Vérificateur général
de la Ville de Montréal

Rapport du vérificateur général de la Ville de Montréal
au conseil municipal et au conseil d'agglomération

Pour l'exercice terminé le 31 décembre 2012

5.13

Protection des renseignements personnels

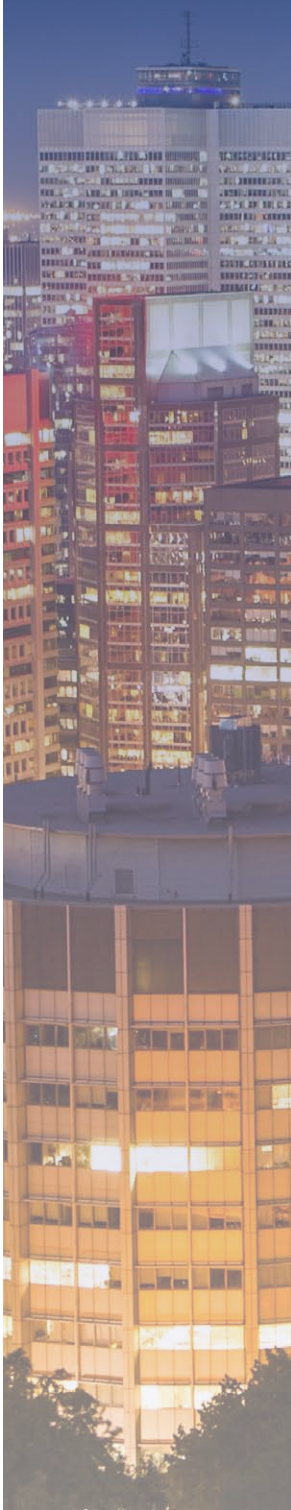

Table des matières

Liste des sigles

CAI	Commission d'accès à l'information
NAS	numéro d'assurance sociale
RP	renseignement personnel
STI	Service des technologies de l'information

5.13. Protection des renseignements personnels

1. Introduction

Avec plus de 1,6 million d'habitants et ses 28 000 employés, la Ville de Montréal (la Ville) collecte et traite un nombre considérable de renseignements afférents à la vie privée des citoyens, des élus et de ses employés. Ces renseignements sont nécessaires afin que la Ville puisse desservir adéquatement le public. Ces activités peuvent être, par exemple, la gestion des demandes des citoyens (par l'entremise du service 311 ou des bureaux d'arrondissement) et la gestion des employés.

Au Canada, la vie privée est un droit fondamental qui est protégé de façon globale par les législations tant fédérales que provinciales.

Adoptée le 27 juin 1975, la Charte des droits et libertés de la personne du Québec fait du droit à la vie privée un droit fondamental. Cette charte stipule, entre autres, que les libertés et droits fondamentaux des citoyens sont :

- le droit à la sauvegarde de sa dignité, de son honneur et de sa réputation;
- le droit au respect de sa vie privée;
- le droit au respect du secret professionnel.

Véritable pionnier en Amérique du Nord en matière d'accès à l'information et de protection de la vie privée, le Québec a bâti, au cours des trois dernières décennies, un modèle législatif original qui a tracé la voie à la mise en place de mesures similaires partout au Canada.

Incarné par la Commission d'accès à l'information (CAI) du Québec, ce modèle original constitue une référence incontournable parmi l'ensemble des pays occidentaux en matière d'accès à l'information en lien avec la protection de la vie privée.

La CAI applique deux législations :

- Pour le secteur public : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1];
- Pour le secteur privé : *Loi sur la protection des renseignements personnels dans le secteur privé*[2].

1 LRQ, chapitre A-2.1.
2 LRQ, chapitre P-39.1.

En tant que municipalité, la Ville est assujettie à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Cette loi énonce deux droits fondamentaux : le droit d'accès et le droit à la protection des renseignements personnels (RP). Elle s'applique à tous les documents, qu'ils soient sous forme écrite, graphique, sonore, visuelle, informatisée ou autre.

