*Office of the Auditor General / Bureau du vérificateur général*

# AUDIT OF INTERNET AND EMAIL USAGE POLICIES AND PROCEDURES

# 2010

# VÉRIFICATION DES POLITIQUES ET PROCÉDURES CONCERNANT L'UTILISATION DES SERVICES D'INTERNET ET DU COURRIEL

# Table of Contents / Table des matières

1 INTRODUCTION ..... 1
2 AUDIT SCOPE, OBJECTIVES AND APPROACH ..... 1
3 DETAILED FINDINGS, OBSERVATIONS AND RECOMMENDATIONS ..... 2
3.1 Responsible Computing Policy ..... 2
3.2 Records Management Policy and Record Retention and Disposition Schedule ..... 4
3.3 Information Management/Information Technology Security Policy ..... 6
3.4 City of Ottawa Information Management/Information Technology Security Standards v1.10 ..... 7
4 CONCLUSION ..... 9
5 ACKNOWLEDGEMENT ..... 9

1 INTRODUCTION ..... 11
2 PORTÉE, OBJECTIFS ET APPROCHE DE LA VÉRIFICATION ..... 11
3 CONSTATATIONS DÉTAILLÉES, OBSERVATIONS ET RECOMMANDATIONS ..... 13
3.1 Politique sur l'utilisation responsable des ordinateurs ..... 13
3.2 Politique sur la gestion des documents et calendrier de conservation et de destruction des documents ..... 14
3.3 Politique sur la gestion de l'information/sécurité de la technologie de l'information ..... 16
3.4 Normes de la gestion de l'information/sécurité de la technologie de l'information de la Ville d'Ottawa v1.10 ..... 18
4 CONCLUSION ..... 20
5 REMERCIEMENTS ..... 20

# 1 INTRODUCTION

During the course of the 2010 Follow-up to the 2005 Audit of Internet Usage and Controls, it was determined that a separate audit report on Internet and email usage policies and procedures would be issued.

This audit was therefore added to the 2010 Audit Plan of the Office of the Auditor General.

# 2 AUDIT SCOPE, OBJECTIVES AND APPROACH

The objective of this audit is to evaluate the Internet and email usage policies and procedures that regulate this corporate tool.

The scope of analysis included:

- Responsible Computing Policy;
- Appendix A: Website Blocking Standard;
- Appendix B: Electronic Messaging Guidelines;
- Appendix C: Data Logging Standard;
- Records Management Policy and Records Retention and Disposition Schedule;
- Information Management/Information Technology Security Policy; and,
- City of Ottawa Information Management/Information Technology Security Standards v1.10.

All of the above documents have been analyzed and compared against the general controls contained in ISO 27002:2005 international standard and other best practice repositories such as CobiT (CobiT - DS 5) and the Val IT framework.

The contents of the Responsible Computing Policy and its appendices were compared to the controls of ISO 27002 as a baseline.

ISO 27002:2005 contains 12 domains (or clauses, as the standard defines them) that normally should be covered in any organization, all depending on the needs and selected controls that answer most to the organization's needs in terms of information security.

The 12 domains are:

1. **Risk assessment –** general requirements for risk assessment and treatment;
2. **Security policy** - management direction and commitment to information security;
3. **Organization of information security** - governance of information security at the enterprise level;

4. **Asset management** - inventory and classification of information assets;
5. **Human resources security** - security aspects for HR management;
6. **Physical and environmental security** - protection of the computer facilities;
7. **Communications and operations management** - management of technical security controls in systems and networks;
8. **Access control** - restriction of access rights to networks, systems, applications, functions and data;
9. **Information systems acquisition, development and maintenance** - building security into applications;
10. **Information security incident management** - anticipating and responding appropriately to information security breaches;
11. **Business continuity management** - protecting, maintaining and recovering business-critical processes and systems;
12. **Compliance** - ensuring conformance with information security policies, standards, laws and regulations.

The section on CobiT DS 5 "Ensure Systems Security" defines the general governance requirements for the management of information security and could be used as a governance level guide for the implementation of an information security management process. CobiT is not a standard and its use remains for consulting purposes, as a complement to ISO 27002:2005. The same applies to Val IT, it is a guide for business optimization of the IT function of organizations and will be used as a guide rather than a mandatory document.

# 3 DETAILED FINDINGS, OBSERVATIONS AND RECOMMENDATIONS

## *3.1 Responsible Computing Policy*

Currently, the City of Ottawa Responsible Computing Policy (RCP) is up to date, with the last review having taken place on January 6, 2010. The three appendices to the RCP, (Website Blocking Standard; Electronic Messaging Guidelines; and, Data Logging Standard) focus on specific aspects of Internet and email usage and management. The RCP is a governance document and its requirements are mandatory for all information technology users of the City of Ottawa.

