COMMISSION MUNICIPALE DU QUÉBEC

SÉCURITÉ DES SYSTÈMES DE CONTRÔLE INDUSTRIELS

AUDIT DE PERFORMANCE

NOVEMBRE 2022

Québec

Québec, siège social
10, rue Pierre-Olivier-Chauveau
Mezzanine, aile Chauveau
Québec (Québec) G1R 4J3

Montréal
500, boulevard René-Lévesque Ouest
Bureau 24.200, 24e étage
Case postale 24
Montréal (Québec) H2Z 1W7

Saint-Hyacinthe
1200, rue Girouard Ouest
Saint-Hyacinthe (Québec) J2S 2Z1

Ce document a été réalisé par la Commission municipale du Québec.

Il est publié à l'adresse suivante : www.cmq.gouv.qc.ca.
ISBN : 978-2-550-92886-7 (IMPRIMÉ)
ISBN : 978-2-550-92887-4 (PDF)

Commission municipale Québec

La saine gestion au bénéfice de tous

La Commission municipale a annoncé, en juin 2021, des travaux d'audit dans trois municipalités concernant l'accès et la sécurité des systèmes de contrôle industriels. Ces travaux ont été réalisés par la Vice-présidence à la vérification de la Commission. Le présent document constitue le rapport de cette dernière.

Conformément à la *Loi sur la Commission municipale*, ce rapport est acheminé aux municipalités concernées. Il est également transmis à la ministre des Affaires municipales et diffusé sur le site Web de la Commission.

La Commission vise, par ses travaux d'audit, à susciter des changements durables et positifs dans le fonctionnement et la performance des municipalités et des organismes municipaux, et ce, au bénéfice des citoyens. Je vous souhaite une excellente lecture.

Le président,

Jean-Philippe Marois
Québec, novembre 2022

Municipalités auditées

Source : MAMH - Direction de la transformation numérique, de la géomatique et de la bureautique, septembre 2022

Commission municipale Québec

La saine gestion au bénéfice de tous

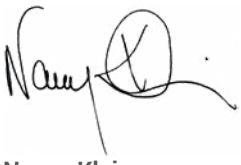
Conformément à la *Loi sur la Commission municipale*, le rapport d'audit de performance portant sur l'accès et la sécurité des systèmes de contrôle industriels est adressé aux municipalités auditées suivantes, plus particulièrement aux :

- Conseil municipal de la Ville de Dollard-Des Ormeaux
- Conseil municipal de la Ville de La Prairie
- Conseil municipal de la Ville de Rouyn-Noranda

Ce rapport doit être déposé à la première séance du conseil qui suit sa réception. De même, il est transmis à la ministre des Affaires municipales et publié sur le site Web de la Commission, accompagné des lettres adressées à chacune des municipalités auditées. Les travaux se sont inscrits dans une approche respectueuse et collaborative.

Enfin, comme indiqué dans le *Guide à l'intention des municipalités et des organismes municipaux audités*, les municipalités auditées sont invitées à produire un plan d'action pour la mise en œuvre des recommandations formulées dans ce rapport et un suivi de l'application de ces recommandations sera réalisé ultérieurement.

La vice-présidente à la vérification,



Nancy Klein
Québec, novembre 2022

Vue d'ensemble de l'audit

Pourquoi avons-nous réalisé cet audit ?

Dans le cadre de leurs activités, les municipalités offrent des services de proximité qui contribuent à la mise en place et au maintien d'un milieu de vie adapté aux besoins des citoyens. À cette fin, elles construisent et entretiennent diverses infrastructures, notamment des usines de traitement de l'eau, des bibliothèques, des piscines et des arénas. Pour la gestion de ces infrastructures, les municipalités utilisent différents systèmes de contrôle industriels, lesquels automatisent et contrôlent les processus industriels et intègrent des équipements et des logiciels de surveillance et de contrôle.

De nos jours, les systèmes de contrôle industriels ne sont plus des systèmes isolés, placés dans des emplacements sécurisés physiquement. Comme ces systèmes doivent permettre la connectivité avec d'autres systèmes et réseaux ainsi que les interventions à distance, ils intègrent de plus en plus de solutions informatiques. Par conséquent, ils sont susceptibles d'être visés par les mêmes enjeux de sécurité que tout autre système informatique de la municipalité. Toutefois, les systèmes de contrôle industriels comportent des risques différents en cas d'attaques informatiques ou d'accès physiques non autorisés, qui peuvent, entre autres, provoquer des incidents, comme la perturbation des services fournis, ou des événements ayant de conséquences mettant en danger la santé publique ou causant des dommages à l'environnement. Ces incidents risquent également d'engendrer des coûts importants et de porter atteinte à la réputation de la municipalité.

Quel était notre objectif ?

Nos travaux d'audit avaient pour objectif de déterminer si des mesures de contrôle et de sécurité appropriées sont déployées afin d'assurer l'efficacité du processus de gestion des accès et la sécurité des systèmes de contrôle industriels sélectionnés, soit ceux liés au traitement de l'eau et à la gestion des bâtiments municipaux.

Qui avons-nous audité ?

- Ville de Dollard-Des Ormeaux
- Ville de La Prairie
- Ville de Rouyn-Noranda

Quels sont les constats importants de l'audit ?

Nous présentons ci-dessous les principaux constats que nous avons faits lors de l'audit concernant la sécurité des systèmes de contrôle industriels. Il est à noter que ces constats portent sur le processus de gestion lié à la sécurité des systèmes de contrôle industriels, et non sur la qualité des mesures mises en place pour assurer la sécurité de ces systèmes.

- Les trois municipalités disposent de diverses données sur les actifs des systèmes de contrôle industriels. Cependant, elles ne réalisent aucune classification de ces actifs en fonction de leur sensibilité et de leur caractère critique. En négligeant cette étape, ces municipalités n'ont pas l'assurance qu'elles déploient les mesures de sécurité appropriées afin de diminuer les risques inacceptables.
- De plus, les municipalités auditées n'ont pas défini formellement dans leurs cadres normatifs leurs objectifs et leurs exigences en matière de sécurité de l'information ou de sécurité des systèmes de contrôle industriels afin notamment d'orienter toutes les activités relatives à la sécurité de l'information. Deux des trois municipalités n'ont pas désigné formellement de responsable en matière de sécurité de l'information.
- Aucune des trois municipalités n'a attribué de responsabilités aux employés et aux partenaires en matière de sécurité de leur système de contrôle industriel, et les activités de sensibilisation réalisées sont insuffisantes, notamment parce qu'elles ne répondent pas aux besoins spécifiques en matière de sécurité des systèmes de contrôle industriels.

En ce qui concerne les mesures sécuritaires d'accès aux systèmes de contrôle industriels, nous présentons les exigences, les saines pratiques et les déficiences possibles en la matière. Toutefois, pour des raisons de sécurité et de sensibilité de l'information, les constats et les recommandations formulés, le cas échéant, aux municipalités auditées, ne sont pas diffusés dans le présent rapport.

Sécurité des systèmes de contrôle industriels

Table des matières

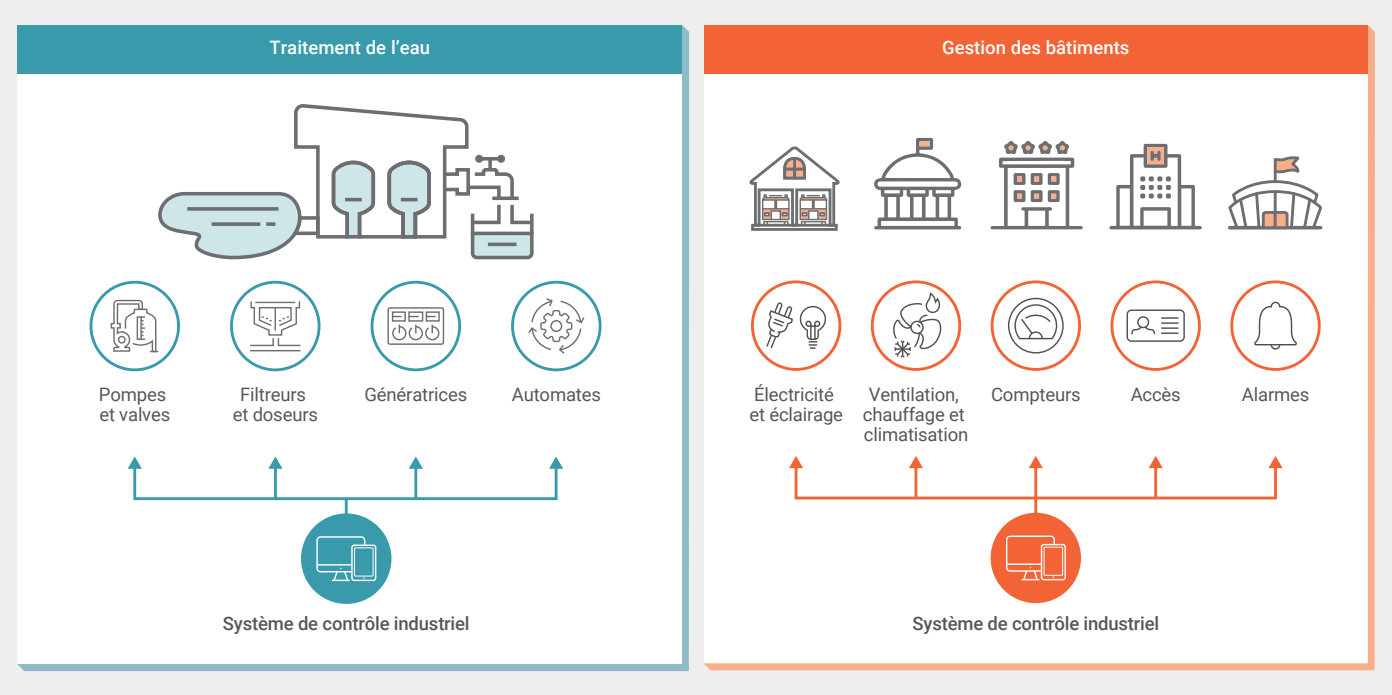
Sigle

SCI	Système de contrôle industriel

01 Mise en contexte

1. Dans le cadre de leurs activités, les municipalités offrent des services de proximité qui contribuent à la mise en place et au maintien d'un milieu de vie adapté aux besoins des citoyens. À cette fin, elles construisent et entretiennent diverses infrastructures, notamment des usines de traitement de l'eau, des bibliothèques, des piscines, des arénas. Pour la gestion de ces infrastructures, les municipalités utilisent différents systèmes de contrôle industriels (SCI), lesquels automatisent et contrôlent les processus industriels et intègrent des équipements et des logiciels de surveillance et de contrôle. La figure 1 présente deux types d'environnement dans lesquels les SCI peuvent intervenir, soit le processus de traitement de l'eau et le processus de gestion des bâtiments municipaux.

