ou l'orientation sexuelle;
- Données qui révèlent une prétendue origine raciale ou ethnique.

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

Les conséquences d'une mauvaise protection des RP, en plus de ne pas être conformes à la loi, peuvent être de permettre la divulgation non autorisée des RP, qu'une personne mal intentionnée utilise l'information des RP aux fins d'usurpation d'identité, d'atteinte à la réputation de la Ville ou de 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

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 autorisés aux RP.

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 les objectifs 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 gestion de la 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.

Notre cabinet applique la Norme canadienne de gestion de la qualité (NCGQ) 1, *Gestion de la qualité par les cabinets qui réalisent des audits ou des examens d'états financiers, ou d'autres missions de certification ou de services connexes*. Cette norme exige du cabinet qu'il conçoive, mette en place et fasse fonctionner un système de gestion de la qualité qui comprend des politiques et des procédures 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 21 juillet 2023 au 6 octobre 2023. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en octobre 2023.

Nos travaux se sont limités et ont été réalisés sur un échantillon de quatre (4) systèmes contenant des RP jugés critiques 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, à la loi 25, ni aux autres lois et normes auxquelles la Ville pourrait se référer en ce qui concerne les RP.

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 discussion. 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 formellement autorisées par la direction, revues périodiquement et diffusées à l'ensemble des employés, consultants et fournisseurs.

Dans le cadre de notre audit, nous avons observé l'existence d'un ensemble de politiques et de directives régissant la gestion de la sécurité, la protection des renseignements personnels et la confidentialité, incluant :

- *Directive – Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, reprenant les deux principes de base importants de la loi applicables à la Ville, et désignant la greffière et la greffière adjointe comme responsables de l'application de la loi au sein de la Ville;
- *Politique d'utilisation des renseignements personnels*, publiée sur le site Web de la Ville, décrivant l'engagement de la Ville à mettre en œuvre les mesures pour se conformer aux principes de la loi sur les renseignements personnels suivants : responsabilité; fins de collecte des renseignements; consentement; limitation d'information; limitation d'utilisation; exactitude; sécurité; transparence; accès aux informations personnelles et possibilité de porter plainte pour le non-respect des principes;

- *Politique de confidentialité (Privacy Policy et Gestion des cookies),* publiée sur le site Web de la Ville, stipulant qu'elle n'utilise et ne communique les renseignements que pour les fins auxquelles ils ont été recueillis, en conformité avec la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, et avec le consentement des citoyens;
- *Politique concernant la sécurité des systèmes et l'intégrité des données,* décrivant les mesures concernant la sécurité, l'intégrité et la confidentialité des données pour les usagers et les fournisseurs;
- *Directive – Utilisation des équipements informatiques,* définissant les principes et encadrant l'utilisation des outils informatiques des employés de la Ville;
- *Politique portant sur le télétravail,* établissant et informant les employés des conditions et modalités qui s'appliquent au télétravail.

L'ensemble des politiques ont été approuvées par le conseil municipal et officiellement communiquées aux employés et mises à la disposition des citoyens, lorsque requis. Un mécanisme est également en place, où les employés doivent attester avoir lu, compris et accepté les termes et conditions des politiques de sécurité et d'utilisation des actifs informatiques en vigueur à la Ville.

Cependant, un programme de gouvernance relatif à la gestion des renseignements personnels n'a toujours pas été établi et adopté. Une politique-cadre sur la gouvernance de l'information et la gestion de la confidentialité est en cours d'élaboration par la greffière adjointe.

Recommandation

1. Nous recommandons à la Ville d'élaborer un programme de gouvernance des renseignements personnels sur la base d'une analyse des risques. À cet effet, des mesures de protection et de sécurisation devront être établies, et ce, pour chaque type de données, ainsi que les processus à mettre en œuvre pour assurer une conformité aux lois et règlements applicables.

3.1.2. Comité et responsables des RP

La mise en place d'un comité permet de suivre l'application des politiques et procédures, et de s'assurer que les attentes sont bien gérées. Les comités doivent se rencontrer périodiquement et tenir des minutes des résolutions prises ou des actions à prendre.

Un responsable de la protection des renseignements personnels (RPRP) doit avoir été mandaté formellement par la Ville et les coordonnées de celui-ci doivent être affichées sur le site Web de la Ville afin de se conformer aux exigences de la loi.