The RCP is in conformity with industry practices for this type of document. The level of compliance to ISO 27002:2005 may vary depending on an organization's needs, and the requirements and scope of the RCP are adequate to suit the City of Ottawa's needs. The City should however clarify what kind of non-business use of these resources it will permit.

The use of computing resources has to be specified as being for business purposes only, or for personal use purposes (as specified in point 2.3 of the RCP) only if there are no productivity impacts. As an example, we may cite restriction of the use of personal email or newsgroups to only lunchtime or outside of working hours.

Currently, "incidental" use is permitted, but this is open to wide interpretation. All City of Ottawa users are required to comply with the RCP and the IM/IT Department has control of the information technology resources that the City offers to its employees.

The Responsible Computing Policy is the main document that guides the use of information technology resources at the City of Ottawa. Other documents, such as the IM/IT Security Policy and Security Standards, are more specific to certain aspects, such as adherence to security controls and their application by IT staff, and the technology solutions that are used by the City in general.

Generally, the City of Ottawa Internet and email usage policies, which are within the scope of this analysis, are in conformity with ISO 27002:2005 specifications and controls.

At the present time, the use of a risk assessment methodology is mentioned in the Responsible Computing Policy, IM/IT Security and the Security Standards. Risk assessment methodologies are: OCTAVE, MEHARI, ISO 27005, etc. We accepted that the City developed its own practice and the City should ensure that any change, implementation, development and new process is analysed for the security risks it may pose to the whole infrastructure and to the existing processes, as well as to the information processed by the City's information resources.

The ITS Department utilizes a modified Royal Canadian Mounted Police (RCMP) risk assessment process to evaluate all technology projects. This high-level risk assessment process provides for the ability to highlight those projects that may be of a higher risk, which in turn allows the Department to focus resources to mitigate the associated risks. In 2010, the ITS Department conducted five of these high level assessments.

## 3.2 Records Management Policy and Record Retention and Disposition Schedule

The Records Management Policy (RMP) was updated on April 6, 2010. It is based on CAN/CGSB 72.34-2005 "Electronic Documents as Documentary Evidence" and complies with City regulations and by-laws, and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The Record Retention and Disposition Schedule is an internal document that defines retention terms for corporate records.

Presently, the email system is not an official business records repository according to Records Management Policy, (p. 12, "Policy Requirements" section) and as such, email correspondence is deleted periodically. In general, records of email traffic are only maintained for a three month period. In some cases, emails that have been deleted cannot be restored, even within this three month period. Email traffic logs are retained for 12 months; email content within an individual's mailbox is retained for three months.

Email traffic logs, according to the evidence provided by the City, do not contain any email body or content record whatsoever. As mentioned further, only the email messages (as an equivalent of paper mail) can be considered records. These records have to be archived applying the same security controls as the regular mail.

As the traffic logs cannot be considered email records, the retention period stays at three months. Another aspect is deleted email. It should be moved to the deleted email folder and not permanently deleted. These requirements arise from the City's obligations as a juridical entity that respects the Municipal Freedom of Information and Protection of Privacy Act (as noted in the Records Management Policy) and Records Retention and Disposition By-law.

Only separate email messages could be considered official records according to the conditions specified in the Records Management Policy.

Email traffic logs cannot be considered full records. As stated previously, emails (separate email messages) only can be considered as records. According to the Records Retention and Disposition Schedule the general files of the majority of the subject contents (Column 2) have a retention period of three years and an absolute majority has a retention period of at least 1 year. This means, in our understanding, that the business related email correspondence, according to RCP and RCP Appendix B 'Electronic messaging guidelines' has to comply with the Records Retention and Disposition By-law.

A review of the retention schedule is recommended in order to ensure a longer time span for the retention of the City's email correspondence. The implications of a shorter retention period are multiple; the most evident being the deletion of activity evidence and documents that might have been transmitted by email. Considering that legal, financial, accounting and other types of documents might be transmitted by email, the Records Retention and Disposition Schedule could apply, and those specified retention periods would have to be respected. Where legal, financial, accounting and other types of documents are transmitted by email, the Records Retention and Disposition Schedule does apply. In order to preserve an activity trail of email correspondence, a retention period of three to five years is recommended, in conformity with the Records Retention and Disposition Schedule for written correspondence. An email archiving tool might be considered in order to facilitate records management.

This illustrates that the email may and in many cases is used for sending all kinds of sensitive information that falls under one or more categories of the Records Retention and Disposition Schedule. Thus, in order to ensure the application of the said Schedule and By-law that enables it, the emails have to be preserved as corporate correspondence, even deleted email. By doing this, the IT/IM Department will comply with City's own By-law.

There is no commonly accepted standard or law that indicates a specific term for email retention, however given the difficulty of filtering official and unofficial email, it is a common industry practice to preserve whole email correspondence in order to ensure appropriate corporate records management. If the IT/IM Department is able to propose a way to filter business and non-business email with a comfortable level of assurance, then it could be discussed internally and proposed to senior management for approval and eventually accepted into production.