Figure 1 Exemples simplifiés d'environnements utilisant des SCI



Système de contrôle industriel

Cette expression désigne un regroupement de plusieurs systèmes, comme des systèmes de contrôle-commande, de télésurveillance, d'acquisition de données, et des automates programmables industriels, regroupement qui assure le fonctionnement et le contrôle des processus industriels.

Selon le *Grand dictionnaire terminologique* du gouvernement du Québec, un automate est une machine conçue pour exécuter sans l'aide d'une personne des opérations déterminées d'avance.

2. Pour le traitement de l'eau, le SCI peut, par exemple, contrôler le blocage de l'analyseur de chlore, la modification du taux d'ozone et le débit d'eau pour remplir ou vider le réservoir. Pour la gestion des bâtiments, le SCI permet, par exemple, le contrôle du système de ventilation, de celui du chauffage, de celui de l'éclairage et de celui des accès aux bâtiments.

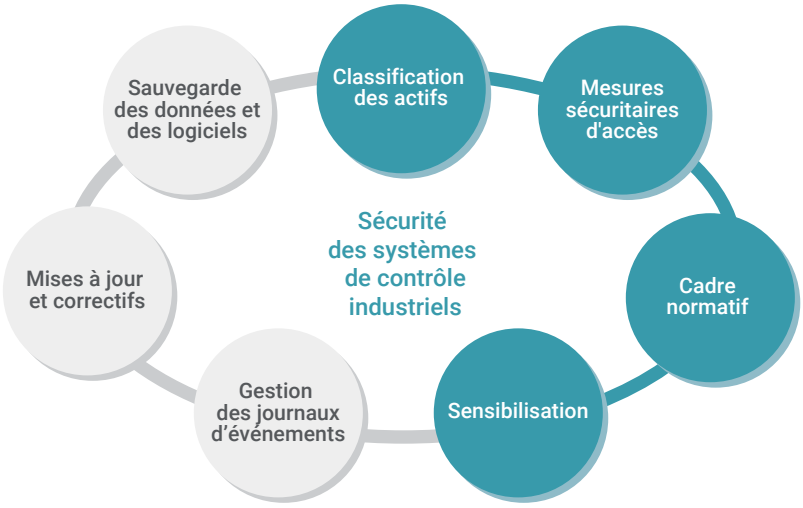
3. Étant donné que les SCI doivent permettre la connectivité avec d'autres systèmes et réseaux ainsi que les interventions à distance, ils intègrent de plus en plus de solutions informatiques. Par conséquent, ils sont susceptibles d'être visés par les mêmes enjeux de sécurité que tout autre système informatique de la municipalité. Toutefois, les SCI comportent des risques différents en cas d'attaques informatiques qui peuvent, entre autres, provoquer des incidents, comme la perturbation des services fournis, ou des événements ayant des conséquences mettant en danger la santé publique ou causant des dommages à l'environnement. Ces incidents risquent également d'engendrer des coûts importants et de porter atteinte à la réputation

de la municipalité. Par conséquent, la sécurité des SCI doit être considérée et intégrée dans le cadre normatif et les activités liées à la sécurité de l'information de la municipalité. Le cadre normatif doit tenir compte des exigences spécifiques aux SCI et à leur environnement.

Mesures de sécurité

4. Afin de réduire la possibilité que des situations susceptibles de compromettre la sécurité des SCI se présentent, la municipalité doit mettre en place différentes mesures de sécurité relatives à la gestion des accès et à la sécurité de leur réseau. En effet, la mise en œuvre de saines pratiques en matière de sécurité des SCI est un préalable incontournable pour que la municipalité puisse atténuer les risques associés aux vulnérabilités des SCI, protéger les actifs et assurer la disponibilité des services qu'elle offre à ses citoyens. La figure 2 présente les éléments à considérer lors de la mise en place des mesures de sécurité quant aux SCI.

Figure 2 Sécurité des systèmes de contrôle industriels[1]



1. Les éléments en gris dans la figure ne sont pas inclus dans la portée de la présente mission d'audit.

Cadre légal et réglementaire

5. Les municipalités sont assujetties à la *Loi concernant le cadre juridique des technologies de l'information*, laquelle prévoit notamment des exigences relatives à l'utilisation sécuritaire des technologies de l'information. De plus, la *Loi sur la sécurité civile* énonce diverses obligations visant la protection des personnes et des biens contre les sinistres. En somme, la sécurité des SCI devrait être prise en compte afin de ne pas provoquer d'incidents mettant en danger les biens, l'environnement ou la santé des personnes.

Municipalités auditées

6. Pour la réalisation de la présente mission d'audit, trois municipalités ont été sélectionnées :

- la Ville de Dollard-Des Ormeaux (Dollard-Des Ormeaux) ;
- la Ville de La Prairie (La Prairie) ;
- la Ville de Rouyn-Noranda (Rouyn-Noranda).

7. Les municipalités ont été sélectionnées parmi celles comptant de 10 000 à 99 999 habitants et pour lesquelles la réalisation des audits de performance a été confiée à la Commission municipale du Québec par règlement en vertu de l'article 108.2.0.2 de la *Loi sur les cités et villes*.

8. Nous présentons ci-dessous certains renseignements sur les municipalités auditées.

	Dollard-Des Ormeaux	La Prairie	Rouyn-Noranda
Loi d'application	*Loi sur les cités et villes*	*Loi sur les cités et villes*	*Loi sur les cités et villes*
Région administrative	Montréal	Montérégie	Abitibi-Témiscamingue
Population (2022)	49 696	26 380	43 092
SCI audité	Gestion des bâtiments	Traitement de l'eau	Traitement de l'eau

Source : Décret de population.

9. Nos travaux d'audit avaient pour objectif de déterminer si les municipalités auditées se sont dotées de mesures de contrôle et de sécurité appropriées en vue de gérer efficacement l'accès aux SCI sélectionnés et d'assurer leur sécurité. Les critères d'évaluation y afférents et la portée des travaux sont présentés à l'annexe 1. Le sommaire des recommandations formulées par la Vice-présidence à la vérification se trouve à l'annexe 2.

10. Les travaux d'audit portaient sur les SCI rattachés aux usines de traitement de l'eau de La Prairie et de Rouyn-Noranda, d'une part, et sur le SCI associé à la gestion des bâtiments municipaux de Dollard-Des Ormeaux, d'autre part. Puisque, dans cette municipalité, une partie des activités en matière de traitement de l'eau potable relève de la Ville de Montréal, nous avons choisi d'auditer une activité réalisée entièrement par la municipalité, soit la gestion des bâtiments.

11. L'attention à apporter à ces SCI par les municipalités s'avère importante, car les usines de traitement de l'eau de La Prairie et de Rouyn-Noranda desservent une grande partie de la population, soit plus de 95 et de 70 % respectivement (logements et locaux commerciaux). Du côté des bâtiments municipaux, c'est l'ensemble de la population de Dollard-Des Ormeaux qui est susceptible de profiter des services qui sont offerts.

Rôles et responsabilités

12. Les rôles et les responsabilités des principaux intervenants relativement à la sécurité de l'information d'une municipalité, notamment ceux liés à la sécurité des SCI, sont présentés dans les paragraphes suivants.

13. Le conseil municipal a notamment pour rôle de veiller à ce que l'offre de services de la municipalité soit en adéquation avec les besoins de sa population, y compris en matière de sécurité et de bien-être. À cette fin, le conseil municipal décide des orientations et des priorités en ce qui a trait à la sécurité de l'information, notamment à la sécurité des SCI, au moyen de règlements et de résolutions en vue de réaliser ses objectifs, le tout dans une perspective de saine administration de la municipalité.

14. Le conseil municipal peut décider de confier à un tiers un contrat pour la gestion complète ou partielle de ses SCI. Le recours aux services d'un cocontractant ne dispense toutefois pas la municipalité des responsabilités qui lui incombent à cet égard.

15. Le directeur général est le premier responsable de la mise en œuvre des orientations du conseil, comme les politiques ou les directives en matière de la sécurité des SCI. Il soutient le conseil dans le développement de ses stratégies et effectue le suivi de l'atteinte des objectifs établis. Ces fonctions sont assumées avec la collaboration des directeurs de services et d'autres fonctionnaires ou d'employés concernés par les SCI.