Un RP se définit comme suit :

- Il identifie une personne physique (par opposition à une personne morale);
- Il permet l'identification d'un individu (par opposition à des données dépersonnalisées);
- Il est factuel ou subjectif sur une personne peu importe sa forme ou son support, qu'il soit consigné ou non.

Compte tenu de leur nature, les RP sont confidentiels. Leur vol et divulgation sont souvent utilisés à des fins frauduleuses pouvant aller jusqu'à l'usurpation d'identité et à l'atteinte à la réputation d'individus. Les types de RP les plus critiques sont, entre autres :

- le numéro d'assurance sociale (NAS);
- le numéro d'assurance maladie;
- la date de naissance;
- le salaire et les relevés d'impôts;
- les coordonnées bancaires;
- les renseignements médicaux;
- le curriculum vitæ.

Comme toute autre information de nature sensible, la Ville doit assurer la confidentialité des RP. À cet effet, elle doit mettre en place des mesures de sécurité afin de les protéger contre le vol, la divulgation et l'utilisation non autorisée.

2. Portée de la mission

L'objectif de notre mission de vérification était d'évaluer l'efficacité des contrôles mis en place pour assurer une sécurité logique et physique adéquate des RP des citoyens et des employés détenus par la Ville, à l'exception de ceux concernant le Service de police de la Ville de Montréal.

À cet effet, nous nous sommes interrogés sur les aspects suivants :

- **Encadrements de la gestion des RP :** Est-ce que la Ville dispose d'encadrements définissant les exigences quant à la saine gestion des RP applicables à l'ensemble des unités d'affaires?

- **Inventaire des RP :** Existe-t-il un inventaire des RP, complet et à jour, permettant à la Ville de disposer d'un portrait global des RP à protéger dans le but d'assurer leur confidentialité?
- **Sensibilisation des employés :** Les employés sont-ils sensibilisés quant aux enjeux et aux risques liés aux RP afin qu'ils soient plus à même de respecter les règles de sécurité relatives à la protection des RP?
- **Gestion des incidents :** Advenant un événement majeur pouvant conduire à la divulgation massive de RP, existe-t-il une procédure de gestion des incidents permettant à la Ville de réagir dans les meilleurs délais afin de limiter les répercussions actuelles et potentielles, et de prendre les mesures nécessaires à la résolution de l'incident?
- **Accès logiques :** Les paramètres de sécurité (p. ex. les mots de passe et les droits d'accès) sont-ils configurés de manière à ce que seules les personnes autorisées, qui de par leurs fonctions requièrent l'utilisation de RP, puissent accéder aux systèmes d'information les traitant?
- **Accès physiques :** Y a-t-il des mécanismes de cloisonnement, tels qu'une voûte sécurisée ou des classeurs verrouillés, afin de limiter l'accès aux RP présents sur des supports physiques (p. ex. des dossiers médicaux et des dossiers d'employés) uniquement aux personnes autorisées?
- **Rétention des RP :** Est-ce que les RP sont hébergés uniquement dans les environnements de production des systèmes d'information qui sont utilisés au quotidien par les employés et les gestionnaires? Au lieu des RP réels, est-ce que des RP dépersonnalisés sont utilisés dans les environnements de test, de développement et de formation pour limiter les risques de perte de confidentialité?
- **Transmission des RP :** Les RP transmis à de tierces parties (p. ex. la CSST, le ministère du Revenu) sont-ils protégés par des mécanismes de sécurité afin de préserver la confidentialité des informations transférées?
- **Destruction des RP :** Les RP sont-ils dépersonnalisés ou détruits de manière à ce qu'ils ne puissent plus être reconstitués afin d'éviter toute utilisation frauduleuse?

À cet égard, les dossiers suivants ont fait l'objet de notre vérification puisqu'ils renferment des RP importants et critiques :

- Concernant les citoyens :
  - Dossiers de candidature,
  - Demandes de services et plaintes,
  - Inscriptions à des activités de loisirs,
  - Demandes de subventions à la rénovation;
- Concernant les employés, les élus, les juges, les commissaires et les retraités :
  - Dossiers des employés,

- Dossiers médicaux,
- Dossiers de paie,
- Dossiers des régimes de retraite.