## Recommendation 1

**That the City review the existing three month retention period for emails, including deleted emails, to ensure it is sufficient. Both legal and IT requirements should be considered.**

### Management Response

Management agrees with this recommendation.

Management will review the existing three month retention period for emails considering both legal and IT requirements, and will provide a report on this subject to the IT Sub-Committee by the end of Q4 2011.

## 3.3 Information Management/Information Technology Security Policy

The Information Management/Information Technology Security Policy is a document produced to ensure the protection of information transmitted over the City network. It is intended for those users that are responsible for the provision and administration of information technology services. General users are not subject to the IT/IM Security Policy as it covers risk management safeguards and defines elements of information security that are to be ensured for data on the City's network.

The current RCP notion for IT assets covers hardware equipment only. Recognizing software as an IT asset will ensure that it is managed and protected in the same way as hardware.

Currently, some information transmitted on corporate handheld and mobile devices does not go through the City network system. (PIN to PIN and SMS messages are not logged on the corporate network as per the Responsible Computing Policy.) If corporate records are sent PIN to PIN, there may be no record of this data on the City network. Corporate records should not therefore be communicated PIN to PIN. All emails and documents transmitted on laptops, tough books, and smart phones go through the City's email network. Voice calls made through corporate handheld and mobile devices have key transaction artefacts logged such as the number and time.

For those using handhelds and mobile devices, email correspondence leaves the corporate network (the telephone provider is not part of the City network). This means that it is not under the full control of the IT/IM Department. Thus, a specific section or policy intended for those who carry corporate handhelds may need to be put in place. By doing this, the City ensures that handheld and smartphone users are aware that those devices hold sensitive information and due care and due diligence should apply.

Also, the increased use of mobile devices creates unique security risks, including the risk of unauthorized access to data. There is also greater risk that information of a private nature may be accessed by unauthorized persons.

The most obvious example of a unique security risk is the loss of an unlocked handheld. This does not mean that the IT/IM Department creates the risk, but that the enacting of a policy requiring the handhelds to be locked in all times could be necessary.

Management indicates that the Responsible Computing Policy and the City of Ottawa's Code of Conduct govern the use of these mobile devices. Handheld and mobile devices are configured in the same manner as City laptops. This configuration includes: encryption of data at arrest and in transmission, password protection of the device, lock down to prohibit the installation of unauthorized software, and remote wiping for lost/stolen devices.

The use of staff's own personal mobile devices while in the workplace is also an emerging issue. We recommend that management proactively deal with the growing use of staff's own personal mobile devices while at work by establishing and enforcing an appropriate policy.

### Recommendation 2

**That the City formalize and include in the Responsible Computing Policy an extended notion of IT assets to include software.**

#### Management Response

Management agrees with this recommendation.

The Responsible Computing Policy will be updated to include the addition of software as a City of Ottawa information technology asset by the end of Q3 2011.

## *3.4 City of Ottawa Information Management/Information Technology Security Standards v1.10*

The City of Ottawa Information Management/Information Technology Security Standards v1.10 is intended to clarify aspects of the IM/IT Security Policy, and to detail and complete the policy specifications.

Requirements and statements contained within the documents that were reviewed are of no use if not reinforced and user compliance monitored. The purpose of policies is to protect the City's IT network as a vital service, and to educate the users in order to optimize the use of equipment and services over the network. In order to ensure that policies are adhered to, users should be notified any time there are monitoring and control tools filtering and analyzing the use of the City's resources. Ideally, permanent monitoring should be in place, and management should decide the consequences resulting from policy violation.

This relates to the fact that as per discussions held with management, it was stated that filtering and protection equipment is used mainly in reaction to incidents and violations. In order to ensure the application of security controls and best practices, permanent monitoring is an obvious option that will permit the identification of behaviour or incident patterns in a timely manner.

It should be mentioned that Internet and email monitoring tools are currently used for incident monitoring and not for operational usage monitoring. Operational monitoring of user activity would provide a better understanding of Internet and email usage on the City network, but that will necessitate a change of view on monitoring. The City could decide on this change of principle and act accordingly to implement it.

Operational usage monitoring is strongly related to permanent monitoring and means allowing resources for overseeing user activity on a permanent basis, not only in case of incidents. The 'operational usage monitoring' will permit a better security position for the City and will ensure security controls contained in the RCP and its appendices, standards and procedures are applied and respected in all times.

Currently, the IM/IT Security standards have not been updated or reviewed since November 3, 2008. The IM/IT Security Policy has not been updated since January 25, 2007. Security standards, as stated in Section 3.3, are to be developed as the City's IT environment and network change. In order to document these changes, and offer a security view on the technologies and processes, the standards need to be updated on a regular basis.