Un responsable de l'accès aux documents et de la protection des renseignements personnels, ainsi que son substitut, ont été formellement mandatés en novembre 2020, et les coordonnées de celui-ci sont affichées sur le site Web de la Ville.

De plus, le conseil municipal a adopté une résolution en avril 2022 pour la mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels constitué du directeur du service informatique, de la greffière, de la greffière adjointe, de la directrice générale adjointe et de la directrice des services juridiques et du service des ressources humaines. Depuis sa mise en place, le comité a tenu quatre rencontres, et un ordre du jour et un compte-rendu sont établis.

Cependant, les règles de fonctionnement du comité restent non formellement définies, incluant les rôles et les responsabilités qui lui sont assignées par la Ville.

Recommandation

1. Nous recommandons à la Ville de formaliser les rôles et responsabilités du comité sur l'accès à l'information et la protection des renseignements personnels en place, ainsi que ses règles de fonctionnement (fréquence des rencontres du comité, plan d'action pour assurer la conformité à la réglementation et promouvoir une culture de protection des RP et de l'accès à l'information, un processus de suivi et de remontée des actions à la direction).

3.1.3. Classification et inventaire des renseignements personnels

Les organismes publics se doivent d'établir et de maintenir à jour un inventaire de leurs 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 RP 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 RP.

De plus, les organismes publics doivent instaurer les mécanismes nécessaires permettant de répondre à une demande d'un citoyen ou d'un employé en ce qui concerne les renseignements personnels collectés, traités et conservés, incluant les fins pour lesquelles les données sont conservées, et ce, dans les délais prescrits.

Dans le cadre de notre audit, nous avons noté que la Ville a élaboré un projet d'inventaire des RP qui identifie les RP détenus par chaque service de la Ville, tant sous format électronique que papier. Cependant, l'élaboration de celui-ci est toujours en cours, considérant qu'il ne contient pas les RP de l'ensemble des services de la Ville et que les mesures de sécurité à mettre en œuvre pour la protection des RP, par catégorie, n'ont pas été définies.

En ce qui concerne les demandes des citoyens concernant les RP collectées, traitées ou conservées par la Ville, celles-ci sont adressées à la RPRP qui accuse réception du courriel de demande et mène les investigations en interne afin de donner une réponse au citoyen ayant fait la demande. Cependant, il n'y a pas de processus formel en place décrivant les délais de prise en charge, ainsi que le cadre de suivi et les responsabilités relatives à ces demandes. Un projet d'avis précisant les délais de réponse, conformément aux articles 137 et 135 de la Loi, est en cours d'élaboration.

Recommandations

1. Nous recommandons à la Ville de compléter son inventaire des actifs informationnels et des RP, et ce, pour l'ensemble des services de la Ville, incluant autant les données électroniques que les documents papier. Cet inventaire doit être maintenu à jour, et ce, conformément aux lois en vigueur.
2. Nous recommandons à la Ville de communiquer l'inventaire des actifs informationnels et les attentes auprès de la direction des différents services afin qu'elle soit impliquée dans le maintien de l'inventaire et la classification des renseignements, incluant les RP.
3. Nous recommandons à la Ville de finaliser l'avis en veillant à y décliner les mécanismes visant à permettre aux citoyens et aux employés de faire des demandes concernant les RP collectés, traités et conservés et que la Ville puisse répondre à ces demandes dans les délais prescrits.

3.1.4. Programme de sensibilisation

La sensibilisation à la sécurité des TI est indispensable afin de protéger une organisation de personnes malveillantes et afin de prévenir les cyberattaques potentielles. En effet, les techniques utilisées sont de plus en plus sophistiquées et les employés, consultants et fournisseurs sont souvent les premiers visés par ces cyberattaques, et ce, du fait de 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 RP. Un programme de sensibilisation performant contient des formations sur la sécurité des TI et sur la protection des RP, 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 noté que la Ville n'a pas mis en place un programme de sensibilisation et/ou un plan de formation relatif à la sécurité, à la cybersécurité et/ou à la protection des renseignements personnels. Il y a présentement un projet en cours visant l'acquisition d'une plateforme qui permettrait à la Ville d'établir un programme de sensibilisation et de le diffuser à l'ensemble des employés.