Parallèlement, nous avons sélectionné les unités administratives suivantes pour notre vérification eu égard à leurs responsabilités relativement à la gestion des RP et au volume d'information détenu et traité :

- Direction du greffe;
- Service du capital humain et des communications;
- Service des technologies de l'information (STI);
- Direction des services regroupés aux arrondissements, relevant du Service de la concertation des arrondissements et des ressources matérielles;
- Division de la paie institutionnelle, relevant de la Direction de la comptabilité et du contrôle financier du Service des finances;
- Division de la gestion des rentes, relevant de la Direction de la gestion financière du Service des finances;
- Division de la gestion des programmes de logement, relevant de la Direction de l'habitation du Service de la mise en valeur du territoire;
- Division des ressources humaines :
  - du Service de sécurité incendie de Montréal,
  - de l'arrondissement de Saint-Laurent,
  - de l'arrondissement de Montréal-Nord,
  - de l'arrondissement de Côte-des-Neiges–Notre-Dame-de-Grâce,
  - de l'arrondissement de Villeray–Saint-Michel–Parc-Extension.

Par ailleurs, voici la liste des systèmes d'information traitant des RP couverts au cours de nos travaux de vérification :

- SIMON RH (dossiers de candidature, dossiers de base des employés);
- SIMON PAIE (paies des juges, des élus, des commissaires et des retraités);
- Employeur D (dossiers médicaux);
- Paie (IBM);
- GDC (gestion des demandes des citoyens);
- Super H (dossiers des employés);
- InfoRH (entrepôt de données du Service du capital humain et des communications);
- Registre des postes (affectations et salaires des employés);
- ARIEL (régimes de retraite);
- Ludik (loisirs);
- SDSR (système des demandes de subventions à la rénovation).

Il est à noter que notre mission de vérification ne peut, en aucun cas, être considérée comme un mandat attestant du niveau de conformité de la Ville à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

3. Constatations et recommandations

Dans l'ensemble, notre vérification n'a révélé aucune lacune majeure quant aux mécanismes de contrôle mis en place pour la protection des RP détenus et traités par la Ville.

Le tableau 1 présente les résultats globaux de notre vérification en fonction des domaines de risques recensés.

Tableau 1 – Résultats globaux selon les domaines de risques

Domaines de risques	Risque inhérent[a]	Risque résiduel[b]
Encadrements de la gestion des RP Divulgation des RP en raison de l'absence d'encadrements définissant les responsabilités et les exigences spécifiques en matière de protection des RP.	Élevé[c]	Faible
Inventaire des RP Perte de confidentialité de certains RP qui n'auraient pas été déterminés correctement au cours du processus d'inventaire des RP et qui n'auraient pas été protégés adéquatement.	Modéré	Faible
Sensibilisation des employés Divulgation de certains RP à la suite de l'ignorance des employés quant à la conduite à adopter pour protéger et maintenir la confidentialité des RP.	Élevé	Faible
Gestion des incidents Incapacité de traiter et de régler en temps opportuns les problèmes majeurs relatifs, par exemple, à la divulgation massive des RP.	Élevé	Faible
Accès logiques Perte de confidentialité des RP subséquente à des accès non autorisés aux systèmes d'information.	Critique	Modéré
Accès physiques Perte de confidentialité de certains RP subséquente à des mesures de sécurité inadéquates appliquées aux documents et aux dossiers physiques renfermant des RP.	Critique	Faible
Rétention des RP Des RP réels sont utilisés pour les environnements autres que ceux de production et pourraient être dérobés ou divulgués.	Critique	Élevé
Transmission des RP Perte de confidentialité des RP après avoir été interceptés au moment de leur transmission entre systèmes d'information.	Élevé	Faible
Destruction des RP Reconstitution et divulgation des RP qui n'ont pas été détruits de façon sécuritaire et irréversible.	Critique	Faible

[a] Risque brut sans considération des mécanismes de contrôle.
[b] Exposition au risque après une évaluation des mécanismes de contrôle en place.
[c] Se référer au tableau 2.