The Security Policy should be reviewed at least on a yearly basis, and should take into account the development and evolution of the IT function. If no changes are needed, a review and re-approval process should take place and the policy should be re-issued to the user community as a reminder of the City's efforts in that regard.

Improved monitoring and control tools usage would mean a regular analysis of user activity in order to ensure compliance to the RCP and other security policy documents at the City. No specific action and end state can be proposed here because it would mean a more thorough evaluation. Otherwise, tools that perform monitoring and control exist at the City (e.g., Websense, Promodag) and others may be implemented depending on management's decisions to improve the City's security position. Optimised use of existing tools, their update, operational monitoring (as stated earlier) may be considered before changing the existing architecture.

During the course of the audit in December 2010, ITS put in place an intrusion prevention and security information and event management service. ITS has contracted a Canadian based managed security service provider that provides 24/7 monitoring of our web-facing services (Ottawa.ca, etc.) and other critical components of the network. During the course of the audit, we had indicated to ITS that monitoring and control tools usage over the City's network should be improved. In our opinion, this new contract helps to address this issue.

### Recommendation 3

**That the City keep Security Standards up to date and review the policies at least on a yearly basis.**

#### Management Response

Management agrees with this recommendation.

A review of the Security Standards will be incorporated into the ITS Department annual operational plans, and an initial review will be undertaken by the end of Q2 2012.

# 4 CONCLUSION

Generally, corporate email and Internet policies are in accordance with industry practices, however some areas require attention. Specifically, the retention period of corporate emails needs to be reviewed. Also, the use of handheld and mobile devices needs to be addressed to ensure that this information is captured in the corporate records system.

# 5 ACKNOWLEDGEMENT

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.

# 1 INTRODUCTION

Au cours du suivi de 2010 sur la vérification de l'utilisation d'Internet et des contrôles de 2005, il a été déterminé qu'un rapport de vérification distinct sur les politiques et les procédures concernant l'utilisation des services d'Internet et du courriel serait émis.

Cette vérification a donc été ajoutée au plan de vérification 2010 du Bureau du vérificateur général.

# 2 PORTÉE, OBJECTIFS ET APPROCHE DE LA VÉRIFICATION

L'objectif de cette vérification est d'évaluer les politiques et les procédures sur l'utilisation des services d'Internet et du courriel régissant cet outil d'entreprise.

La portée de l'analyse comprenait :

- la Politique sur l'utilisation responsable des ordinateurs;
- l'annexe A : norme sur le blocage de site Web;
- l'annexe B : lignes directrices sur la messagerie électronique;
- l'annexe C : norme sur la collecte de données;
- la Politique sur la gestion des dossiers et le calendrier de conservation et de destruction des dossiers;
- la Politique sur la gestion de l'information/sécurité de la technologie de l'information;
- les normes de la gestion de l'information/sécurité de la technologie de l'information de la Ville d'Ottawa v1.10.

Tous les documents susmentionnés ont été analysés et comparés aux contrôles généraux dont il est question dans la norme internationale ISO 27002:2005 et d'autres répertoires de pratiques exemplaires, comme le CobiT (CobiT -DS 5) et le Val IT.

Le contenu de la Politique sur l'utilisation responsable des ordinateurs et ses annexes a été comparé aux contrôles de l'ISO 27002 comme ligne de référence.

L'ISO 27002:2005 contient ainsi 12 domaines (ou articles, comme la norme les définit) qui devraient être normalement couverts par tout organisme, en fonction des besoins et des contrôles sélectionnés qui répondent à la majorité des besoins d'un organisme en matière de sécurité de l'information.

Les 12 domaines sont les suivants :

1. **Évaluation du risque –** exigences générales d'évaluation et de traitement du risque;

2. **Politique de sécurité –** orientation et engagement de la direction envers la sécurité de l'information;
3. **Organisation de la sécurité de l'information** - gouvernance de la sécurité de l'information au niveau de l'entreprise;
4. **Gestion des biens –** inventaire et classification des actifs informatiques;
5. **Sécurité liée aux ressources humaines –** aspects de la sécurité pour la gestion des RH;
6. **Sécurité physique et environnementale** - protection des installations d'informatique;
7. **Gestion des communications et des activités –** gestion des contrôles techniques de sécurité dans les systèmes et les réseaux;
8. **Contrôle d'accès** - restriction des droits d'accès aux réseaux, aux systèmes, aux applications, aux fonctions et aux données;
9. **Acquisition, développement et maintenance des systèmes d'information –** intégration de la sécurité dans les applications;
10. **Gestion des incidents liés à la sécurité de l'information –** anticipation et réponse appropriée aux violations de la sécurité de l'information;
11. **Gestion de la continuité des affaires –** protection, maintenance et rétablissement des processus et des systèmes d'affaires essentiels;
12. **Conformité –** assurance de la conformité aux politiques, aux normes, aux lois et aux règlements en matière de sécurité de l'information.