Recommandation

1. Nous recommandons à la Ville de mettre en place un programme de sensibilisation formel à l'égard de la sécurité de l'information et de la protection des RP. 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 RP.

3.2. CONSERVATION ET DESTRUCTION DES RP

La Ville doit prendre les mesures de sécurité nécessaires afin d'assurer la protection des RP collectés, utilisés, communiqués, conservés ou détruits, comme l'exige 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 RP, et ce, autant en ce qui concerne les données sur support papier et support électronique. En effet, la capacité et le désir de conserver d'importantes quantités de renseignements personnels augmentent les risques relatifs à la protection de ceux-ci. 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 des 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 ces 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 documents papier et les données électroniques collectés et conservés, ceux-ci devant être détruits selon les délais établis. Pour ce faire, un calendrier de conservation doit être instauré et suivi.

À cet effet, la Ville a établi un calendrier de conservation approuvé par la BAnQ (Bibliothèque et Archives nationales du Québec) en juin 2023, précisant les règles de conservation des données, les délais de conservation pour chaque type de documents, les mesures en cas de conservation et les dispositions en cas de non-utilisation. De plus, un processus de sauvegardes régulières des données électroniques de l'ensemble des systèmes de la Ville, suivant leur criticité, est en place. Celui-ci s'exécute de façon automatique avec un protocole de chiffrement des données lors de leur transfert vers les serveurs, garantissant authenticité et confidentialité dans la communication. De plus, les copies de données sont dupliquées dans un second site, distant du site principal. Un dispositif est en place pour assurer le suivi de l'exécution des sauvegardes et alerter le service informatique de la Ville pour une prise en charge des incidents éventuels.

Les documents physiques collectés sont quant à eux conservés dans un local dédié aux archives.

Les accès à la salle des archives sont limités aux employés du service du secrétariat général et greffe alors que les accès aux salles des serveurs informatiques sont limités au service de l'informatique. De plus, les armoires d'archives et les armoires contenant les serveurs sont verrouillées à clé.

Par ailleurs, la Ville a instauré un logiciel de gestion intégré des documents (format papier) qui permet de générer des listes de documents à détruire selon les délais définis dans le calendrier de conservation en place. Cependant, à terme du délai de conservation, il n'y a pas de processus formel pour la destruction sécurisée des documents et la destruction des actifs informatiques contenant des RP.

Recommandations

1. Nous recommandons à la Ville de définir des mécanismes de contrôle permettant de garantir que les RP sous format électronique sont conservés uniquement pour la durée appropriée et conformément aux exigences légales.
2. Nous recommandons à la Ville de rédiger et de formaliser le processus de destruction des documents papier et 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 documents ou 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 RP. Les mesures de protection sont les procédures et contrôles mis en place par la Ville afin de protéger l'accès non autorisé aux RP. 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 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 RP ou aux RP directement sont restreints au personnel approprié en fonction de ses 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 de restreindre l'accès aux RP pour les systèmes inclus dans la portée de nos travaux.

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 formellement 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

Dans le cadre de nos travaux, nous avons noté qu'un processus de gestion des accès est mis en œuvre et adossé à un outil de billetterie. Les niveaux d'accès à octroyer par les responsables des systèmes sont déterminés par les gestionnaires, conformément aux besoins opérationnels.

Des profils d'usagers et de groupe sont utilisés pour contrôler l'accès aux données et à l'information des systèmes inclus dans la portée de nos travaux.

Les droits d'accès permettant de gérer les profils d'accès et les menus pour deux (2) des systèmes inclus dans la portée de nos travaux sont restreints aux employés du service informatique. Cependant, pour les deux autres systèmes, nous avons noté que certains des employés des services, en plus du service informatique, pouvaient gérer et octroyer les accès.

Retrait des accès

Nous avons noté que le processus de retrait des accès n'était pas formalisé, établissant les rôles et responsabilités en cas de départ afin que les droits d'accès des employés ayant quitté soient retirés en temps opportun. En effet, les ressources humaines n'avisent pas systématiquement le service informatique ou un autre service responsable de la gestion des accès suite au départ d'un employé ou d'un changement d'emploi nécessitant le retrait des accès.