En outre, la section 3.1 et les suivantes détaillent des déficiences spécifiques que nous avons constatées au cours de notre vérification et qui nécessitent des correctifs. Soulignons que nous avons évalué ces déficiences à la lumière des niveaux d'impact présentés dans le tableau 2.

Tableau 2 – Définitions des niveaux d'impact

Niveaux d'impact	Définitions des niveaux d'impact
Critique	Conséquence directe sur la sécurité des personnes, atteinte majeure à la réputation des personnes et à la réputation de la Ville advenant la divulgation de RP.
Élevé	Bien qu'il n'y ait pas de conséquence sur la sécurité des personnes en raison de la présence d'un grand volume de RP, la perte de confidentialité de ces informations nuirait de façon importante aux opérations et à la réputation de la Ville. Les personnes pourraient être victimes de vol et d'usurpation d'identité.
Modéré	À cause de la présence de certains RP, une perte de confidentialité de ces derniers nuirait modérément à la réputation et aux opérations de la Ville.
Faible	Répercussions négligeables sur les opérations et les services de la Ville. Perte de confiance improbable des citoyens envers la Ville.

3.1. Renseignements personnels présents dans des environnements de systèmes d'information autres que ceux de production

3.1.A. Contexte et constatations

Les systèmes d'information ont, en général, plusieurs environnements distincts. Il y a l'environnement de production, utilisé par les employés dans le cadre de leur travail, qui contient des données réelles afin de répondre aux besoins d'affaires. Ensuite, il y a les environnements utilisés à d'autres fins, par exemple :

- les environnements de développement : ils sont utilisés par les spécialistes en technologies de l'information pour développer ou améliorer les fonctionnalités des applications;
- les environnements de tests : ils sont utilisés par des groupes d'utilisateurs et d'informaticiens pour s'assurer que les changements apportés aux applications fonctionnent correctement;
- les environnements de formation : ils permettent aux employés d'acquérir l'expertise nécessaire pour utiliser efficacement les systèmes d'information.

Cependant, les environnements autres que ceux de production n'ont nullement besoin d'utiliser des données réelles, surtout lorsqu'il s'agit de données confidentielles comme les RP. Cela n'est justifié par aucun besoin d'affaires. Les saines pratiques de l'industrie recommandent que des données fictives soient utilisées dans les environnements autres que ceux de production.

Au cours de nos travaux de vérification, nous avons constaté que des RP réels étaient copiés, en totalité ou en partie, des environnements de production aux différents

environnements de tests et de développement. De plus, aucune procédure systématique d'effacement des RP n'est appliquée une fois les tests ou les travaux de développement terminés. Les systèmes d'information en cause sont énumérés ci-après.