La section de CobiT DS 5, « Assurer la sécurité des systèmes » définit les exigences de gouvernance générales en matière de gestion de la sécurité de l'information et pourrait être utilisée comme guide de gouvernance pour la mise en œuvre d'un processus de gestion de la sécurité de l'information. Le CobiT n'est pas une norme et est réservé à des fins de consultation, comme complément à l'ISO 27002:2005. Le même principe s'applique à Val IT, qui est un guide sur l'optimisation des affaires de la fonction de TI des organismes, et qui sera utilisé comme guide et non comme un document obligatoire.

# 3 CONSTATATIONS DÉTAILLÉES, OBSERVATIONS ET RECOMMANDATIONS

## *3.1 Politique sur l'utilisation responsable des ordinateurs*

Actuellement, la Politique sur l'utilisation responsable des ordinateurs (URO) de la Ville d'Ottawa est à jour, la dernière révision ayant été effectuée le 6 janvier 2010. Les trois annexes de cette politique (norme sur le blocage de site Web; lignes directrices sur la messagerie électronique; norme sur la collecte de données) sont axées sur des aspects précis de la gestion et de l'utilisation d'Internet et du courriel. La Politique sur l'URO est un document de gestion et tous les utilisateurs de la technologie de l'information de la Ville d'Ottawa sont tenus d'en respecter les exigences.

La Politique sur l'URO est conforme aux pratiques de l'industrie pour ce type de document. Le niveau de conformité à l'ISO 27002:2005 peut varier selon les besoins d'une organisation, et les exigences et la portée de la Politique sur l'URO répondent adéquatement aux besoins de la Ville d'Ottawa. La Ville devrait cependant clarifier le type d'utilisation non professionnelle de ces ressources qu'elle permettra.

L'utilisation des ressources informatiques doit être précisée comme étant réservée aux activités professionnelles seulement, ou pour une utilisation personnelle (tel que précisé au point 2.3 de la Politique sur l'URO) seulement si elle n'a pas d'incidence sur la productivité. Par exemple, nous pourrions citer des restrictions sur l'utilisation du courriel personnel ou de forums de discussion seulement lors des heures de dîner ou en dehors des heures de travail.

Présentement, l'utilisation « fortuite » est permise, mais ceci donne lieu à une interprétation trop large. Tous les utilisateurs de la Ville d'Ottawa doivent se conformer à la Politique sur l'URO et le service de la GI/TI a le contrôle des ressources informatiques que la Ville offre à ses employés.

La Politique sur l'utilisation responsable des ordinateurs est le document principal qui sert de guide pour les ressources informatiques à la Ville d'Ottawa. D'autres documents, comme la Politique sur la sécurité de la GI/TI et les normes de sécurité, portent sur des aspects plus spécifiques, comme le respect des contrôles de sécurité et de leur application par le personnel de la TI, et les solutions technologiques utilisées par la Ville en général.

Habituellement, les politiques sur l'utilisation d'Internet et du courriel de la Ville d'Ottawa, qui relèvent de la portée de cette analyse, sont conformes aux spécifications et aux contrôles de l'ISO 27002:2005.

Au moment présent, l'utilisation d'une méthodologie d'évaluation du risque est mentionnée dans la Politique sur l'utilisation responsable des ordinateurs et dans les normes de sécurité et de sécurité de la GI/TI. Les méthodologies d'évaluation du risque sont les suivantes : OCTAVE, MEHARI, l'ISO 27005, etc. Nous avons

accepté que la Ville développe ses propres pratiques et elle devrait s'assurer que tout changement, développement, nouveau processus et toute mise en œuvre soient analysés pour les risques de sécurité qu'ils pourraient poser à l'infrastructure et aux processus actuels ainsi qu'à l'information traitée par les ressources d'information de la Ville.

Le service de l'information de la technologie utilise un processus d'évaluation du risque modifié de la Gendarmerie royale du Canada (GRC) pour évaluer tous les projets de technologie. Ce processus d'évaluation du risque de haut niveau permet de mettre en lumière les projets pouvant représenter un risque plus élevé, qui à son tour, permet au service de concentrer des ressources pour atténuer les risques connexes. En 2010, le service de l'information de la technologie a mené cinq de ces évaluations de haut niveau.

## *3.2 Politique sur la gestion des documents et calendrier de conservation et de destruction des documents*

La Politique sur la gestion des documents (PGD) a été mise à jour le 6 avril 2010. Elle est fondée sur la CAN/CGSB 72.34-2005 « Enregistrements électroniques – Preuve documentaire » et est conforme aux règlements et aux lois municipales ainsi qu'à la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP). Le calendrier de conservation et de déclassement des documents est un document interne qui établit les modalités de conservation des documents de l'entreprise.