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 comporte généralement des accès privilégiés et ne permet pas l'imputabilité des actions commises. Dans le contexte des RP, il peut aussi y avoir des comptes génériques avec de moindres privilèges, mais possédant des accès en lecture ou écritures aux RP. Cela peut rendre difficile l'imputation des actions ou des accès aux RP en cas de bris de confidentialité avec l'utilisation de ces comptes génériques.

Dans le cadre de notre audit, nous avons relevé que les comptes à hauts privilèges des systèmes dans l'étendue de nos travaux sont restreints à des membres du service informatique et sont nominatifs. De plus, l'administration des mises à jour des logiciels reste sous la responsabilité des fournisseurs. Certains comptes génériques existent, mais ceux-ci correspondent à des comptes de services et ne disposent pas d'accès privilégiés aux différents systèmes.

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 groupe permet de mieux gérer les accès, autant lors de l'octroi que lors d'une modification ou d'une révision des accès. Dans le cadre de notre audit, nous avons observé que les accès sont gérés par groupe pour les applications évaluées et pour le contrôleur de domaine.

Accès aux bases de données

Les accès aux bases de données sont réservés aux fournisseurs pour toutes les applications évaluées.

Recommandations

1. Nous recommandons à la Ville de restreindre au service des TI la capacité de gérer les accès aux applications, et ce, afin d'assurer une séparation adéquate des tâches.
2. Nous recommandons à la Ville de mettre en place un processus formel afin d'aviser le service des TI ainsi que les responsables applicatifs pour assurer le retrait des accès en temps opportun lors du départ des employés, tant sur le réseau que sur les applications.

Révision périodique des accès

Une révision périodique des accès permet 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 RP sont restreints au personnel approprié.

Lors de notre audit, 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 RP, en lecture ou en écriture, de leurs bases de données, des systèmes de fichiers et du contrôleur de domaine.

Cependant, un rapport est généré automatiquement au service informatique pour les comptes non connectés depuis 30 jours sur les systèmes. Sur cette base, nous avons noté que les TI désactivent les comptes sur les systèmes qu'ils gèrent et contactent le service responsable pour aviser de désactiver les comptes des applications non gérées. Ce processus reste informel.

Recommandation

1. Nous recommandons à la Ville de mettre en place un processus formel 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 RP, autant en lecture qu'en écriture, est restreint au personnel approprié. Le processus devrait être appliqué pour l'ensemble des applications ainsi qu'aux accès aux serveurs de fichiers contenant des RP.

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. À cet effet, nous avons noté que les paramètres de mots de passe pour certaines applications dans l'étendue de nos travaux n'étaient pas conformes aux bonnes pratiques.

Recommandations

1. Nous recommandons à la Ville d'établir une politique de mots de passe alignée aux bonnes pratiques en matière d'authentification, et de veiller à l'implémentation de celle-ci.

Accès physiques

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

En ce qui concerne les salles hébergeant les serveurs de données, nous avons noté que toutes les salles sont verrouillées avec un code pour y accéder, connu uniquement des employés du service informatique. Les serveurs de données sont dans des cabinets de serveurs verrouillés dont uniquement les employés du service informatique ont les clés. Cependant, il n'y a pas de processus visant à modifier, périodiquement ou suite au départ d'un membre du service informatique, les codes d'accès aux salles des serveurs.

Recommandation

1. Nous recommandons à la Ville de mettre en place un processus visant à modifier, périodiquement ou à la suite du départ d'un membre du service informatique, les codes d'accès aux salles des serveurs. De plus, la Ville pourrait envisager la mise en place d'un système (p. ex., lecteurs de cartes) permettant d'identifier les utilisateurs accédant aux locaux critiques de la Ville.

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 de détecter les menaces, incluant celles reliées aux RP.

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

Mise à jour des rustines (*patches*)

Une stratégie est mise en œuvre pour assurer la surveillance des mises à jour de sécurité sur les serveurs. Leur déploiement est alors lancé après une analyse de façon centralisée et séquencée sur l'ensemble des serveurs de la Ville.

Finalement, la Ville a mis en place différents outils afin de prévenir, de détecter et de suivre les vulnérabilités potentielles sur les actifs au travers d'un tableau de bord.