- **SIMON (SIMON RH et SIMON PAIE) :** SIMON est le progiciel de gestion intégré de la Ville. SIMON RH contient les dossiers de base des employés ainsi que les dossiers de candidature. SIMON PAIE comprend les 14 500 dossiers de paie des élus, des juges, des commissaires et des retraités. Il y a, en moyenne, une douzaine d'environnements utilisés pour du développement et des tests. Uniquement deux de ces environnements ont le NAS et la date de naissance dépersonnalisés pour ne plus correspondre à des personnes physiques réelles. Les autres contiennent des copies, parfois intégrales, des RP de l'environnement de production dont les plus critiques sont, entre autres, le NAS, la date de naissance, la rémunération et les coordonnées bancaires.
- **Super H :** il contient l'ensemble des dossiers des employés en plus de ceux des postulants, des élus, des juges, des commissaires et des retraités. L'environnement de tests utilise des RP réels provenant de l'environnement de production tels que le NAS, la date de naissance, le salaire, l'adresse et le numéro de téléphone résidentiels.
- **InfoRH :** c'est l'entrepôt de données du Service du capital humain et des communications qui contient les RP de l'ensemble des employés ainsi que des postulants, des élus, des juges, des commissaires et des retraités. L'environnement de développement contient des RP réels, dont le NAS, la date de naissance, le salaire, l'adresse et le numéro de téléphone résidentiels.
- **Registre des postes :** cette application contient les informations d'affectation des employés de la Ville. Les RP réels sont copiés de l'environnement de production à l'environnement de tests. Ainsi, on trouve, entre autres, les événements salariaux.
- **Employeur D :** ce système contient les dossiers médicaux des employés, des élus, des juges et des commissaires lorsqu'ils font face à des problèmes de santé. L'environnement de tests utilise des RP réels provenant de l'environnement de production. Parmi ces renseignements sont présents, entre autres, les renseignements médicaux, le NAS, le numéro d'assurance maladie, la date de naissance et le salaire.
- **Paie (IBM) :** cette application gère la paie de la plupart des employés de la Ville et contient les RP afférents aux salaires. Les environnements de développement et de tests contiennent des extractions des RP réels provenant de l'environnement de production. Les types de RP sont, entre autres, les coordonnées bancaires, le NAS, la rémunération, l'adresse résidentielle, la date de naissance et les relevés d'impôts.

Nous estimons que le niveau d'impact est **élevé,** car la Ville fait face aux risques potentiels suivants : en permettant l'utilisation de RP réels en dehors des environnements de production, les RP de l'ensemble des employés, des élus, des juges, des commissaires,

des retraités et des postulants pourraient être dérobés et divulgués à des personnes non autorisées. Avec de tels renseignements, des individus malintentionnés pourraient perpétrer des actions frauduleuses telles que le vol et l'usurpation d'identité. Dans tous les cas, cela porterait grandement atteinte à la réputation de la Ville.

3.1.B. Recommandation

Nous recommandons au Service du capital humain et des communications ainsi qu'à la Division de la paie institutionnelle du Service des finances, en concertation avec le Service des technologies de l'information, de mettre en place des procédures de caviardage des renseignements personnels réels (p. ex. le numéro d'assurance sociale, la date de naissance) pour les données des environnements autres que ceux de production relativement aux systèmes d'information dont ils sont propriétaires :

- **Service du capital humain et des communications :**
  - **SIMON RH,**
  - **Super H,**
  - **InfoRH,**
  - **Registre des postes,**
  - **Employeur D;**
- **Division de la paie institutionnelle :**
  - **Paie (IBM),**
  - **SIMON PAIE.**

Réponses des unités d'affaires :

SERVICE DU CAPITAL HUMAIN ET DES COMMUNICATIONS

SIMON RH et InfoRH : Nous avons communiqué avec le STI afin de faire brouiller les données confidentielles dans tous les environnements autres que celui de production. ***(Complété, avril 2013)***

Super H et Registre des postes : Le STI a déjà pris les mesures nécessaires afin de brouiller les données de l'environnement « test ». Néanmoins, nous sommes actuellement en communication avec lui afin de nous assurer des éléments d'information qui ont été pris en considération. ***(Complété, avril 2013)***

Employeur D : La demande a déjà été faite au STI afin de brouiller les données confidentielles.

De plus, étant donné que cette application contient des données sur les accidents et les maladies, nous sommes en train de réviser les informations qui seront considérées comme confidentielles. ***(Complété, mars 2013)***

SERVICE DES FINANCES

Une demande de travail a été produite auprès du STI afin de mettre en place des procédures de caviardage des RP pour les systèmes de gestion de la paie. ***(Échéancier prévu : décembre 2013)***

3.2. Paramètres de sécurité des mots de passe non configurés

3.2.A. Contexte et constatations

Les mots de passe sont la première ligne de défense pour empêcher les accès non autorisés aux systèmes d'information contenant des données critiques et confidentielles, telles que les RP.