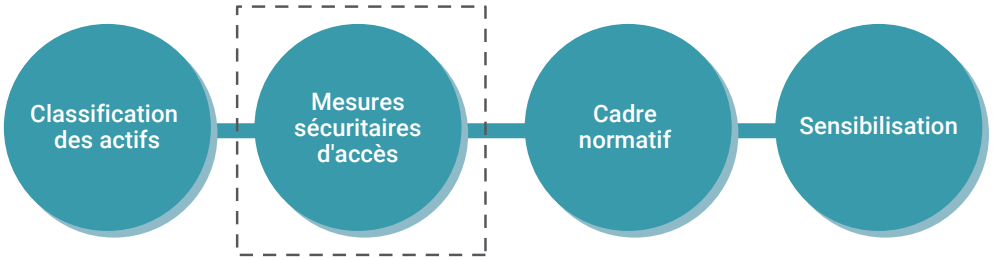
16. Un responsable de la sécurité de l'information peut être désigné, notamment pour faciliter, en collaboration avec le directeur général, l'élaboration du cadre normatif en sécurité de l'information et sa mise en œuvre.

02

Résultats de l'audit

17. Bien que la sécurité des SCI comporte plusieurs éléments, comme le démontre la figure 2, nos travaux et les résultats de notre audit faisant l'objet du présent rapport portent sur la classification des actifs des SCI, les mesures sécuritaires d'accès aux SCI, le cadre normatif de sécurité de l'information et la sensibilisation des utilisateurs des SCI, et ceux, pour les SCI audités (figure 3). Nous présentons, pour chaque section représentée par une bulle, les exigences et les saines pratiques liées au sujet abordé ainsi que les constats et les recommandations formulés à la suite de notre audit. En ce qui concerne la section Mesures sécuritaires d'accès, nous présentons seulement les exigences, les saines pratiques et les déficiences possibles pour permettre à un lecteur intéressé d'approfondir ses connaissances en la matière. Pour des raisons de sécurité et de sensibilité de l'information, si des constats et des recommandations ont été formulés aux municipalités, ils ne sont pas diffusés dans le présent rapport.

Figure 3 Sections du rapport d'audit



18. Le paragraphe qui suit présente la conclusion générale que nous formulons pour l'ensemble des municipalités auditées, et ce, à la lumière de nos travaux. Ce constat est mis en contexte et expliqué en détail dans les sections suivantes.

19. **Les trois municipalités disposent de diverses données sur les actifs des SCI. Cependant, elles ne réalisent aucune classification de ces actifs en fonction de leur sensibilité et de leur caractère critique. En négligeant cette étape, ces municipalités n'ont pas l'assurance qu'elles déploient les mesures de sécurité appropriées afin de diminuer les risques inacceptables. De plus, des éléments d'amélioration à apporter ont été identifiés par rapport à la gestion des accès et à la sécurité du réseau des SCI. Enfin, les cadres normatifs des municipalités auditées sont incomplets et les activités de sensibilisation réalisées sont insuffisantes, notamment parce qu'elles ne répondent pas aux besoins spécifiques en matière de sécurité des SCI.**

2.1 Classification des actifs

20. La classification des actifs des SCI constitue une assise essentielle pour déterminer les mesures de sécurité à mettre en place afin de prévenir, de détecter et de réagir efficacement et adéquatement face aux risques propres à un actif. Pour ce faire, la municipalité doit déterminer ses actifs critiques et sensibles ainsi que le niveau de risque qu'elle choisit d'accepter pour chacun de ces actifs et, de ce fait, entreprendre les actions nécessaires pour réduire les risques qui ne sont pas acceptables.

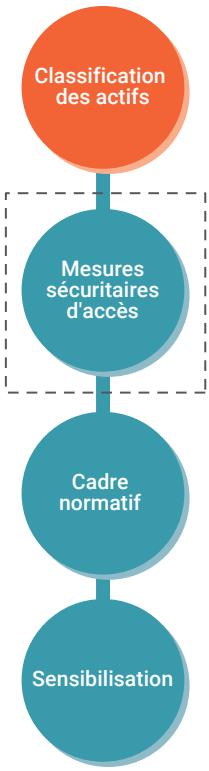
21. Dans le contexte de la sécurité d'un SCI, pour classifier les actifs, la municipalité doit dresser l'inventaire des actifs du SCI, tels que les logiciels, les postes de travail, les automates programmables, les contrôleurs ainsi que le réseau et ses équipements (ex. : serveurs, routeurs). De plus, la représentation schématique du réseau du SCI permet d'identifier les flux d'information internes et externes et la position physique des équipements. Ce schéma permet d'avoir une vision globale du réseau et, ainsi, de déterminer par la suite plus rapidement les risques qui concernent les actifs du SCI, les mesures de sécurité à appliquer afin de diminuer les risques et la gravité de l'événement en cas d'incident.

22. En plus de permettre une identification des actifs critiques et sensibles du SCI à protéger, l'inventaire des actifs peut servir à d'autres fins, par exemple pour des raisons financières et de prise de décision, et ce, tant pour les activités de gestion courante que pour la planification à long terme (ex. : activités d'entretien et de maintenance, planification budgétaire, programme triennal d'immobilisations). Le rapport d'audit portant sur l'information relative à la gestion d'actifs en immobilisations, publié par la Commission municipale du Québec en février 2021, présente des renseignements supplémentaires à ce sujet.

23. La classification, quant à elle, reflète la valeur de chaque actif en fonction de son niveau de sensibilité et de criticité ; le tout s'établit en fonction de trois objectifs de sécurité, soit la confidentialité, l'intégrité, et l'élément généralement le plus important d'un SCI, la disponibilité. La classification est la suite de l'appréciation des risques, qui estime la probabilité qu'un risque se concrétise et la sévérité des effets si cet événement se produisait. Plus particulièrement, l'analyse des risques associés aux actifs d'un SCI doit intégrer l'évaluation des risques physiques et celle des risques liés à la cybersécurité du SCI, et estimer la sévérité des impacts sur les citoyens, l'environnement et les biens de la municipalité.

24. Chaque actif évolue dans un milieu informationnel complexe qui lui est spécifique. Par conséquent, périodiquement, l'inventaire doit être mis à jour et la classification des actifs doit être actualisée au cours de leur cycle de vie.

25. **Les trois municipalités auditées disposent de certaines données sur plusieurs actifs de leurs SCI. Cependant, aucune n'a réalisé d'exercice de classification pour évaluer leur sensibilité et leur caractère critique. Sans cette classification, la municipalité pourrait ne pas avoir identifié tous ses actifs sensibles ou critiques. De ce fait, il pourrait être difficile pour elle de prévenir et de détecter les vulnérabilités de ses actifs et de réagir adéquatement pour mettre en place des mesures de sécurité et ainsi assurer notamment la disponibilité du SCI.**



Contrôleur

Aux fins du présent rapport, un contrôleur est un dispositif électronique faisant partie des systèmes de contrôle de chauffage, de ventilation, d'air climatisé, d'éclairage, d'accès et de sécurité des bâtiments, qui réagit automatiquement afin de réguler une variable contrôlée.

Actif critique d'un SCI

Aux fins du présent rapport, un actif critique d'un SCI est un actif dont la défaillance peut entraîner des conséquences liées directement à la sécurité humaine et environnementale, à la perte d'équipements et à la perturbation des services fournis par la municipalité.

Réseau informatique

Un réseau informatique est un ensemble d'équipements reliés entre eux par le biais de connexions et de protocoles de communication afin de permettre l'échange d'information.

Aux fins du présent rapport, le réseau informatique du SCI sera nommé « réseau du SCI », et le réseau informatique de la municipalité, excluant le réseau informatique du SCI, sera nommé « réseau de la municipalité ». L'utilisation seule du terme « réseau » renvoie à la notion générale de réseau informatique.

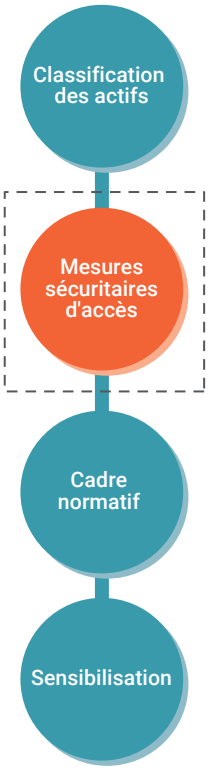
26. La Prairie et Rouyn-Noranda ont inventorié en partie les actifs liés à l'infrastructure du réseau de la municipalité. Pour leur SCI, elles ont compilé certaines données sur les équipements et leur entretien. Cependant, une partie des actifs des SCI n'a pas été inventoriée. Pour sa part, Dollard-Des Ormeaux utilise un logiciel de gestion des actifs qui permet d'avoir un inventaire en temps réel des actifs présents sur le réseau de la municipalité. Pour le SCI, l'inventaire contient seulement la liste de certains équipements et logiciels utilisés pour la gestion des bâtiments.

27. Bien que le personnel reconnaisse que certains actifs sont critiques en termes de disponibilité des SCI (ex. : automates pour les SCI de traitement de l'eau, génératrices pour le SCI de gestion des bâtiments), aucune classification des actifs en fonction de leur sensibilité et de leur caractère critique n'a été réalisée par les trois municipalités auditées. Sans appréciation des risques, les actifs sensibles ou critiques pourraient ne pas être protégés adéquatement.