Présentement, le système de courriels n'est pas un répertoire de documents d'affaires officiels selon la Politique sur la gestion des documents (p. 12, section « Exigences de la politique ») et à ce titre, la correspondance par courriel est supprimée périodiquement. De manière générale, les fichiers de courriels envoyés ne sont conservés que pendant trois mois. Dans certains cas, les courriels qui ont été supprimés ne peuvent pas être récupérés, même dans la période de trois mois. Des registres de courriels envoyés et reçus sont conservés pendant 12 mois; le contenu des courriels dans la boîte de réception d'une personne est conservé trois mois.

Les registres de courriels envoyés, en fonction de preuves fournies par la Ville, ne contiennent aucun corps de message ni de fichier de contenu quelconque. Comme il est mentionné plus loin, seuls les messages courriel (comme un équivalent d'un courrier papier) peuvent être considérés comme des documents. Ces documents doivent être archivés selon les mêmes contrôles de sécurité que le courrier normal.

Puisque les registres de courriels envoyés ne peuvent pas être considérés comme des fichiers de courriel, la période de conservation est toujours de trois mois. Un autre aspect vise les courriels supprimés, qui devraient être déplacés dans le fichier des courriels supprimés et non être supprimés de façon permanente. Ces exigences découlent des obligations de la Ville comme personne morale qui respecte la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP) (tel que

mentionné dans la Politique sur la gestion des documents) et le Règlement municipal sur la conservation et le déclassement des documents.

Seuls les messages courriel séparés pourraient être considérés comme des documents officiels selon les conditions précisées dans la Politique sur la gestion des documents.

Les registres de courriels envoyés ne peuvent pas être considérés comme des documents complets. Comme il a été mentionné auparavant, seuls les courriels (messages séparés) peuvent être considérés comme des documents. Selon le calendrier de conservation et de déclassement des documents, les documents généraux de la majorité des contenus (colonne 2) sont conservés pendant trois ans, et une majorité absolue est conservée pendant au moins un an, ce qui signifie, de ce que nous comprenons, que la correspondance d'affaires par courriel doit être conforme au Règlement municipal sur la conservation et le déclassement des documents selon la Politique sur l'utilisation responsable des ordinateurs et son annexe B intitulée Lignes directrices sur la messagerie électronique.

Un examen du calendrier de conservation est recommandé afin d'assurer une période de temps plus longue pour la conservation des correspondances par courriel de la Ville. Les répercussions d'une période de conservation plus courte sont multiples, la plus évidente étant la suppression de la preuve et de documents sur les activités pouvant avoir été transmis par courriel. En prenant en considération que des documents légaux, financiers et comptables ainsi que d'autres types de documents peuvent être transmis par courriel, le calendrier de conservation et de déclassement pourrait s'appliquer, et les périodes de conservation devraient alors être respectées. Dans les cas où des documents légaux, financiers et comptables ainsi que d'autres types de documents sont transmis par courriel, le calendrier de conservation et de déclassement des documents s'applique. Afin de garder un suivi des activités de correspondances par courriel, une période de conservation de trois à cinq ans est recommandée, conformément au calendrier de conservation et de déclassement des documents en matière de correspondance écrite. Un outil d'archivage des courriels peut être considéré afin de faciliter la gestion des documents.

Ceci illustre le fait que le courriel peut être utilisé pour envoyer toutes sortes de renseignements sensibles relevant d'une ou de plusieurs catégories du calendrier de conservation et de déclassement des documents et que, dans bien des cas, il l'est. Ainsi, pour assurer l'application dudit calendrier et du règlement municipal le permettant, les courriels doivent être conservés comme de la correspondance d'affaires, même les courriels supprimés. Ce faisant, le service de GI/TI se conformera au règlement municipal de la Ville.

Il n'existe aucune norme ou loi communément acceptée qui prescrit une période précise de conservation des courriels; cependant, étant donné la difficulté entourant le filtrage des courriels officiels et non officiels, il est pratique courante de conserver l'ensemble des correspondances par courriel afin d'assurer une gestion des documents de l'entreprise appropriée. Si le service de la GI/TI est en mesure de proposer une façon de filtrer les courriels d'affaires et ceux qui ne sont pas liés aux affaires avec un niveau d'assurance confortable, alors la question pourrait être discutée à l'interne et proposée à la direction afin qu'elle soit acceptée et éventuellement mise en œuvre.

### Recommandation 1

**Que la Ville revoit l'actuelle période de trois mois de conservation des courriels, y compris les courriels supprimés, pour s'assurer qu'elle est suffisante. Les exigences légales et en matière de TI doivent être prises en compte.**

#### Réponse de la direction

La direction est d'accord avec cette recommandation.

La direction examinera la période de trois mois de conservation des courriels en tenant compte des exigences légales et en matière de TI et fournira un rapport à ce sujet au Sous-comité de la TI d'ici à la fin du quatrième trimestre de 2011.