Les paramètres de sécurité des mots de passe permettent d'exiger des utilisateurs le choix de mots de passe robustes. Ils définissent, entre autres, la longueur du mot de passe, sa complexité, son délai d'expiration et l'historique des derniers mots de passe utilisés.

Selon la procédure du STI intitulée « Standard sur les clefs d'accès aux ressources informationnelles », les exigences en matière de mots de passe sont, entre autres, les suivantes :

- Délai d'expiration : 90 jours;
- Longueur des mots de passe : huit caractères minimum;
- Historique : six derniers mots de passe;
- Activation de la complexité des mots de passe (p. ex. la combinaison de caractères alphanumériques, de caractères spéciaux et de lettres majuscules et minuscules).

Au cours de nos travaux de vérification, nous avons constaté que les paramètres de sécurité des mots de passe n'étaient pas activés pour l'application Employeur D. Quant à Ludik, l'application n'a aucun paramètre de sécurité activable. La seule contrainte pour ces applications est que l'utilisateur doit choisir un mot de passe d'un caractère au minimum. Il n'y a aucun délai d'expiration ni historique des mots de passe. Dans le cas d'Employeur D, le mot de passe assigné à l'utilisateur au moment de la création de son accès correspond à son prénom, et le système ne requiert pas qu'il soit changé lors de la première connexion.

Nous estimons que le niveau d'impact est **élevé,** car la Ville fait face aux risques potentiels suivants : étant donné qu'aucune exigence de sécurité n'est requise pour les mots de passe, des personnes malintentionnées pourraient les découvrir facilement. En conséquence, elles auraient accès, dans le cas d'Employeur D, aux RP critiques des employés, des élus, des juges et des commissaires qui ont eu des problèmes de santé (p. ex. le NAS, le numéro d'assurance maladie, la date de naissance, le salaire, le dossier

médical) et, dans le cas de Ludik, sur les 800 000 dossiers citoyens, environ 15 200 contiennent le NAS et le numéro d'assurance maladie. Advenant la divulgation de tels renseignements, ces personnes pourraient commettre des vols d'identité et porter atteinte non seulement à la réputation de la Ville, mais aussi à celle des employés, des élus, des juges et des commissaires.

3.2.B. Recommandation

Nous recommandons au Service du capital humain et des communications, propriétaire d'Employeur D et de Ludik, en concertation avec le Service des technologies de l'information :

- **de configurer les paramètres de sécurité des mots de passe avec, au minimum, les exigences suivantes :**
  - **longueur minimale : huit caractères,**
  - **délai d'expiration : 90 jours,**
  - **historique : six derniers mots de passe,**
  - **activation de la complexité des mots de passe;**
- **d'effectuer le changement de tous les mots de passe actuels dans les meilleurs délais, sans attendre le délai de 90 jours, pour se conformer aux nouveaux paramètres;**
- **d'exiger que les nouveaux utilisateurs changent leur mot de passe initial lors de leur première connexion.**

Réponse de l'unité d'affaires :

Pour l'application Employeur D, des mesures ont été prises à la suite de la vérification du Bureau du vérificateur général en décembre dernier.

La longueur minimale est maintenant de huit caractères avec au moins deux chiffres.

Le délai d'expiration a été configuré à 90 jours.

Un communiqué a été envoyé à tous les utilisateurs afin de les informer de ces changements.

Tous les mots de passe ont été changés. ***(Complété, décembre 2012)***

Pour le progiciel Ludik, le STI est en discussion avec le fournisseur afin de déterminer la meilleure méthode à utiliser afin d'appliquer les recommandations et de limiter les développements applicatifs du progiciel. ***(Complété, avril 2013 [stratégie de correction]; échéancier prévu : à venir [mise en œuvre de la stratégie])***

3.3. Lacune dans le processus de révision des utilisateurs et de leurs droits d'accès

3.3.A. Contexte et constatations

Pour une protection adéquate des RP, la gestion des droits d'accès des utilisateurs aux systèmes d'information doit non seulement prévoir les exigences et les mécanismes de sécurité pour la création, la suppression et la modification des accès, mais elle doit également comprendre un processus de révision des comptes d'utilisateurs.