RECOMMANDATION

À toutes les municipalités auditées

1. Inventorier et classifier les actifs du SCI en fonction de leur caractère critique et de leur sensibilité en termes de disponibilité, d'intégrité et de confidentialité, afin d'identifier les actifs critiques et de déployer des mesures de sécurité adéquates pour protéger ces actifs.



2.2 Mesures sécuritaires d'accès

28. Pour des raisons de sensibilité de l'information, comme nous l'avons spécifié dans l'introduction de la section Résultats de l'audit, seules les saines pratiques et les déficiences possibles sont publiées dans la présente sous-section.

29. Afin de réduire les risques rattachés aux menaces liées au SCI et de protéger les ressources les plus critiques, la municipalité doit mettre en œuvre les mesures requises pour atténuer les risques à un niveau qu'elle considère comme acceptable et faire en sorte que ces mesures soient efficaces pour que la gestion des accès et du réseau du SCI soit sécuritaire.

Gestion des accès

30. Au moyen d'une gestion des accès efficace, la municipalité assure une protection de première ligne en matière de sécurité de l'information. Plus particulièrement, la mise en place d'un processus efficace de gestion des accès au SCI permet à la municipalité de protéger les actifs du SCI en restreignant les accès non autorisés aux réseaux, aux logiciels et aux équipements, et en limitant les possibilités qu'une action inappropriée soit réalisée de façon volontaire ou non. Après avoir déterminé la criticité et la sensibilité de ses actifs, la municipalité devrait déterminer quelles sont les mesures de protection à instaurer relativement aux accès logiques et physiques au SCI.

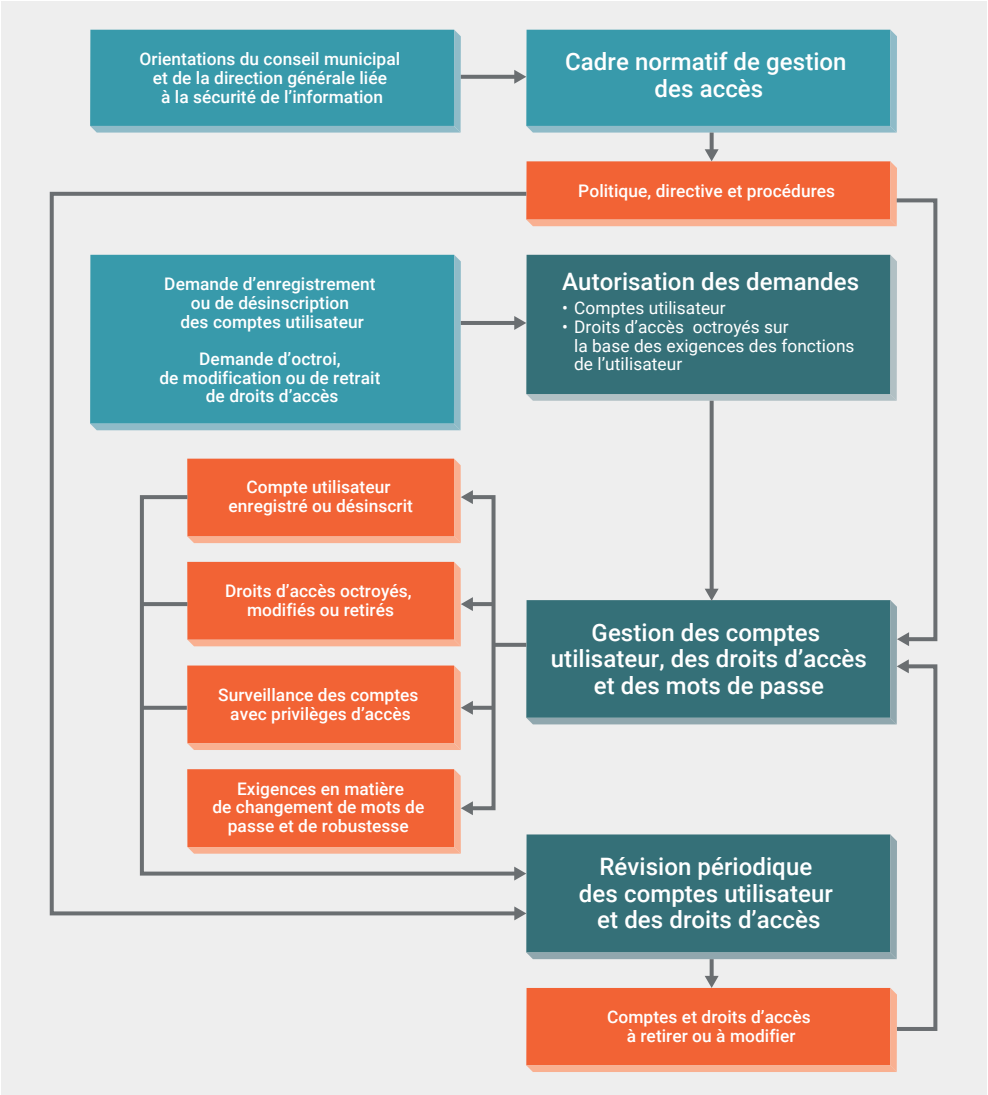
31. La gestion des accès est le processus qui permet notamment à la municipalité d'accepter ou de refuser une demande d'accès logique ou physique aux actifs du SCI et, ainsi, de s'assurer que seulement les utilisateurs autorisés accèdent au réseau, aux logiciels, aux équipements et aux locaux du SCI, et que leurs accès se limitent aux actifs qu'ils ont besoin de connaître et d'utiliser.

32. Pour que les contrôles d'accès logiques et physiques soient adéquatement mis en place et exercés, il est primordial que la municipalité mette en œuvre un processus formel, uniforme et efficace de gestion des accès au SCI. Un tel processus aide à garantir qu'aucune étape dans la gestion des accès n'est oubliée (ex. : retrait ou modification des accès), et que les étapes ne sont pas accomplies de façon inadéquate ou par des intervenants inappropriés. Le processus de gestion des accès ne doit pas s'appliquer seulement aux processus administratifs. En effet, vu l'importance des services offerts par la municipalité par l'entremise du SCI, il est essentiel que le processus de gestion des accès au SCI fasse partie intégrante de la gestion générale des accès logiques et physiques de la municipalité.

Gestion des accès logiques au SCI

33. Dans le but de maintenir et de gérer les systèmes industriels, les utilisateurs ont besoin d'un accès pour se connecter au réseau du SCI et des accès aux différents logiciels de celui-ci. Ces accès se nomment « accès logiques ». Les étapes relatives au processus général de la gestion des accès logiques aux réseaux et aux logiciels des SCI sont présentées dans la figure 4.

Figure 4 Processus général de gestion des accès logiques



Source : Cette figure s'inspire du *Guide de gestion des accès logiques* du Secrétariat du Conseil du trésor.

Compte utilisateur

Aux fins du présent rapport, un compte utilisateur inclut l'information dont un utilisateur a besoin pour se connecter au réseau de la municipalité ou à celui du SCI, ou à un logiciel du SCI.

Droit d'accès logique

Le droit d'accès logique est le droit qui permet à un utilisateur, d'accéder à un système et de lire, de modifier, de supprimer, de transmettre ou d'approuver.

Accès régulier

L'accès régulier est l'accès standard nécessaire à un utilisateur pour accéder à un système.

Accès privilégié

L'accès privilégié est l'accès qui donne des pouvoirs élargis (ex. : modifier la sécurité des systèmes, les caractéristiques des mots de passe, l'accès à de l'information sensible, et octroyer ainsi que modifier des accès aux systèmes informatiques).

34. Toutes les déficiences dans la gestion des accès logiques au réseau et aux logiciels des SCI augmentent les risques d'accès non autorisés et de compromission des actifs des SCI. Certaines déficiences possibles sont présentées ci-dessous.

Compte générique

Un compte générique est un compte qui n'appartient pas à un utilisateur en particulier et dont plusieurs utilisateurs se servent.

	Déficience possible	Impact et information complémentaire
Compte utilisateur	Utilisation de comptes génériques	◆ Confidentialité du mot de passe non respectée (connu par plusieurs utilisateurs, d'où risque d'accès non autorisés) ◆ Difficulté à relier les utilisateurs à leurs actions et à les rendre imputables ◆ Utilisation non recommandée, en particulier pour les comptes utilisateur dotés de privilèges importants, à moins d'une contrainte opérationnelle majeure ◆ Limitation, précise et bien documentée, de l'usage de comptes génériques, lorsqu'indispensable
	Comptes non supprimés ou bloqués immédiatement lors du départ ou de la réaffectation d'un utilisateur	◆ Personnes non autorisées accédant au réseau ou aux logiciels, les moyens d'accès ayant été conservés
Droits d'accès logiques	Droits d'accès octroyés sans autorisation	◆ Personnes non autorisées accédant au réseau ou aux logiciels et les utilisant
	Droits d'accès octroyés non en lien avec les fonctions de l'utilisateur	◆ Accès excédant les permissions requises pour effectuer le travail (principe du droit d'accès minimal non respecté) – Accès privilégié octroyé alors qu'un accès régulier suffit – Accès octroyé non utilisé ◆ Accès non cohérent avec d'autres accès de l'utilisateur, le principe de séparation des tâches incompatibles étant non respecté (ex. : vérification d'une action accomplie dans le système par la même personne ayant réalisé l'action)
	Absence de révocation ou de modification des accès lors du départ ou de la réaffectation d'un utilisateur	◆ Personnes non autorisées accédant au réseau ou aux logiciels et les utilisant, les moyens d'accès ayant été conservés