## *3.3 Politique sur la gestion de l'information/sécurité de la technologie de l'information*

La Politique sur la gestion de l'information/sécurité de la technologie de l'information est un document produit dans le but d'assurer la protection de l'information transmise sur le réseau de la Ville. Elle vise les utilisateurs responsables de la prestation et de la gestion des services de technologie de l'information. Les utilisateurs généraux ne sont pas visés par la Politique sur la sécurité de la GI/TI, car elle porte sur les mesures de précaution de la gestion du risque et définit des éléments de la sécurité de l'information devant être assurés en ce qui concerne les données se trouvant sur le réseau de la Ville.

La notion actuelle de la Politique sur l'utilisation responsable des ordinateurs en ce qui a trait aux actifs informatiques porte seulement sur l'équipement informatique. Le fait de reconnaître un logiciel comme un actif informatique en assurera la gestion et la protection au même titre que le matériel informatique.

Présentement, certaines informations transmises sur les appareils mobiles et portatifs ne passent pas par le système de réseau de la Ville (NIP à NIP et les messages textes ne sont pas connectés au réseau de l'entreprise, conformément à la Politique sur l'utilisation responsable des ordinateurs.) Si des documents d'affaires sont envoyés NIP à NIP, il pourrait ne pas y avoir de fichier sur ces données sur le réseau de la Ville. Les documents d'affaires ne devraient donc pas être transmis NIP à NIP. Tous les courriels et les documents transmis sur des ordinateurs portables,

des ordinateurs tout-terrain et des téléphones intelligents passent par le réseau de courriels de la Ville. Les appels vocaux faits par l'entremise d'appareils mobiles et portatifs ont des artefacts de transaction clés consignés, comme le numéro et l'heure.

Pour les personnes qui utilisent des appareils mobiles et portatifs, la correspondance par courriel quitte le réseau de l'entreprise (le fournisseur du téléphone ne fait pas partie du réseau de la Ville), ce qui signifie qu'elle n'est pas sous le contrôle complet du service de GI/TI. Par conséquent, une section ou une politique précise prévue pour les personnes qui utilisent des appareils portatifs de la Ville pourrait être nécessaire. Ce faisant, la Ville s'assurera que les utilisateurs d'appareils portatifs et de téléphones intelligents sont au courant que leurs appareils peuvent contenir de l'information sensible et qu'une attention spéciale et de la diligence s'appliquent.

Aussi, une plus grande utilisation d'appareils portatifs crée des risques de sécurité uniques, notamment le risque d'accès non autorisé aux données. Il existe également un plus grand risque que des personnes non autorisées aient accès à de l'information confidentielle.

L'exemple le plus évident d'un risque de sécurité unique est la perte d'un appareil portatif déverrouillé, ce qui ne veut pas dire que le service de la GI/TI crée le risque, mais que la promulgation d'une politique exigeant que tous les appareils portatifs soient verrouillés en tout temps pourrait s'avérer nécessaire.

La direction indique que la Politique sur l'utilisation responsable des ordinateurs et le Code de conduite de la Ville d'Ottawa gouvernent l'utilisation de ces appareils mobiles. Les appareils mobiles et portatifs sont configurés de la même manière que les ordinateurs portables de la Ville. Cette configuration comprend le cryptage des données lors de leur saisie et de leur transmission, la protection par mots de passe de l'appareil, le verrouillage pour éviter l'installation de logiciel non autorisé, et la suppression à distance sur des appareils perdus ou volés.

L'utilisation par le personnel d'appareils mobiles personnels sur les lieux de travail est également un problème émergent. Nous recommandons que la direction aborde de manière proactive cette question en établissant une politique appropriée et en l'appliquant.

## Recommandation 2

**Que la Ville officialise et inclue dans la Politique sur l'utilisation responsable des ordinateurs une notion étendue des actifs informatiques pour y inclure les logiciels.**

### Réponse de la direction

La direction est d'accord avec cette recommandation.

La Politique sur l'utilisation responsable des ordinateurs sera mise à jour pour inclure les logiciels comme étant un actif informatique de la Ville d'Ottawa, d'ici à la fin du troisième trimestre de 2011.

## *3.4 Normes de la gestion de l'information/sécurité de la technologie de l'information de la Ville d'Ottawa v1.10*

Les normes de la gestion de l'information/sécurité de la technologie de l'information de la Ville d'Ottawa v1.10 ont pour objet de clarifier des aspects de la Politique sur la sécurité de la GI/TI, et de détailler et de compléter les spécifications de la politique.

Les exigences et les énoncés des documents qui ont été révisés ne sont pas utiles s'ils ne sont pas renforcés et si la conformité des utilisateurs n'est pas surveillée. Le but de ces politiques est de protéger le réseau TI de la Ville en tant que service essentiel, et d'éduquer les utilisateurs pour optimiser l'utilisation de l'équipement et des services sur le réseau. Afin de s'assurer que les politiques sont respectées, les utilisateurs devraient être avisés en tout temps lorsque des outils de surveillance et de contrôle filtrent et analysent l'utilisation des ressources de la Ville. Idéalement, une surveillance permanente devrait être en place, et la direction devrait décider des conséquences découlant d'une violation à la politique.