Antivirus

Les postes de travail et les serveurs de la Ville sont tous protégés par un antivirus qui se met à jour automatiquement. L'administrateur gère les mises à jour de façon centralisée via une console. Cette console contient, entre autres, un tableau de bord lui permettant d'identifier rapidement les versions des antivirus déployés sur chaque équipement, ainsi que les alertes pour les postes qui ne sont pas à jour.

Cet outil assure également une surveillance en temps réel des comportements anormaux et alerte le service informatique pour la prise en charge, le cas échéant.

Coupe-feu

Nous avons observé le diagramme réseau de la Ville qui permet de visualiser la façon dont le réseau est segmenté et les équipements de protection implémentés.

Le réseau interne de la Ville est divisé en sous-réseaux logiques : postes de travail, centre de données et zones de serveurs et d'applications. Les coupe-feux sont configurés à l'entrée des points d'accès externes de la Ville pour assurer le trafic sécurisé entre le réseau interne de la Ville et les réseaux externes. Les pare-feu sont maintenus à jour et les règles sont révisées lors des activités de maintenance. Nous avons observé sur la console de sécurité que les paramètres IPS (*Intrusion Prevention System*) sont activés et offrent les traces des journaux sur la console de gestion.

Cependant, nous avons noté qu'il n'y a pas de processus de révision du diagramme réseau de la Ville visant à s'assurer que l'environnement TI est à jour, adéquatement segmenté et protégé.

Tests d'intrusion

Les tests d'intrusion permettent à la Ville de valider si ses réseaux comportent des failles de sécurité qu'une personne malintentionnée pourrait utiliser. Les vulnérabilités soulevées lors de tels tests doivent être suivies et corrigées en fonction de leur importance. Il est à noter que la Ville n'a pas réalisé de tels tests d'intrusion et qu'il n'y a pas de processus visant une évaluation périodique de la sécurité des périmètres interne et externe de la Ville par un tiers externe.

Recommandations

1. Nous recommandons à la Ville de mettre en place un processus de révision du diagramme réseau de la Ville visant à s'assurer que l'environnement TI est à jour, adéquatement segmenté et protégé.
2. Nous recommandons à la Ville de réaliser des tests d'intrusion sur une base périodique, et ce, autant sur les périmètres externe et interne de la Ville.

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 RP, et permet de s'assurer que des mesures de mitigation appropriées sont mises en place afin d'éviter qu'un incident se reproduise.

Nous avons noté la mise en place d'un outil pour le signalement des incidents de la Ville. En effet, l'outil de billetterie en place permet une gestion des incidents suivant leur catégorie et leur niveau de priorité. L'outil permet le suivi et l'historique des mesures déployées pour la résolution.

Par ailleurs, différents outils sont en place et permettent de détecter rapidement si des incidents de sécurité, une intrusion ou des actions malveillantes surviennent sur le réseau. Ainsi, ces outils envoient des alertes au service informatique et gardent une trace des journaux (*logs*) de vulnérabilité auxquelles l'infrastructure du réseau a été confrontée.

Cependant, il n'y a pas de processus de gestion des incidents de sécurité et de RP en place, incluant un processus d'escalade. De plus, aucune mesure n'est en place pour s'assurer de la gestion optimale des incidents de sécurité et de confidentialité portant atteinte à la confidentialité des RP de citoyens et d'employés au sein de la Ville. Nous avons noté qu'un plan de réponse en cas d'incidents de confidentialité est en cours d'élaboration par le service du secrétariat général et greffe.

Par ailleurs, nous avons noté que la Ville ne dispose pas d'un plan de relève TI formellement documenté, afin d'assurer la disponibilité et la restauration des systèmes dans des conditions sécurisées en cas d'incidents.

Un plan de relève TI documenté permet d'être en mesure de réagir rapidement en cas d'incident majeur ou de désastre, et de définir les applications critiques à relever en premier.

Recommandations

1. Nous recommandons à la Ville d'élaborer un processus de gestion des incidents portant atteinte à la confidentialité des RP, incluant notamment le rôle du RPRP, le processus de remontée des incidents, l'identification des incidents, la méthodologie afin d'évaluer les incidents, le délai de notification à la Commission d'accès à l'information (72 heures), le processus d'escalade, etc.
2. Nous recommandons à la Ville d'élaborer un plan de relève TI qui va comprendre la liste des actifs critiques, leur temps d'interruption maximum (RTO) et la perte maximale de données (RPO), les principaux acteurs, les étapes de relève, etc.

