Rapport

Audit d’optimisation des ressources – Protection des renseignements personnels

22 décembre 2023

Présenté à :

Raymond Chabot Grant Thornton

BEACONSFIELD

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 décembre 2023

Aux membres du conseil municipal
Ville de Beaconsfield
303, boulevard Beaconsfield
Beaconsfield, Québec H9W 4A7

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 Beaconsfield (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
2. Objectif de l’audit et portée des travaux 3
3. Résultats de l’audit 5
4. Conclusion 18
5. Objectif et critères d’audit 21

1. Contexte et objectifs

1.1. CONTEXTE

La Ville de Beaconsfield (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 19 000 citoyens et plus de 75 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 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 « loi 25 »), dont certaines dispositions sont entrées en vigueur le 22 septembre 2022 et d'autres dispositions enteront 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 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;
- 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 l'on retrouve les informations des propriétaires, soit nom, prénom, 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 conforme 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, 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-conformités 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 5 juin 2023 au 29 septembre 2023. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en décembre 2023.

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

- Unicité – système de gestion Finance, Paie et Ressources Humaines du fournisseur PG Solutions (hébergé par la Ville) ;
- Ludik – système des loisirs du fournisseur PG Solutions (hébergé par la Ville) ;
- Bciti – portail citoyen pour les services de la Ville en mode (« SAAS ») (géré et hébergé par le fournisseur externe Bciti) ;
- Horizon – système d'inscription à la bibliothèque en mode (« SAAS ») (géré et hébergé par le fournisseur externe SirsiDynix) ;
- Serveur de fichiers et contrôleur de domaine – système 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, 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 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 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’une *directive FIN-001 pour l'utilisation des actifs technologiques*, entrée en vigueur le 20 mai 2021. Elle définit un cadre normatif régissant l’utilisation des actifs technologiques pour tout le personnel de la Ville de Beaconsfield et à tout autre usager autorisé à utiliser des actifs technologiques. Nous avons constaté qu'elle décrit :

- Les principes d'utilisation autorisée des actifs;
- Les mesures de sécurité et d'intégrité des actifs technologiques;
- Les mesures de contrôle de l’utilisation des actifs technologiques (poste de travail, portable et Internet) par les représentants autorisés de la section TI;
- Les règles d'utilisation de matériel personnel (BYOD, acquisition de matériel ou logiciels protection de la vie privée ; utilisation des médias sociaux en tant qu’employé de la Ville);
- Les cas d'utilisation illégale et mesures disciplinaires en conséquence.

Par ailleurs, nous avons observé le *Guide de l'usager des TI* datant du 20 mai 2021 et que celui-ci renforce la directive FIN-001 pour l'utilisation des actifs technologiques en précisant les règles de sécurité à appliquer pour l'accès aux actifs informationnels de la Ville, tant sur le réseau, la messagerie, la manipulation des fichiers, l'accès à internet, l'accès à distance, la téléphonie et les périphériques informatiques (imprimantes, projecteurs, etc.). De plus, les règles d'acquisition, de maintenance et d'appels de service, de même que l'utilisation des médias sociaux en tant qu'employé de la Ville sont établis.

Nous avons noté que ces deux documents ont été présentés à tous les utilisateurs internes qui ont alors signé l'accusé de réception en mai 2021. De plus, les ressources humaines veillent à présenter ces deux documents aux nouveaux employés, qui en accusent réception.

De plus, spécifiquement en ce qui concerne les RP, la Ville a élaboré une politique de confidentialité et une *Politique-Cadre sur la Gouvernance des Renseignements Personnels*, tous deux entrées en vigueur le 22 septembre 2023 et disponible sur le site Web de la Ville. La politique de confidentialité décrit la manière dont la Ville recueille, utilise et communique les renseignements personnels, ainsi que la manière pour un citoyen de demander accès à ses renseignements ou les faire rectifier, si requis.

La Politique-Cadre sur la Gouvernance des Renseignements Personnels établit les principes pour :

- La gouvernance à l'égard des RP tout au long de leur Cycle de vie et de l'exercice des droits des Personnes concernées;
- Le processus de traitement des plaintes;
- Les rôles et responsabilités en matière de protection des RP;
- La stratégie de formation et de sensibilisation du personnel accédant aux RP des usagers.