	Déficience possible	Impact et information complémentaire
Mot de passe	Mot de passe non requis	◆ Information confidentielle ou fonctionnalités des SCI pouvant servir à des utilisateurs non autorisés
	Mot de passe non choisi par l'utilisateur Aucune exigence pour changer le mot de passe par défaut à la première connexion	◆ Mot de passe pouvant être utilisé par les administrateurs pour avoir accès de façon non autorisée
	Mot de passe avec faibles exigences de complexité (non robuste) Absence d'historique des mots de passe, donc sans limite de réutilisation Aucune exigence pour changer périodiquement le mot de passe	◆ Intrusion ou action non autorisée à risque accru, mot de passe étant soit facile à deviner, soit inchangé depuis la création du compte création du compte
	Mot de passe de groupe, associé à un compte générique, inchangé lors du départ ou de la réaffectation d'un utilisateur	◆ Personnes accédant au réseau ou aux logiciels et les utilisant, malgré leur départ ou leur réaffectation
Connexion au réseau	Nombre illimité de tentatives de connexion infructueuses, sans verrouiller le compte utilisateur Absence de fermeture de session après une période d'inactivité	◆ Connexion au poste de travail d'un autre utilisateur et usage non autorisé de ce poste

Mot de passe de groupe

Le mot de passe de groupe est le mot de passe associé à un compte générique et connu par plusieurs utilisateurs.

Gestion des accès physiques au SCI

35. Au niveau des accès physiques au SCI, la municipalité devrait protéger les locaux où les équipements industriels sont installés (ex. : automates, contrôleurs, génératrices) et sécuriser, dans la mesure du possible, ces équipements dans des armoires ou des salles fermées à clé, ainsi que protéger les serveurs du SCI dans des salles fermées et verrouillées. Ces mesures permettent de contrôler les accès physiques afin de s'assurer que seul le personnel autorisé accède à ces locaux et aux équipements.

36. Le contrôle des accès physiques aux locaux, aux serveurs du réseau et aux installations du SCI devrait faire partie des préoccupations de la municipalité. Les SCI sont habituellement plus vulnérables aux attaques physiques, vu l'étendue de leur emplacement et leurs dimensions. En présence de déficiences en matière de sécurité logique (ex. : absence de fermeture de session sur un poste de travail), le contrôle et la sécurité des accès physiques sont d'autant plus importants et peuvent permettre de compenser certaines failles de sécurité logique.

37. Les déficiences possibles dans la gestion des accès physiques aux serveurs du réseau, aux postes de travail, aux équipements et aux locaux des SCI augmentent les risques d'accès non autorisés et de compromission des actifs des SCI. Certaines déficiences sont présentées ci-dessous.

	Déficience possible	Impact et information complémentaire
Droits d'accès physiques	Contrôle d'accès physique inadéquat (ex. : local non verrouillé, sans carte ou code d'accès)	◆ Personnes non autorisées accédant aux serveurs du réseau, aux postes de travail et aux installations (contrôle insuffisant)
	Absence de révocation ou de modification des accès physiques lors du départ ou de la réaffectation d'un utilisateur Code unique d'accès aux locaux techniques inchangé lors du départ ou de la réaffectation d'un utilisateur	◆ Personnes non autorisées accédant aux serveurs du réseau, aux postes de travail et aux installations, les moyens d'accès (ex. : clés, cartes ou codes d'accès) ayant été conservés

Révision et surveillance des accès au SCI

38. Par l'entremise de la révision et de la surveillance des accès logiques et physiques au SCI, la municipalité corrige des déficiences reliées aux accès non autorisés et diminue ainsi les risques de compromission des actifs du SCI. Certaines déficiences possibles sont présentées ci-dessous.

	Déficience possible	Impact et information complémentaire
Révision des accès	Absence de révision ou révision non périodique des comptes utilisateur ainsi que des accès logiques et physiques danslecasd'unchangement de situation	◆ Personnes non autorisées accédant aux réseaux et aux installations, les moyens d'accès (ex. : comptes et droits d'accès, clés ou des cartes d'accès) ayant été conservés ◆ Vérifications alors nécessaires pour identifier par exemple les droits d'accès pour un utilisateur ayant quitté ou ayant été réaffecté, les droits d'accès octroyés sans autorisation, les droits d'accès octroyés différents de ceux autorisés, les droits d'accès excessifs (droit minimal non respecté), les droits d'accès incompatibles (séparation des tâches non respectée)
Surveillance	Absence de surveillance ou surveillance inefficace des comptes utilisateur avec accès privilégiés (ex. : journalisation des activités ou révision des journaux absentes) Surveillance absente ou inefficace des accès physiques (ex. : aucun système de traçabilité électronique des accès physiques ou de journalisation des présences physiques)	◆ Présence de comptes utilisateur avec accès privilégiés non autorisés, non documentés ou non surveillés ◆ Personnes non autorisées accédant physiquement aux serveurs du réseau et aux installations ◆ Difficulté à relier les utilisateurs à leurs actions et à les leur imputer

Sécurité du réseau du SCI

39. Une menace importante susceptible de nuire à la sécurité du réseau du SCI est le risque de cyberattaque. Ce risque pourrait potentiellement permettre à une personne malveillante d'altérer le fonctionnement normal du système, d'endommager les actifs critiques du SCI ou, encore, d'accéder à de l'information sensible et de l'extraire de. Puisque ces menaces sont de plus en plus présentes, des coûts importants pour la municipalité peuvent être engendrés en raison par exemple de demandes de rançon ou des coûts de remise en fonction des équipements.

40. De surcroît, la gestion et la maintenance à distance sont des pratiques courantes, les employés ainsi que les partenaires étant amenés à se connecter davantage aux réseaux des SCI. La connexion à distance augmente considérablement les vulnérabilités du système à cause de l'utilisation potentielle de réseaux externes non sécuritaires. Les interconnexions du réseau du SCI avec le réseau de la municipalité et les réseaux externes, notamment Internet, élargissent les possibilités d'attaque des installations industrielles et des infrastructures critiques. Il est donc important de cloisonner le réseau du SCI et de sécuriser les connexions à distance au réseau du SCI.

Cloisonnement du réseau du SCI

Cloisonnement

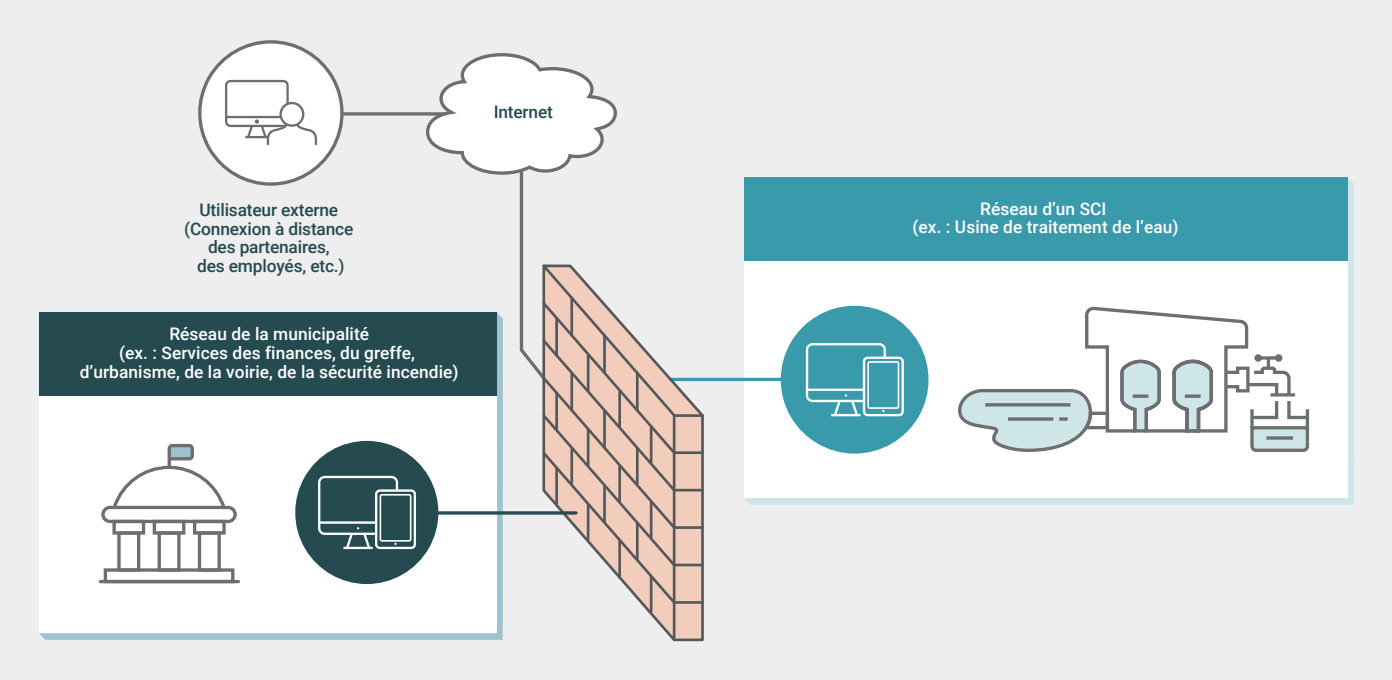
Le cloisonnement des réseaux informatiques peut être comparé à une valve d'étanchéité permettant d'isoler un système par rapport à un autre et de laisser passer seulement les éléments permis. Autrement dit, il s'agit d'une mesure de sécurité qui permet de séparer un réseau en groupes de composantes physiques et logiques qui partagent les mêmes ressources, et de mettre en place des mesures de sécurité entre les groupes pour n'autoriser que les flux d'information nécessaires à leur fonctionnement.