   La définition des indicateurs RTO et RPO devra résulter d'une analyse d'impacts sur les affaires réalisée de connivence avec les autres services de la Ville.

3.3.4. Gestion des fournisseurs

La Ville collabore avec des fournisseurs qui hébergent des données contenant des RP et/ou gèrent des serveurs contenant des RP.

Considérant que ces RP collectés pour ou par la Ville peuvent être accessibles par certains fournisseurs, il est important pour la Ville de mettre en place un processus formel de gestion des fournisseurs afin de s'assurer que les fournisseurs avec qui la Ville collabore répondent aux standards établis en matière de sécurité et de protection des RP. 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 mis en place un processus formel de gestion des fournisseurs permettant de s'assurer que les bonnes pratiques de sécurité sont prises en compte dans les contrats.

Aussi, la Ville ne procède pas à une évaluation périodique de ses fournisseurs afin d'identifier les fournisseurs les plus à risque selon les RP hébergés et 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.

La Ville a élaboré une entente de confidentialité, celle-ci étant définie en Annexe de sa *Politique concernant la sécurité des systèmes et l'intégrité des données*. Cependant, nous avons noté qu'elle n'est pas systématiquement mise en œuvre avec l'ensemble des fournisseurs visés.

Finalement, en ce qui concerne les données hébergées/gérées par les fournisseurs, les ententes auprès de ceux-ci devraient spécifier les exigences quant à la conservation et à la destruction des données.

Recommandations

1. Nous recommandons à la Ville de mettre en place un processus formel de gestion des fournisseurs critiques 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 RP.
2. Nous recommandons à la Ville d'intégrer des clauses au contrat de service auprès des nouveaux fournisseurs critiques relativement aux attentes en matière de sécurité et de protection des RP ainsi qu'aux divulgations nécessaires en cas de violation de confidentialité. Voici une liste non exhaustive de clauses à considérer :
    - Accès aux RP restreint au personnel autorisé du fournisseur;
    - Confidentialité des RP 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 RP et méthodes de destruction;
    - Etc.
3. Nous recommandons à la Ville de veiller à systématiquement établir les ententes de confidentialité pour tous ses fournisseurs ayant accès à des données confidentielles, incluant les RP collectés par la Ville.

4. Conclusion

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

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

Gouvernance

Critère – La Ville dispose de politiques définissant les exigences quant à la gestion des RP, et ce, pour l'ensemble des services de la Ville.

Nous pouvons conclure que la Ville a élaboré différentes politiques ou directives définissant les exigences en matière de sécurité TI et de gestion des RP. Cependant, un programme de gouvernance relatif à la gestion des renseignements personnels n'a toujours pas été établi et adopté, celui-ci étant en cours d'élaboration.

De plus, la Ville a adopté la mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels et nommé un responsable de l'accès et de la protection des renseignements personnels, également responsable de l'accès aux documents, et ce, comme exigé par la loi 25. Les règles de fonctionnement du comité seront cependant à définir.

Critère – La Ville maintient un inventaire des RP, permettant à celle-ci d'avoir un portrait global des renseignements à protéger.

Nous pouvons conclure que la Ville est à mettre en place son inventaire des RP, qui identifie les RP détenus par chaque service de la Ville, tant sous format électronique que papier. Cependant, l'élaboration de celui-ci est toujours en cours et la Ville n'a pas défini les mesures de sécurité à mettre en œuvre pour la protection des RP.

Critère – Les employés de la Ville sont sensibilisés quant aux enjeux et risques liés à la gestion des RP afin que ceux-ci respectent les politiques ou mesures visant la sécurité de ces renseignements.

Nous pouvons conclure que la Ville n'a pas mis en place un programme de sensibilisation et/ou un plan de formation relatif à la sécurité, à la cybersécurité et/ou à la protection des renseignements personnels. Cependant, il y a un projet en cours visant l'acquisition d'une plateforme qui permettrait d'établir un programme de sensibilisation et de le diffuser à l'ensemble des employés.

Conservation et destruction des RP

Les RP 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.

Nous pouvons conclure que les RP sont conservés selon un calendrier de conservation, et ce, autant pour les documents papier et les données électroniques collectés et conservés. Le calendrier détaille les règles de conservation des données, les délais de conservation pour chaque type de documents, les mesures en cas de conservation et les dispositions en cas de non-utilisation. Un cadre de sécurisation des RP collectées par la Ville est également mis en œuvre.