Ceci renvoie au fait que, selon des discussions tenues avec la direction, il a été établi que l'équipement de filtrage et de protection est surtout utilisé en réaction aux incidents et aux violations. Afin de s'assurer que les contrôles et les pratiques exemplaires en matière de sécurité sont appliqués, une surveillance permanente est une option évidente qui permettra l'établissement de comportement ou d'incident de manière opportune.

Il devrait être mentionné que des outils de surveillance d'Internet et du courriel sont présentement utilisés pour surveiller les incidents, et non pour surveiller l'utilisation opérationnelle. La surveillance opérationnelle de l'activité des utilisateurs fournirait une meilleure compréhension de l'utilisation d'Internet et du courriel sur le réseau de la Ville, mais cela exigera un changement de vision en ce qui concerne la surveillance. La Ville pourrait décider de changer ce principe et d'agir en conséquence pour le mettre en œuvre.

La surveillance de l'utilisation opérationnelle est fortement liée à la surveillance permanente et signifie que des ressources sont allouées pour superviser l'activité des utilisateurs sur une base permanente, et non seulement en cas d'incidents. La « surveillance de l'utilisation opérationnelle » offrira une meilleure sécurité à la Ville et fera en sorte que les contrôles de sécurité contenus dans la Politique sur l'utilisation responsable des ordinateurs et ses annexes, les normes et les procédures sont appliqués et respectés en tout temps.

Actuellement, les normes de sécurité de la GI/TI n'ont pas été mises à jour ou révisées depuis le 3 novembre 2008. La Politique de sécurité de la GI/TI n'a pas été mise à jour depuis le 25 janvier 2007. Des normes de sécurité, telles que mentionnées dans la Section 3.3, doivent être élaborées à mesure que l'environnement de la TI et le réseau de la Ville changent. Afin de documenter ces changements, et d'offrir une vision de sécurité sur les technologies et les processus, les normes doivent être mises à jour de façon régulière.

La Politique sur la sécurité devrait être révisée au moins une fois par année, et devrait tenir compte du développement et de l'évolution des fonctions de la TI. Si aucun changement n'est requis, une révision et un processus de nouvelle approbation devraient être menés et la politique devrait être redistribuée à la communauté des utilisateurs pour rappeler les efforts de la Ville à cet effet.

Une meilleure utilisation des outils de surveillance et de contrôle signifierait une analyse régulière des activités des utilisateurs afin d'assurer le respect de la Politique sur l'utilisation responsable des ordinateurs et d'autres documents sur la politique de sécurité de la Ville. Aucune action précise et aucun objectif final ne peuvent être proposés ici, car cela exigerait une évaluation encore plus exhaustive. Autrement, il y a des outils qui effectuent la surveillance et le contrôle au sein de la Ville (p. ex., Websense, Promodag) et d'autres peuvent être mis en place selon les décisions de la direction en ce qui concerne l'amélioration de la sécurité de la Ville. L'utilisation optimisée des outils existants, leur mise à jour, la surveillance opérationnelle (comme mentionnée plus tôt) peuvent être considérées avant de changer l'architecture existante.

En décembre 2010, au cours de la vérification, les services de TI ont mis en place un service de prévention des intrusions, de la sécurité de l'information et de la gestion des événements. Les services de TI ont demandé à un fournisseur canadien de services de sécurité de surveiller jour et nuit nos services sur le Web (Ottawa.ca, etc.) et d'autres composantes essentielles du réseau. Au cours de la vérification, nous avons indiqué aux services de la TI que l'utilisation des outils de surveillance et de contrôle sur le réseau de la Ville devrait être améliorée. Selon nous, ce nouveau contrat contribue à aborder le problème.

## Recommandation 3

**Que la Ville garde ses normes de sécurité à jour et révise les politiques au moins une fois par année.**

### Réponse de la direction

La direction est d'accord avec cette recommandation.

Une révision des normes de sécurité sera intégrée dans les plans opérationnels annuels du Service de la TI, et une révision initiale sera entreprise d'ici à la fin du deuxième trimestre de 2012.

# 4 CONCLUSION

De façon générale, les politiques sur l'utilisation d'Internet et du courriel sont conformes aux pratiques de l'industrie; cependant, certains secteurs demandent d'être examinés de plus près. En particulier, la période de conservation des courriels d'entreprise doit être révisée. Aussi, l'utilisation des appareils mobiles et portatifs doit être abordée pour faire en sorte que cette information soit saisie dans le système de dossiers de l'entreprise.

# 5 REMERCIEMENTS

Nous tenons à remercier la direction pour la coopération et l'assistance accordées à l'équipe de vérification.