Considérant que cette politique ait été récemment adoptée, les différents principes établis sont toujours à mettre en œuvre.

Finalement, une directive administrative des ressources humaines N°RH-1008 indique qu'aucun employé n'est autorisé à divulguer noms, adresses, numéros de téléphone ou autres informations nominatives sur qui que ce soit (citoyens ou employés).

Recommandations

- Nous recommandons à la Ville de veiller à la stricte mise en œuvre des principes énumérés dans la *Politique-Cadre sur la Gouvernance des Renseignements Personnels*.

3.1.2. Comités et Responsables des RP

La mise en place de comités 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.

Nous avons observé l'extrait du procès-verbal de la séance ordinaire du conseil municipal de la Ville du 22 août 2022 où a été adoptée la mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels. Ce comité est composé de la greffière et directrice du greffe et affaires publiques, de la greffière adjointe responsable de la gestion documentaire, du chef de section TI et responsable de la sécurité de l'information, de la directrice des ressources humaines, ainsi que du chef de section services au public.

De plus, la greffière et directrice du greffe et affaires publiques a été formellement nommée à titre de responsable de l'accès et protection des renseignements personnels et celle-ci agit également à titre de responsables de l'accès aux documents, ses coordonnées étant indiquées sur le site web de la Ville, tel qu'exigé par la loi 25.

La *Politique-cadre sur la gouvernance des Renseignements Personnels* vient établir les rôles et les responsabilités qui lui sont assignées par la Ville. De plus, le comité sur l'accès à l'information et la protection des renseignements personnels a tenu diverses rencontres depuis sa création.

Recommandation

- Nous recommandons à la Ville de formaliser 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 et un processus de suivi et de reddition de comptes 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 lesquels les données sont conservées, et ce, dans les délais prescrits.

Dans le cadre de notre audit, nous avons noté que la Ville n'a pas mis en place un inventaire des actifs informationnels et des renseignements personnels ni des documents conservés et des RP qu'ils contiennent. Le logiciel de gestion de documents et d'archives CIGIR est en place mais il n'est pas utilisé pour le suivi de la conservation des documents conformément aux délais appropriés. Par ailleurs, nous avons également noté que la Ville n'a pas mis en place les mécanismes permettant de répondre à une demande d'un citoyen ou d'un employé.

En ce qui concerne l'inventaire des actifs informatiques, une liste a été développée en 2018, celle-ci recensant tous les équipements (actifs) en place, et cette liste est maintenue à jour en fonction des changements d'équipements. Cependant, cet inventaire ne tient pas compte des informations collectées et stockées par la Ville à travers les différents canaux (bases de données, courriels, applications /logiciels, sites web, etc.).

Recommandations

- Nous recommandons à la Ville de procéder à l'élaboration d'un inventaire des actifs informationnels et des RP ainsi que des documents conservés contenant des RP autant pour le volet papier que les données électroniques. Cet inventaire doit être maintenu à jour, et ce, conformément aux lois en vigueur.
- Nous recommandons à la Ville de communiquer l'inventaire des actifs informationnelles et les attentes auprès de la direction des différents services afin qu'elles soient impliquées dans le maintien de l'inventaire et la classification des renseignements, incluant les RP.
- Nous recommandons à la Ville de mettre en place les mécanismes nécessaires 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 dans les délais prescrits à ces demandes.

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 connaissance 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 la mise en place d'un programme de formation sur la cybersécurité par l'entremise d'une plateforme de formation en cybersécurité, déployée à la Ville depuis décembre 2021 et qui permet de dispenser des campagnes de sensibilisation et des formations sur la sécurité de l'information et la cybersécurité à l'ensemble des employés, et à faire le suivi de celles-ci.

La Ville a dispensé différentes formations en 2022 et 2023, celles-ci portant sur la confidentialité des données, les atteintes à la protection des données, et la cybersécurité.

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 telle qu'exigée par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ainsi que par la Loi 25.