Un processus de révision récurrent permet de s'assurer que tous les employés ayant quitté la Ville ou ayant changé de fonction ne conservent pas leurs anciens privilèges d'accès.

Au cours de nos travaux de vérification, nous avons constaté qu'il n'y avait pas de processus formel de révision des droits d'accès des utilisateurs pour les systèmes d'information suivants :

- GDC;
- Employeur D;
- SIMON RH;
- Ludik.

Pour les systèmes d'information Registre des postes, Super H et InfoRH, la révision des droits d'accès des utilisateurs est effectuée annuellement. Compte tenu des RP critiques, la fréquence de révision est, à notre avis, insuffisante.

Nous estimons que le niveau d'impact est **modéré,** car la Ville fait face aux risques potentiels suivants : des personnes ayant quitté leur emploi à la Ville pourraient conserver des droits d'accès aux systèmes d'information et celles ayant changé de fonction pourraient conserver d'anciens droits d'accès ne correspondant plus à leurs nouvelles tâches et responsabilités. Cela pourrait engendrer une perte de confidentialité des RP détenus par la Ville.

3.3.B. Recommandation

Nous recommandons à la Direction des services regroupés aux arrondissements du Service de la concertation des arrondissements et des ressources matérielles et au Service du capital humain et des communications de mettre en place un processus récurrent de révision (au minimum trimestriel) des droits d'accès des utilisateurs relativement aux systèmes d'information dont ils sont propriétaires :

- **Direction des services regroupés aux arrondissements :**
  - **GDC;**
- **Service du capital humain et des communications :**
  - **Employeur D,**
  - **SIMON RH,**
  - **Super H,**
  - **Registre des postes,**
  - **InfoRH,**
  - **Ludik.**

Réponses des unités d'affaires :

SERVICE DE LA CONCERTATION DES ARRONDISSEMENTS ET DES RESSOURCES MATÉRIELLES

Un rapport trimestriel sera extrait par le pilote du système GDC (Section de l'expertise et du soutien 311) et sera envoyé aux utilisateurs experts des 19 arrondissements pour faire le suivi des accès.

Le tout sera documenté et enregistré dans un processus interne à la Section de l'expertise et du soutien 311. ***(Échéancier prévu : mai 2013)***

SERVICE DU CAPITAL HUMAIN ET DES COMMUNICATIONS

Une procédure sera mise en place d'ici la fin avril 2013 afin de valider les accès une fois par trimestre. ***(Complété, avril 2013)***

Pour le progiciel Ludik, une procédure est en cours de rédaction afin de valider les accès une fois par trimestre. ***(Complété, avril 2013)***

3.4. Procédures de gestion des accès absentes ou incomplètes

3.4.A. Contexte et constatations

Les procédures de gestion sont importantes au sein d'une organisation afin que les différents services utilisent le même *modus operandi* en matière d'activités qui répondent aux risques d'affaires décelés et, plus précisément dans le cadre de notre mission de

vérification, qui diminuent à un niveau acceptable les risques afférents aux accès des utilisateurs aux systèmes d'information contenant des RP.

Par exemple, une procédure de gestion des accès des utilisateurs comprendra les exigences à respecter pour les éléments suivants :

- Demande d'accès;
- Modification des accès;
- Révision des utilisateurs et de leurs droits d'accès;
- Suppression des accès.

Au cours de nos travaux de vérification, nous avons constaté les lacunes suivantes :

- Il n'existe pas de procédure de gestion des accès pour l'application SDSR;
- La procédure de gestion des accès de l'application Employeur D est incomplète, puisqu'elle ne contient que la description succincte des étapes à suivre au moment des demandes de création d'accès.

Nous estimons que le niveau d'impact est **modéré,** car la Ville fait face aux risques potentiels suivants : des procédures absentes ou non exhaustives pourraient faire en sorte que les exigences de sécurité afférentes à la gestion des accès ne soient pas respectées. Par conséquent, des personnes non autorisées pourraient avoir accès aux RP hébergés au sein d'Employeur D et de SDSR.