41. Lorsqu'un réseau informatique n'est pas cloisonné par rapport aux autres réseaux, chaque ordinateur (poste de travail) connecté à un réseau pourrait avoir accès à n'importe quel autre ordinateur connecté à d'autres réseaux. Ainsi, la compromission de l'un d'eux met alors à risque tous les ordinateurs connectés. Par exemple, en l'absence de cloisonnement, si une personne malveillante compromet un ordinateur du réseau de la municipalité, elle peut ensuite attaquer les serveurs critiques ou d'autres ordinateurs du réseau du SCI.

42. Le cloisonnement permet de restreindre l'accès à l'information sensible, aux équipements et aux ordinateurs et de rendre l'intrusion considérablement plus difficile pour un attaquant informatique, et empêche un accès non permis du réseau de la municipalité au réseau du SCI et vice-versa. Pour cette raison, il est indispensable de cloisonner le réseau du SCI par rapport aux autres réseaux de la municipalité ainsi qu'aux réseaux externes, comme Internet, à l'aide de mesures de sécurité.

43. Le cloisonnement assure la protection du périmètre entre les réseaux, minimise l'exposition aux risques et bloque les attaques, le tout sans perturber les processus critiques. La figure 5 représente un exemple de cloisonnement du réseau d'un SCI de manière simplifiée.

Figure 5 Exemple de cloisonnement du réseau d'un SCI



44. Plus particulièrement, des mesures de sécurité qui permettent le cloisonnement, telles que le filtrage des flux d'information par pare-feu, les listes de contrôle d'accès, les antivirus, les postes d'administration dédiés, devraient être mises en place afin d'empêcher les connexions non autorisées et de protéger l'information sensible. De plus, les points communs d'accès entre les réseaux devraient être limités au minimum et être bien documentés. Enfin, les mesures de sécurité en matière de connexion à distance au réseau, telles que le chiffrement des flux, ont un impact sur l'efficacité du cloisonnement.

45. Les déficiences possibles en lien avec le cloisonnement augmentent les risques d'accès non autorisés et de compromission des actifs des SCI. Certaines déficiences possibles sont présentées ci-dessous.

Chiffrement des flux

Il s'agit d'une méthode de sécurité qui permet de protéger la confidentialité et l'intégrité de l'information (document ou donnée) pendant sa transmission et son entreposage. Ce chiffrement génère une clé pour chiffrer les données numériques et les rend ainsi illisibles pour toute personne n'ayant pas accès à la clé de déchiffrement. Par conséquent, les parties non autorisées ne peuvent pas y avoir accès.

	Déficience possible	Impact et information complémentaire
Cloisonnement	Réseau du SCI non cloisonné par rapport au réseau de la municipalité	◆ Risque de compromission du réseau du SCI ou du réseau de la municipalité mal sécurisés, par exemple s'il y a absence du contrôle des points communs d'accès des deux réseaux : – par une personne malveillante par le biais d'un des deux réseaux – par un employé, soit par mégarde ou volontairement (ex. : collecte de données confidentielles) ◆ Absence de mesures de sécurité, telles que le filtrage des flux d'information par pare-feu, les listes de contrôle d'accès des antivirus, le chiffrement des flux, les postes d'administration dédiés, d'où augmentation du risque d'intrusion à partir du réseau de la municipalité et vice-versa, c'est-à-dire risque de compromission du réseau de la municipalité par le biais du réseau du SCI
	Réseau du SCI non cloisonné par rapport aux réseaux externes, notamment Internet	◆ Risque de compromission des postes de travail et des serveurs du SCI causé par l'accès d'un utilisateur interne à un site Web non sécurisé ◆ Absence des mesures de sécurité mentionnées précédemment, d'où augmentation du risque de cyberattaques associé à la disponibilité du réseau du SCI à partir des réseaux externes

Connexion à distance au réseau

Compte individuel

Un compte individuel est un compte relié à un seul utilisateur.

Authentification multifacteur

Il s'agit d'un mécanisme qui permet de vérifier et de valider plusieurs facteurs d'identité d'un utilisateur lors de la connexion à distance au réseau informatique. Il est recommandé d'utiliser au moins deux facteurs d'authentification de catégorie différente : connaissance (ex. : mot de passe), possession (ex. : jeton d'authentification) ou inhérence (ex. : empreinte digitale).

46. Les interconnexions du réseau du SCI avec les partenaires et les employés devraient assurer la confidentialité, l'intégrité et l'authenticité des échanges. Donc, les connexions à distance aux systèmes devraient être examinées et évaluées rigoureusement en fonction des risques. Afin d'assurer la sécurité, l'utilisation des comptes individuels à authentification multifacteur et du chiffrement des flux lors des connexions à distance pour restreindre l'accès non autorisé aux actifs du SCI sont à considérer selon les niveaux de criticité et de sensibilité des systèmes.

47. Les déficiences possibles en lien avec les connexions à distance augmentent les risques d'accès non autorisés et de compromission des actifs des SCI. Certaines déficiences possibles sont présentées ci-dessous.

	Déficience possible	Impact et information complémentaire
Connexion à distance au réseau	Utilisation des comptes génériques pour la connexion à distance	◆ Absence de confidentialité du mot de passe liée à sa circulation parmi plusieurs utilisateurs et risque d'accès non autorisées ◆ Difficulté à relier les utilisateurs à leurs actions et à les leur imputer
	Absence d'authentification multifacteur pour les connexions à distance des partenaires et des employés	◆ Augmentation du risque lié à l'usurpation de l'identité d'un utilisateur légitime par un attaquant (ce dernier accède ainsi au SCI pour y faire des actions non autorisées)
	Absence du chiffrement des flux lors de la connexion à distance	◆ Confidentialité et intégrité des données échangées non assurées
	Utilisation par les partenaires et les employés d'un logiciel de connexion à distance à sécurité faible	◆ Risque d'accès non autorisé à un poste de travail ou au serveur du réseau, notamment lié à la vulnérabilité du mot de passe utilisé lors de la connexion à distance

48. Comme spécifié précédemment, pour des raisons de sécurité et de sensibilité de l'information, si des constats et des recommandations ont été formulés aux municipalités auditées pour la section *Mesures sécuritaires d'accès*, ils ne sont pas diffusés dans le présent rapport.

2.3 Cadre normatif de la sécurité de l'information

49. L'élaboration de politiques, de directives, de processus ou de procédures en matière de sécurité de l'information, l'ensemble étant nommé ci-après « cadre normatif », et la mise en œuvre de ce dernier, y compris les mesures relatives aux SCI, constituent un gage de succès en ce qui a trait à la protection des actifs informationnels d'une municipalité.

50. En effet, par l'entremise d'un cadre normatif en matière de sécurité de l'information, une municipalité peut, entre autres, déterminer ses orientations, ses objectifs, ses exigences ainsi que les rôles et les responsabilités des utilisateurs des actifs informationnels. Ce cadre doit également prévoir toutes les mesures de sécurité visant à tenir compte du contexte particulier du SCI afin de diminuer les risques qui y sont associés. À titre d'exemple, le processus de gestion des accès devrait inclure non seulement la gestion des accès au réseau et aux logiciels de la municipalité, mais également la gestion des accès liée au réseau et aux logiciels du SCI, et prendre en considération son environnement spécifique.

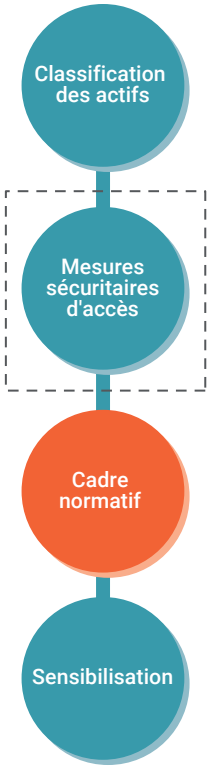
51. En plus de prévoir les rôles et responsabilités des employés et des partenaires de la municipalité, il est tout indiqué de prévoir dans le cadre normatif la désignation d'un responsable de la sécurité de l'information et des documents spécifiques portant sur la sécurité de l'information, tout en considérant l'environnement spécifique du SCI. Par exemple, la procédure sur la gestion des accès logiques et physiques devrait tenir compte de la gestion des accès au SCI, et la procédure sur la classification des actifs informationnels devrait tenir compte de celle des actifs du SCI. L'annexe 3 présente les avantages d'inclure ces éléments dans un cadre normatif en matière de sécurité de l'information.

52. Il convient de souligner que l'adoption d'une politique en sécurité de l'information par le conseil municipal favorise la mise en œuvre des mesures qui y sont prévues ainsi que l'atteinte des objectifs y afférents.

53. De plus, la municipalité devrait réviser périodiquement son cadre normatif pour refléter notamment les changements opérationnels et technologiques ainsi que l'évolution des risques, particulièrement ceux liés au SCI, et s'assurer que les mesures de sécurité prévues dans le cadre sont toujours appropriées.