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 est 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 et les données conservés ou détruits. Pour conserver et par la suite détruire les documents / les données au bon moment, un calendrier de conservation doit être instauré. Nous avons observé le plan de classification des documents papier. Bien que celui-ci intègre des codes de classification pour chaque catégorie de document, il ne définit pas les RP collectés ainsi que les délais de conservation pour chaque type de données, dont les RP. De plus, le système d'archivage en place ne permet pas une gestion des délais de conservation avec des alertes à la fin de vie des documents. Par ailleurs, aucune mesure n'est définie pour les données électroniques collectées.

Concernant les données électroniques, celles-ci sont sauvegardé régulièrement, sécurisée et les fichiers de sauvegardes sont encryptés, empêchant la lecture non autorisée de celles-ci. Cependant, il n'y a pas de stratégies et mécanismes pour la destruction des données électroniques, et ce, une fois que celles-ci ont atteint les délais de conservation établis.

Concernant la destruction des documents papier, nous avons observé des traces de destruction sécurisée de documents d'archives et d'une unité de stockage par des entreprises spécialisées. Cependant, la Ville n'a pas mis en place une directive pour définir les processus de destruction des données électroniques et des documents physiques collectés par celle-ci, les délais appropriés et la méthodologie sécurisée à employer.

Concernant les lieux de conservation des RP, une des deux salles d'archives est accessible par carte magnétique alors que la deuxième est accessible par l'entremise d'un code sur la serrure. L'utilisation du code de la serrure à lui seul ne garantit pas une stricte restriction des accès. Nous avons observé des systèmes de vidéosurveillance couvrant les entrées des deux salles ainsi que les zones critiques. De plus, il n'y a aucun dispositif de détection et d'extinction automatique des incendies en place.

Recommandations

- Nous recommandons à la Ville de tenir à jour un plan de classification sur la base d'une identification de l'ensemble des RP, tant dans les documents papier que dans les données électroniques. Le plan devra également contenir les délais de conservation pour chaque type de RP, les mesures de sécurité appropriées pour protéger les RP pendant leur conservation, ainsi que les procédures de destruction sécurisée des RP une fois leur période de conservation échue.
- Nous recommandons à la Ville de définir des mécanismes de contrôle permettant de garantir que les RP contenus dans les documents et les données sont conservés uniquement pour la durée appropriée et conformément aux exigences légales.
- 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.
- Nous recommandons à la Ville de veiller à renforcer la sécurité des salles de conservation des documents par :
    - La mise en place d'un dispositif de contrôle d'accès permettant d'identifier clairement les employés ;
    - La mise en place de systèmes de détection d'incendie et d'extinction automatique pour prévenir les risques d'incendie, et
    - L'aménagement pour se prémunir de tous risques environnementaux ou de sabotages des installations.

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 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 RP pour les systèmes incluent dans la portée de nos travaux, soit les systèmes Unicité, Ludik, Bciti, Horizon 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, la modification et le 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'il n'y a pas de procédure formelle en place visant à encadrer le processus de demandes d'accès et d'approbation.

À l'arrivée d'un nouvel employé, le gestionnaire remplit un formulaire de demande SharePoint qui avise directement par courriel le service TI. Cette demande inclut les fonctions du nouvel employé, ainsi que la liste des logiciels, des outils de bureautique et des espaces réseau auxquels l'usager doit accéder. Cependant, la demande ne détaille pas les droits d'accès autorisés aux logiciels et aux données sur le réseau.

Une fois la demande reçue, le service TI se charge de mettre à la disposition du nouvel employé le matériel requis et configuré. Cependant, nous avons noté que l'octroi des profils d'accès aux différents logiciels est décentralisé au niveau des différents services, soit :

- Unicité et Ludik : Service des finances et trésorerie;
- Bciti : Service des communications;
- Horizon : Service des loisirs.

Retrait des accès

Nous avons noté que le processus de retrait des accès n'était pas formalisé. Le service TI est avisé des départs par le gestionnaire à travers le formulaire de départ d'un employé sur SharePoint. Nous avons observé que le gestionnaire soumet au service TI des instructions pour le matériel à restituer, la messagerie électronique et la téléphonie uniquement.

L'équipe TI procède par la suite à la désactivation des accès au contrôleur de domaine, et ce, à la réception du formulaire par le gestionnaire. Cependant, il n'y a aucun mécanisme en place afin de procéder au retrait des accès aux applications, les responsables applicatifs des différents services n'étant pas systématiquement avisés afin de retirer ces accès applicatifs en temps opportun.