3.4.B. Recommandation

Nous recommandons au Service du capital humain et des communications (pour le système d'information Employeur D) et à la Division de la gestion des programmes de logement, relevant de la Direction de l'habitation du Service de la mise en valeur du territoire (pour le système d'information SDSR) de définir une procédure de gestion des accès contenant, au minimum, les exigences à respecter pour les éléments suivants :

- **Demande d'accès;**
- **Modification des accès;**
- **Révision des utilisateurs et de leurs droits d'accès;**
- **Suppression des accès.**

Réponses des unités d'affaires :

SERVICE DU CAPITAL HUMAIN ET DES COMMUNICATIONS

À la suite de votre recommandation, la procédure a été révisée. ***(Complété, mars 2013)***

SERVICE DE LA MISE EN VALEUR DU TERRITOIRE

Rédaction d'une procédure de gestion des accès au système SDSR qui prévoit la marche à suivre pour les demandes, les modifications et les annulations d'accès ainsi que pour la mise à jour biannuelle de la liste des utilisateurs.

Diffusion à l'ensemble de la Direction de l'habitation de la procédure de gestion des accès par courriel et dépôt des documents dans le répertoire commun sur le réseau informatique.

Première mise à jour du tableau des utilisateurs du système. Cette mise à jour devra être réalisée deux fois par année. ***(Complété, avril 2013)***

3.5. Lacunes dans la sécurisation physique des locaux hébergeant les dossiers de paie

3.5.A. Contexte et constatations

La Division de la paie institutionnelle occupe, entre autres, les locaux de la mezzanine de l'édifice Chaussegros-de-Léry. Dans ces locaux, certains dossiers de paie des employés sont rangés dans des rayonnages mobiles (de type Rolodex). Ces dossiers contiennent de nombreux RP sensibles comme le prénom, le nom, l'adresse, le NAS, les coordonnées bancaires et la date de naissance des employés.

Selon les bonnes pratiques de l'industrie et conformément à l'esprit de la *Loi d'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les accès aux locaux contenant des données sensibles doivent être protégés par des mécanismes de cloisonnement des accès physiques. Ces mécanismes peuvent être, par exemple, un local réservé à l'entreposage des dossiers, des portes installées séparant les couloirs d'accès des bureaux ou d'autres points d'accès comme des escaliers. Ces portes doivent être verrouillées, par exemple, par des lecteurs de cartes d'accès.

En visitant l'ensemble des locaux de la Division de la paie institutionnelle, nous avons constaté que, à partir de la mezzanine, un escalier, qui n'est pas une sortie de secours, se rend aux étages supérieurs occupés uniquement par des employés d'autres services de la Ville. Cet escalier, qui offre un accès physique sans obstacle aux niveaux supérieurs, n'est pas doté de mécanisme de cloisonnement des accès physiques.

Nous estimons que le niveau d'impact est **modéré,** car la Ville fait face aux risques potentiels suivants : des employés ne faisant pas partie de la Division de la paie institutionnelle pourraient, en empruntant l'escalier, circuler sans entrave jusqu'aux dossiers de paie présents dans le Rolodex de la mezzanine. Par conséquent, un employé

malintentionné pourrait avoir accès à des RP et les dérober en consultant certains dossiers de paie.

3.5.B. Recommandation

Nous recommandons à la Division de la paie institutionnelle du Service des finances de mettre en place des mesures de sécurité permettant le contrôle des accès physiques provenant de l'escalier menant aux étages supérieurs afin que seuls les employés autorisés puissent avoir accès à la mezzanine de l'édifice Chaussegros-de-Léry.

Réponse de l'unité d'affaires :

> *La Division de la paie institutionnelle déménagera ses activités au 740, rue Notre-Dame Ouest à compter de l'été 2013. Les locaux seront sécurisés par des portes à accès magnétique.* ***(Échéancier prévu : été 2013)***