De plus, les accès physiques aux salles des archives et aux salles des serveurs informatiques sont limités au personnel approprié.

Finalement, la Ville a instauré un logiciel de gestion intégré des documents afin de gérer la conservation des documents selon les délais définis au calendrier de conservation. Cependant, il n'y a pas de processus formel pour la destruction sécurisée des documents et la destruction des actifs informatiques contenant des RP une fois les délais de conservation atteints.

Mesures de protection

Critère – Les accès sont accordés de manière à ce que les accès aux RP soient limités aux personnes autorisées uniquement, par leurs rôles et responsabilités. De plus, les paramètres de sécurité sont assez robustes pour prévenir des accès non autorisés aux RP.

Nous pouvons conclure que, bien que certains mécanismes soient en place afin d'assurer que les accès soient accordés aux personnes autorisées uniquement et que certains paramètres de sécurité permettent de prévenir des accès non autorisés aux RP, ces mécanismes pourraient être améliorés :

- Restreindre au service des TI la capacité de gérer les accès aux applications;
- Mise en place d'un processus formel afin d'aviser le service des TI et les responsables applicatifs lors du départ d'un employé, et ce, pour assurer le retrait des accès en temps opportun;
- Mise en place d'un processus formel de révision périodique des accès, incluant une revue complète des utilisateurs et de leurs rôles pour s'assurer de la juste séparation des tâches et que l'accès aux RP, autant en lecture qu'en écriture, est restreint au personnel approprié;
- Renforcer les paramètres d'authentification.

Critère – La Ville a mis en place des mesures de surveillance afin de prévenir et de 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 RP face aux cyberattaques.

Nous pouvons conclure que les mesures de surveillance en place sont suffisantes afin de prévenir et de détecter des attaques ou des vulnérabilités potentielles. Cependant, la Ville ne procède pas, sur une base périodique, à des tests d'intrusion lui permettant de mesurer les vulnérabilités des systèmes contenant des RP face aux cyberattaques.

Critère – 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 RP afin de minimiser les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de résoudre celui-ci.

Nous pouvons conclure que la Ville n'a pas mis en place de processus formel décrivant le cadre pour la détection et les niveaux d'escalade en cas d'incident de sécurité et de bris de RP. Cependant, les incidents signalés sont journalisés, analysés et réglés, et ce, selon la catégorie et le niveau de priorité de l'incident, ce qui permet le suivi et l'historique des mesures déployées pour la résolution.

Finalement, la Ville ne dispose pas d'un plan de relève TI formellement documenté.

Critère – Les RP transmis, gérés ou hébergés par de tierces parties (fournisseurs) sont protégés afin de préserver la confidentialité de celles-ci.

Nous pouvons conclure qu'en ce qui concerne la gestion des fournisseurs, ceux-ci pouvant accéder à des RP collectés au bénéfice de la Ville, aucun processus formel n'est en place pour la gestion de ceux-ci 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, il n'y a pas systématiquement de clauses au contrat de service auprès de ces fournisseurs en ce qui concerne les attentes en matière de sécurité et de protection des RP, ainsi qu'aux divulgations nécessaires en cas de violation 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 violation de confidentialité, de vol ou d'accès non autorisés aux RP.

5.2. CRITÈRES D'AUDIT

- Gouvernance :
  - La Ville dispose de politiques définissant les exigences quant à la gestion des RP, et ce, pour l'ensemble des services de la Ville;
  - La Ville maintient un inventaire des RP, 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 RP afin que ceux-ci respectent les politiques ou mesures visant la sécurité de ces renseignements;
- Conservation et destruction des RP :
  - Les RP 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 RP :
  - Les accès sont accordés de manière à ce que les accès aux RP 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 RP;
  - La Ville a mis en place des mesures de surveillance afin de prévenir et de 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 RP 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 RP afin de minimiser les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de résoudre celui-ci;
  - Les RP transmis, gérés ou hébergés par de tierces parties (fournisseurs) sont protégés afin de préserver la confidentialité de ceux-ci.

rcgt.com

Raymond Chabot Grant Thornton

Certification | Fiscalité | Conseil