Par ailleurs, il est à noter que le formulaire n'est pas systématiquement utilisé et documenté au départ d'un employé.

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 possédants 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 l'existence des comptes génériques (Active Directory, Unicité, Ludik et Horizon – Bibliothèque) utilisés et partagés par des membres des services des TI ou par le fournisseur de l'application. En ce qui concerne Bciti, le service TI de la Ville n'a aucun accès sur la liste exhaustive des comptes d'usagers actifs et donc nous n'avons pas été en mesure d'évaluer l'existence de comptes génériques.

De plus, il est à noter qu'il n'y a pas de contrôles en place concernant les comptes à privilèges des fournisseurs des applications dans l'étendue d'audit.

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 plus facilement gérer les accès autant lors de l'octroi que de modification ou de révision des accès. Dans le cadre de notre audit, nous avons observé que les accès sont gérés par groupe pour les applications et pour le réseau.

Accès aux bases de données

Les accès directs aux bases de données sont réservés aux fournisseurs pour l'ensemble des applications évaluées.

Recommandations

- Nous recommandons à la Ville de formaliser le processus d'octroi d'accès et de modification des accès pour les applications et les serveurs de fichiers. Le processus doit comprendre une autorisation du propriétaire de l'application avant d'octroyer un accès. Ce processus doit être documenté et appliqué à toutes les applications aussi bien au niveau du réseau que des répertoires de fichiers confidentiels.
- 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.
- 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.

- Nous recommandons à la Ville d'éviter ou de minimiser 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 mot 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 de surveiller les comptes génériques attribués aux fournisseurs afin de s'assurer que leur utilisation est restreinte et autorisée. Ces accès peuvent également être octroyés au besoin seulement pour limiter un accès permanent aux environnements de la Ville.

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 écriture, de leurs bases de données et des systèmes de fichiers et du contrôleur de domaine. Il est à noter que le portail de services au citoyen BCITI ne permet pas d'extraire une liste d'utilisateurs et de leur accès, ne permettant ainsi pas d'avoir une vue globale des accès aux RP.

Recommandations

- 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.

  En ce qui concerne les accès aux bases de données et aux systèmes d'exploitation, cette révision devrait être effectuée par la direction du service des TI.

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 en ce qui concerne l'expiration, la longueur minimale, la complexité des mots de passe et/ou le verrouillage après un nombre de tentatives erronées.

Recommandation

- 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 son implémentation sur le contrôleur de domaine, ainsi qu'à l'ensemble des applications.

  La Ville devrait également envisager la mise en place d'une authentification multi facteur 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 RP 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 adressée à la section 3.2 – Conservation et destruction des RP.

En ce qui concerne les salles des serveurs hébergeant les serveurs de données, nous avons noté que l'accès est autorisé par carte et par un système de surveillance couvrant les entrées et les zones critiques. Les accès physiques sont restreints aux agents de la sécurité physique, aux agents des TI et au responsable de bâtiment. Les accès physiques sont gérés par le responsable du service des bâtiments. Le processus des octrois et des retraits des cartes d'accès physique suit le même processus que pour les accès logiques, soit via un formulaire. Le responsable des bâtiments est avisé des accès à octroyer ou à retirer. Cependant, il n'y a pas de processus de revue périodique des accès physiques de mis en œuvre.

De plus, nous avons noté qu'il n'y a pas de dispositif de détection et d'extinction automatique des incendies et qu'il n'y a pas de détecteur de fumée dans la salle.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus de révision des accès physiques aux endroits critiques détenant des RP incluant l'accès aux salles des serveurs.

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*)

La Ville utilise un système qui permet la supervision des vulnérabilités en lien avec les connexions sur les serveurs et celui-ci met automatiquement à jour les serveurs à fréquence hebdomadaire. De plus, les mises à jour des postes de travail sont automatisées et l'antivirus en place permet d'identifier les postes de travail n'ayant pas redémarré après la mise à jour aux fins de suivi par le service des TI.