54. Enfin, le cadre normatif devrait être le véhicule d'information à privilégier pour informer le personnel de la municipalité. Les exigences qu'il contient devraient également être diffusées aux intervenants externes. Par exemple, lorsque la municipalité fait appel à un fournisseur de services informatiques, elle devrait s'entendre avec ce fournisseur sur les modalités de sécurité de l'information à respecter afin de limiter les risques découlant d'un accès aux actifs du SCI par un tiers.

55. **Les trois municipalités auditées n'ont pas défini formellement leurs objectifs et leurs exigences en matière de sécurité de l'information ou de sécurité des SCI afin notamment d'orienter toutes les activités relatives à la sécurité de l'information. De plus, les municipalités de Dollard-Des Ormeaux et de La Prairie n'ont pas désigné formellement de responsable en matière de sécurité de l'information. Aucune des trois municipalités n'a attribué de responsabilités en matière de sécurité de leur SCI aux employés et aux partenaires. Ainsi, les employés et les partenaires pour les SCI ne sont pas clairement informés des exigences auxquelles ils devraient répondre.**



Cadre normatif de la sécurité de l'information

Aux fins du présent rapport, le cadre normatif de la sécurité de l'information est constitué d'un ensemble de politiques, de directives, de processus et de procédures qui permettent la mise en place de saines pratiques en matière de sécurité de l'information.

56. Les constats relevés au cours de cet audit démontrent l'importance pour les municipalités de se doter d'un cadre normatif de sécurité adéquat pour les SCI, notamment pour préciser leurs exigences en matière de sécurité.

57. Plus particulièrement, Rouyn-Noranda n'a pas défini de politiques, de directives, de processus ou de procédures en matière de sécurité de l'information. Dollard-Des Ormeaux et La Prairie, quant à elles, ont défini dans des documents certaines exigences à respecter en matière de sécurité de l'information. Cependant, ces documents ne ciblent qu'une partie seulement des saines pratiques à mettre en place pour assurer la sécurité de l'information et aucun des documents ne traite des aspects de sécurité spécifiques à leur SCI. À titre d'exemple, le processus de gestion des accès logiques et physiques aux SCI et les règles entourant les interventions des fournisseurs sur les actifs des SCI sont absents de ces documents.

58. De plus, les trois municipalités n'ont pas convenu formellement avec les partenaires qui interviennent sur les SCI des exigences à respecter à l'égard de la sécurité des SCI.

59. Enfin, Rouyn-Noranda a formellement désigné un responsable en matière de sécurité de l'information. À Dollard-Des Ormeaux, la responsabilité de la sécurité du réseau informatique est reconnue et prise en charge par un cadre de la municipalité. Cependant, la responsabilité de la sécurité de l'information, incluant la sécurité du SCI de gestion des bâtiments, n'est pas reconnue et assignée formellement. Pour La Prairie, deux cadres reconnaissent avoir la responsabilité en matière de sécurité de l'information de la municipalité, mais aucun n'a été désigné formellement comme responsable et la description de leurs rôles et responsabilités n'en fait pas état.

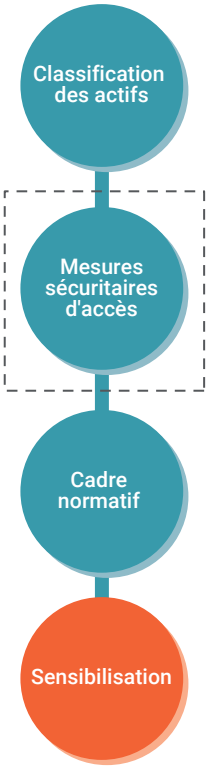
RECOMMANDATIONS

À toutes les municipalités auditées

◢ *2.* Établir un cadre normatif complet portant sur la sécurité de l'information en considérant notamment le contexte spécifique du SCI et en assurer la mise en place.

À Dollard-Des Ormeaux et à La Prairie

◢ *3.* Désigner formellement un responsable en matière de sécurité de l'information afin de faciliter l'élaboration du cadre normatif, la mise en œuvre des mesures prévues, dont celles afférentes au SCI, ainsi que l'atteinte des objectifs y afférents.



2.4 Sensibilisation des utilisateurs

60. La mise en place de toutes les saines pratiques présentées dans les sections précédentes n'assure pas la sécurité de l'information si ces pratiques ne sont pas appliquées adéquatement et de façon systématique par les employés et les partenaires d'une municipalité. La sécurité de l'information de la municipalité passe par la sensibilisation de ses employés et la mise en place d'un programme d'activités de sensibilisation. De même, il convient de sensibiliser à la sécurité de l'information l'ensemble des partenaires qui intervient sur les systèmes d'information de la municipalité. L'objectif est notamment de s'assurer que tous les utilisateurs sont adéquatement informés des exigences de la municipalité en matière de sécurité, qu'ils sont conscients de leurs responsabilités en cette matière, qu'ils les assument et qu'ils respectent les exigences. Le niveau de sensibilisation à la sécurité devrait correspondre à leurs fonctions dans la municipalité.

61. La sensibilisation à la sécurité de l'information devrait inclure des thèmes spécifiques destinés à certains utilisateurs, comme les employés et partenaires qui interviennent sur les SCI de traitement de l'eau ou de gestion des bâtiments.

62. Les activités planifiées dans le programme de sensibilisation des employés devraient prévoir des activités récurrentes à échéance régulière, de manière à ancrer solidement les notions véhiculées et d'inclure les nouveaux employés. Il est également indiqué de prévoir dans le programme de sensibilisation des mécanismes de suivi (ex. : retour sur l'activité, rétroaction) auprès des employés qui ont participé à ces activités. En plus de permettre à la municipalité de s'assurer que tous les employés ont participé à l'activité et que les objectifs sont atteints, la mise en place d'un mécanisme de suivi permet de recueillir les commentaires des participants et d'optimiser le programme de sensibilisation.

63. Ce programme devrait d'ailleurs être actualisé régulièrement pour rester cohérent avec le cadre normatif portant sur la sécurité de l'information de la municipalité, les changements opérationnels et technologiques et l'évolution des risques.

64. **Les trois municipalités auditées ont mis en place une ou plusieurs activités de sensibilisation portant sur certains risques liés à la sécurité de l'information. Cependant, ces activités ne tiennent pas compte des aspects spécifiques des SCI. Les trois municipalités auditées n'ont pas établi de programme structuré d'activités réservé aux employés en matière de sensibilisation à la sécurité de l'information. De plus, aucune municipalité n'a sensibilisé l'ensemble de ses partenaires qui intervient sur les SCI concernant la sécurité de ces derniers. Enfin, pour La Prairie et Rouyn-Noranda, les activités de sensibilisation réalisées ne visaient pas l'ensemble des employés des SCI.**

65. Plus particulièrement, les activités de sensibilisation réalisées portaient sur certains risques liés à la sécurité de l'information, notamment la cybersécurité, et étaient orientées sur la sécurité des réseaux des municipalités. Ces dernières auraient avantage à sensibiliser l'ensemble des employés des SCI aux risques liés à la sécurité de ceux-ci, afin que les employés connaissent et comprennent les risques de sécurité qui peuvent compromettre les SCI et les saines pratiques à adopter pour les protéger.

66. En ce qui concerne la sensibilisation des partenaires à la sécurité des SCI, les municipalités n'ont pas pu démontrer que l'ensemble de leurs partenaires qui interviennent sur les SCI a reçu les documents existants contenant les exigences à respecter en matière de sécurité de l'information.

67. Enfin, aucun mécanisme de suivi ou de retour sur les activités de sensibilisation réalisées auprès des employés n'a été fait par Dollard-Des Ormeaux et Rouyn-Noranda, alors que La Prairie a demandé à ses gestionnaires de faire un suivi auprès des employés.

RECOMMANDATIONS

À toutes les municipalités auditées

- *4.* Élaborer un programme d'activités de sensibilisation sur la sécurité de l'information adaptées au contexte du SCI, établir la fréquence, la stratégie de diffusion, la nature ainsi que le suivi de ces activités en s'assurant de joindre tous les employés du SCI.
- *5.* S'assurer que les partenaires qui interviennent sur le SCI sont sensibilisés en matière de sécurité du SCI.

Commentaires des municipalités auditées

Les municipalités auditées ont eu l'occasion de transmettre leurs commentaires officiels, qui sont reproduits dans la présente section. Nous tenons à souligner qu'elles ont adhéré à toutes les recommandations.

Ville de Dollard-Des Ormeaux

« Nous avons pris connaissance du rapport d'audit de performance sur la « Sécurité des systèmes de contrôle industriels » et nous l'accueillons très favorablement.

« Ce rapport constitue un outil précieux car il détaille de quelle façon la sécurité des systèmes de contrôle industriels doit être considérée et intégrée dans les cadres normatifs et les activités liées à la sécurité de l'information de notre ville. Il nous aura permis de nous questionner et de revoir certains processus. Une liste claire et bien documentée de recommandations a été formulée et nous nous engageons à l'implanter. Nous avons d'ailleurs déjà débuté par la création d'un comité dont le mandat est d'établir la politique de sécurité informatique.

« Cet audit nous permettra également d'augmenter nos standards de vigilance afin de réduire les risques d'intrusion avec les autres systèmes en place et ceux que nous allons acquérir prochainement.

« En conclusion, nous souhaitons remercier sincèrement l'équipe qui a réalisé cet audit pour son professionnalisme, sa perspicacité et sa rigueur. »

Ville de La Prairie

« La ville de La Prairie a pris connaissance du rapport d'audit de performance sur la sécurité des systèmes de contrôle industriels, et a l'intention de corriger les points ayant été soulevés. Tel que cité à même le rapport, certaines recommandations sont d'ailleurs déjà en place.