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

Antivirus

Les postes de travail sont tous protégés par un antivirus qui se met à jour automatiquement. L'administrateur gère les mises à jour via une console. Cette console contient entre autres un tableau de bord lui permettant de voir rapidement les versions des antivirus déployés sur les postes de travail, et d'envoyer des mises à jour de façon centralisées sur les postes de travail.

Par ailleurs, sur les serveurs, la supervision antivirale est assurée par un outil de suivi en temps réel et d'alertes sur les comportements anormaux observés.

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, zones serveurs et applications. Un pare-feu est en place pour protéger ce réseau interne de l'internet et du périmètre externe de la Ville.

Le pare-feu est maintenu 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 offre les traces des journaux sur la console de gestion.

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.

Nous avons noté que les derniers tests d'intrusions ont été réalisés en mai 2021 par l'entremise d'un tiers externe. De plus, ce même tiers réalise à fréquence mensuelle des scans de vulnérabilités du réseau de la Ville. Un cadre formel n'est cependant pas mis en place pour assurer le suivi des vulnérabilités soulevées à la suite de ces tests.

Recommandations

- Nous recommandons à la Ville de réaliser des tests d'intrusion sur une base périodique (aux 2 ans minimalement), et ce, autant sur les périmètres externe et interne de la Ville.
- Nous recommandons à la Ville de s'assurer que les vulnérabilités relevées à la suite des tests d'intrusion ou des scans de vulnérabilités sont suivies et priorisées en fonction de leur criticité.

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 interne pour le signalement des incidents de la Ville. Les employés l'utilisent pour déclarer leurs incidents qui sont alors classés en 3 niveaux de priorité et des délais de prise en charge automatiquement imputés suivant le niveau de priorité : Haute (30 minutes),

Moyenne (4 heures) et Basse (2 jours ouvrables). Les incidents sont formellement documentés dans un billet, incluant les actions mises en œuvre pour résoudre celles-ci, et ce, directement dans l'outil.

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

Les incidents de cybersécurité qui sont remontés par les différentes plateformes de suivi en place font l'objet d'alertes directes sur les courriels des membres du service des TI, de même que les incidents de sauvegarde. Ces derniers sont automatiquement pris en charge et une base de connaissance est en place sous un format Notebook partagé au sein de l'équipe TI pour les solutions sur les incidents non remontés dans l'outil d'incident et les problèmes techniques rencontrés. Cependant, une politique de gestion des incidents de sécurité incluant un processus d'escalade n'est pas établie.

En outre, nous avons relevé l'absence d'une procédure de gestion des atteintes à la confidentialité des renseignements personnels au sein de la Ville. Néanmoins, selon les informations recueillies, les incidents présentant un risque de préjudice sérieux sont remontés à la commission d'accès à l'information du Québec. De plus, aucune mesure n'est en place pour s'assurer de la gestion optimale des incidents de confidentialité portant atteinte sur la confidentialité des RP de citoyens et d'employés au sein de la Ville.

Par ailleurs, nous avons noté qu'il n'y a pas de plan de relève TI formellement documenté. Un plan de relève TI documenté permet d'être en mesure de réagir rapidement en cas d'incident majeur ou de désastre, et permet de définir les applications critiques à relever en premier.

Recommandations

- Nous recommandons à la Ville de définir 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 de l'incident, la méthodologie afin d'évaluer l'incident, le délai de notification à la Commission d'accès à l'information (72 heures), le processus d'escalade; etc.
- Nous recommandons à la Ville d'élaborer un plan de relève TI qui va comprendre la liste des actifs critiques et 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 peuvent héberger des RP, et ce, collectés au bénéfice de la Ville. Dans le cas de Bciti et Horizon, il s'agit d'applications hébergées et gérées par leurs fournisseurs. Les RP se retrouvent donc chez ces fournisseurs.

Portail de services Bciti

Nous pouvons retrouver les RP suivants sur l'application :

- Ouverture de dossiers citoyens : Nom, prénom, carte de citoyen, date de naissance, adresse, courriel, statut de famille, téléphone.

Horizon, logiciel de Bibliothèque

Nous pouvons retrouver les RP suivants sur l'application :

- Données personnelles d'un usager ayant un compte citoyen : Nom, prénom, carte de citoyen et date de naissance. Par la suite, le courriel est requis pour créer un compte d'utilisateur.