« Finalement, la ville tient à remercier l'équipe de la CMQ ayant participé à cet audit pour leur professionnalisme. Le fruit de leur travail ne peut être que constructif pour l'ensemble des municipalités. »

Ville de Rouyn-Noranda

« La Ville de Rouyn-Noranda a pris acte des constats et recommandations émises dans le présent audit de performance.

« La Ville de Rouyn-Noranda prend très au sérieux la question de la sécurité et ne lésinera pas sur les efforts afin de mettre en place les recommandations et encore plus. Par conséquent, la Ville de Rouyn-Noranda a déjà mis en place un plan d'action afin de se conformer au présent audit et par le fait même d'améliorer ses façons de faire.

« La Ville de Rouyn-Noranda tient à remercier la Commission municipale du Québec pour son travail de qualité et de son professionnalisme tout au long du mandat. »

ANNEXES

ANNEXE 1

À propos de l'audit

La responsabilité de la Vice-présidence à la vérification de la Commission municipale du Québec consiste à exprimer une conclusion sur l'objectif de l'audit. Pour ce faire, 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 critères se fondent principalement sur les saines pratiques de gestion liées à l'activité auditée, lesquelles s'appuient sur les mesures de réduction des risques proposées notamment par le Centre canadien pour la cybersécurité. Ces mesures incluent celles relatives au contrôle et à la sécurité pertinentes aux SCI.

OBJECTIF DE L'AUDIT

Objectif

Déterminer si des mesures de contrôle et de sécurité appropriées sont déployées afin d'assurer l'efficacité du processus de gestion des accès et la sécurité des systèmes de contrôle industriels sélectionnés.

Critères d'évaluation

1. Les systèmes de contrôle industriels sont pris en compte adéquatement dans le cadre normatif mis en place en matière de sécurité, lequel précise notamment les rôles et responsabilités des intervenants.
2. Des activités de sensibilisation sont réalisées afin de minimiser les risques propres à ces systèmes.
3. Les actifs sont identifiés et classifiés en fonction de leur sensibilité et de leur caractère critique.
4. Des mesures de sécurité permettant de protéger les systèmes de contrôle industriels sont mises en place, dont le cloisonnement du réseau, les connexions au réseau dédiées aux partenaires et l'accès physique aux serveurs et aux locaux techniques.
5. Des mesures de sécurité efficaces en matière de gestion des identités et des accès sont mises en place.

Les travaux d'audit dont traite ce rapport ont été menés en vertu de *la Loi sur la Commission municipale* et conformément aux méthodes de travail en vigueur à la Vice-présidence à la vérification. Ces méthodes respectent les Normes canadiennes de missions de certification (NCMC) présentées dans le *Manuel de CPA Canada – Certification*, notamment la norme sur les missions d'appréciation directe (NCMC 3001).

De plus, la Vice-présidence à la vérification applique la Norme canadienne de contrôle de qualité (NCCQ1) du *Manuel de CPA Canada – Certification*. Ainsi, elle maintient un système de contrôle de qualité qui comprend des normes internes documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. Au cours de ses travaux, la Vice-présidence à la vérification se conforme aux règles sur l'indépendance et aux autres règles prévues dans son code de déontologie, lesquelles reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

ANNEXE 1

PORTÉE DES TRAVAUX

Les municipalités que nous avons auditées sont la Ville de Dollard-Des Ormeaux, la Ville de La Prairie et la Ville de Rouyn-Noranda. Nos travaux d'audit portent plus particulièrement sur la sécurité et la gestion des accès à l'égard des systèmes de contrôle industriels de traitement de l'eau de La Prairie et de Rouyn-Noranda et du système de contrôle industriel de gestion des bâtiments de Dollard-Des Ormeaux. Cette distinction s'explique ainsi : pour Dollard-Des Ormeaux, une partie des activités en matière de traitement de l'eau relevant de la Ville de Montréal, nous avons choisi d'auditer une activité réalisée entièrement par la municipalité auditée, soit la gestion des bâtiments.

Afin de mener à bien ces travaux, nous avons obtenu de l'information auprès des représentants de chacune des municipalités auditées, nous avons également analysé divers documents et procédé à certaines observations des SCI. Il est à noter que la réalisation de tests d'intrusion et de vulnérabilité n'est pas un procédé d'audit inclus dans la portée de la présente mission d'audit.

Nos travaux se sont déroulés principalement de juillet 2021 à avril 2022. Notre audit a porté principalement sur les activités de la période du 1er janvier au 31 août 2021. Toutefois, certaines de nos observations peuvent avoir trait à des situations antérieures ou postérieures à cette période.

Le présent rapport a été achevé le 11 octobre 2022.

ANNEXE 2

Sommaire des recommandations

Nous présentons ci-dessous les recommandations formulées dans le présent rapport par la Vice-présidence à la vérification aux municipalités auditées. S'il y a lieu, d'autres recommandations propres aux mesures sécuritaires d'accès ont été formulées et communiquées aux municipalités auditées concernées.

	Recommandation	Dollard-Des Ormeaux	La Prairie	Rouyn-Noranda
1.	Inventorier et classifier les actifs du SCI en fonction de leur caractère critique et de leur sensibilité en termes de disponibilité, d'intégrité et de confidentialité, afin d'identifier les actifs critiques et de déployer des mesures de sécurité adéquates pour protéger ces actifs.	◆	◆	◆
2.	Établir un cadre normatif complet portant sur la sécurité de l'information en considérant notamment le contexte spécifique du SCI et en assurer la mise en place.	◆	◆	◆
3.	Désigner formellement un responsable en matière de sécurité de l'information afin de faciliter l'élaboration du cadre normatif, la mise en œuvre des mesures prévues, dont celles afférentes au SCI, ainsi que l'atteinte des objectifs y afférents.	◆	◆	
4.	Élaborer un programme d'activités de sensibilisation sur la sécurité de l'information adaptées au contexte du SCI, établir la fréquence, la stratégie de diffusion, la nature ainsi que le suivi de ces activités en s'assurant de joindre tous les employés du SCI.	◆	◆	◆
5.	S'assurer que les partenaires qui interviennent sur le SCI sont sensibilisés en matière de sécurité du SCI.	◆	◆	◆

ANNEXE 3

Éléments à considérer pour établir un cadre normatif de la sécurité de l'information et leurs avantages (incluant les SCI)

Élément	Avantages
Désignation d'un responsable de la sécurité de l'information	◆ Prévoir la désignation formelle d'un responsable de la sécurité de l'information à la municipalité facilite l'élaboration du cadre normatif, la prise en charge des orientations, des objectifs et des exigences liés au cadre normatif et l'attribution des responsabilités en matière de sécurité de l'information aux responsables des actifs et aux utilisateurs.
Rôles et responsabilités des utilisateurs	◆ Une définition claire et une diffusion des rôles et des responsabilités des utilisateurs en matière de sécurité de l'information, qui tiennent compte du caractère spécifique des SCI, permettent de s'assurer que tous les intervenants connaissent leurs tâches et les exigences de la municipalité en la matière, diminuent les risques liés à la sécurité des SCI et favorisent l'imputabilité des utilisateurs.
Lignes directrices sur la classification des actifs	◆ Le cadre normatif devrait prévoir des lignes directrices pour encadrer le processus de classification des actifs informationnels en tenant compte des actifs des SCI afin d'assurer que : – l'inventaire est dressé et maintenu à jour ; – les actifs sensibles ou critiques ont été identifiés et des mesures de sécurité ont été mises en place pour les protéger ; – les responsables des actifs sont désignés.
Gestion des comptes utilisateur, des droits d'accès logiques et des mots de passe	◆ Le cadre normatif devrait prévoir des lignes directrices pour encadrer le processus de gestion des comptes utilisateur, des droits d'accès logiques et des mots de passe, processus qui devrait comprendre les accès aux logiciels et au réseau des SCI. L'objectif est de permettre un meilleur contrôle des accès et de protéger les actifs informationnels, notamment en prévoyant : – les droits d'accès à attribuer aux utilisateurs en fonction de leur poste, tout en s'assurant du respect des droits d'accès minimaux et de la séparation des tâches incompatibles, et la documentation afférente ; – une révision périodique ainsi qu'une surveillance des droits d'accès, plus particulièrement ceux des droits d'accès privilégiés ; – des exigences liées à la robustesse et aux changements des mots de passe.
Gestion des accès physiques	◆ Le cadre normatif devrait prévoir des lignes directrices pour encadrer le processus de gestion des accès physiques aux SCI afin d'établir les exigences en matière de sécurité et les façons de procéder, telles que : – la limitation de l'accès aux utilisateurs autorisés ; – les conditions et les restrictions d'utilisation liées à l'équipement et à l'environnement physique lors de la gestion à distance ; – le contrôle et la restriction des accès des fournisseurs ; – la récupération des clés, des jetons ou des cartes d'accès au départ d'un employé ; – le changement des codes d'alarme aux bâtiments abritant des SCI ; – la journalisation et la vérification des accès aux locaux.

ANNEXE 4

Constats et recommandations portant sur les mesures sécuritaires d'accès – Annexe confidentielle

Le cas échéant, les constats et les recommandations formulés concernant les mesures sécuritaires d'accès aux systèmes de contrôle industriels ne sont pas diffusés dans le présent rapport pour des raisons de sécurité et de la sensibilité de l'information.

Commission municipale Québec

La saine gestion au bénéfice de tous