Considérant que des RP collectés pour la Ville sont hébergés chez des 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.

Finalement, en ce qui concerne les données 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

- 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'ils respectent les clauses contractuelles et les standards établis en matière de sécurité et de protection des RP.
- 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.

4. Conclusion

La Ville possède plusieurs RP 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 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'amélioration et d'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 les politiques définissant les exigences quant à la gestion des RP. En effet, la Ville a élaboré une politique de confidentialité, sa *Politique-Cadre sur la Gouvernance des Renseignements Personnels* ainsi *que* certaines politiques/directives définissant certaines exigences en matière de sécurité TI et de gestion des RP.

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 nommée un responsable de l'accès et protection des renseignements personnels, également responsable de l'accès aux documents, et ce, tel qu'exigé par la loi 25. Les règles de fonctionnement du comité seront cependant à établir.

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 n'a pas mis en place un inventaire des actifs informationnels et des renseignements personnels ni des documents conservés et des RP qu'ils contiennent. De plus, bien que la Ville dispose d'un logiciel de gestion de documents et d'archives, celui-ci n'est pas utilisé pour le suivi de la conservation des documents comportant des RP conformément aux délais appropriés et aucun mécanisme n'est en place permettant de répondre à une demande sur les RP d'un citoyen ou d'un employé.

L'inventaire des actifs informatiques se limite actuellement aux équipements et ne tient pas compte des informations collectées et stockées par la Ville à travers les différents canaux (bases de données, courriels, applications /logiciels, sites web, etc.).

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 a mis en place un programme de formation sur la cybersécurité par l'entremise d'une plateforme de formation en cybersécurité, La Ville a dispensé différentes formations en 2022 et 2023, celles-ci portant sur la confidentialité des données, les atteintes à la protection des données, et la cybersécurité

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 qu'ils ne puissent plus être reconstitués.

Nous pouvons conclure que bien que la Ville ait un plan de classification, celui-ci ne tient pas compte des données électroniques et ne définit pas les RP collectés ainsi que les délais de conservation pour chaque type de données, dont les RP.

De plus, le système d'archivage en place ne permet pas une gestion des délais de conservation avec des alertes à la fin de vie des documents et aucune mesure n'est définie pour les données électroniques collectées.

En ce qui concerne la destruction des documents papier, bien que la Ville procède à la destruction sécurisée de ceux-ci, il n'y a pas de directive pour définir les processus de destruction des données électroniques et des documents physiques collectés par celle-ci, les délais appropriés et la méthodologie sécurisée à employer.

Mesures de protection

Critère – Les accès sont accordés de manière 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 sont accordés aux personnes autorisées uniquement que certains paramètres de sécurité permettent de prévenir des accès non autorisés aux RP, ces mécanismes pourraient être améliorés :

- Formaliser le processus d'octroi d'accès et de modification des accès pour les applications et les serveurs de fichiers, incluant l'autorisation du propriétaire de l'application avant d'octroyer un accès, et ce, pour l'ensemble des applications.
- 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 responsables applicatifs lors du départ d'un employé, et ce, pour assurer le retrait des accès en temps opportun.
- Éviter ou minimiser l'utilisation de comptes génériques ou pour les situations où ces comptes sont requis, contrôler l'utilisation de ceux-ci, et ce, afin d'assurer l'imputabilité des actions commises.
- 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.

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, bien que la Ville procède à des tests d'intrusion qui permettent de mesurer les vulnérabilités des systèmes contenant des RP face aux cyberattaques, ceux-ci ne sont pas réalisés à une fréquence régulière.

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. De plus, les incidents ou problèmes identifiés directement par le service des TI ne sont pas formellement journalisés dans le système de billetterie, ce qui permettrait d'avoir une vue globale des incidents et d'identifier les tendances ou les incidents récurrents.

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

Nous pouvons conclure qu'en ce qui concerne la gestion des fournisseurs, ceux-ci pouvant héberger 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 qu'ils ne puissent plus être reconstitués;
- Mesures de protection à l'égard des RP :
  - Les accès sont accordés de manière 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;
  - 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