

Guide

Gestion des actifs

Partenaires – Consultants – Fournisseurs



Table des matières

1. Introduction	3
1. Objectifs.....	3
2. Champ d'application et personnes visées	3
2. Conditions d'utilisation et comportements interdits	4
1. Sécurité physique	4
2. Authentification	4
3. Gestion des sessions de travail	5
4. Gestion des actifs informationnels	6
5. Mobilité	6
6. Accès à distance.....	6
7. Accès sans-fil sécurisé	6
8. Stockage, manipulation et transfert des données de la Ville	7
9. Courrier électronique	7
10. Clavardage	8
11. Échange de documents électroniques.....	8
12. Propriétés matérielles, logicielles et progiciels.....	8
13. Utilisation de l'accès Internet de la Ville.....	8
14. Incidents de sécurité.....	9
3. Renseignements supplémentaires	11
1. Conséquence du non-respect.....	11
2. Référence	11
3. Cas d'exception	11
4. Acronymes.....	11

1. Introduction

1.1 Objectifs

L'objectif de ce document est d'expliquer l'application de la Politique de sécurité de l'information, du Cadre de gestion qui s'y rapporte, ainsi que les directives de sécurité de l'information.

Ce guide se veut explicatif et ciblé pour les consultants, les partenaires et les fournisseurs; pour plus de détail, veuillez consulter les documents suivants :

- Politique de sécurité de l'information;
- Cadre de gestion de la sécurité de l'information;
- Directive sur la gestion des actifs informationnels;
- Directive sur la gestion des incidents de sécurité;
- Directive sur l'accès Internet.

En cas de disparité, ces documents ont préséance sur le présent document.

1.2 Champ d'application et personnes visées

Ce guide est spécifique aux consultants, aux partenaires et aux fournisseurs de la Ville de Laval, notamment en ce qui a trait :

- à la sécurité physique des infrastructures de la Ville;
- à l'accès et la gestion des ressources informationnelles de la Ville;
- au traitement des incidents de sécurité.

2. Conditions d'utilisation et comportements interdits

2.1 Sécurité physique

L'accès aux locaux de la Ville dans les zones autres que publiques doit être régi par un contrat pour les employés ou un contrat de consultation, de partenariat ou pour fournisseur dûment signé et valide.

Seules les zones des bâtiments qui sont nécessaires pour exécuter les travaux selon les fonctions et les services requis sont autorisées.

Les visiteurs doivent être enregistrés à leur arrivée et doivent être accompagnés en tout temps dans les locaux de la Ville en dehors des zones publiques.

Les bureaux doivent faire l'objet d'un « bureau propre », ce qui signifie qu'il doit être exempt de documents et de papier.

Tous les documents et tout le matériel sensibles doivent être conservés sous clé.

Les corbeilles à papier, à recyclage et les autres contenants doivent être exempts d'information sensible.

Toute information sensible pouvant se trouver sur des documents de toute forme doit être mise dans les boîtes sécurisées destinées à la destruction des documents ou dûment déchiquetée. Ces boîtes sont disposées sur les étages de chaque édifice de la Ville.

Les documents imprimés doivent être ramassés dans les plus brefs délais. Les documents confidentiels imprimés ne peuvent être laissés sans surveillance. L'impression sécurisée au moyen d'un code est à privilégier lorsqu'il y a des documents contenant de l'information sensible.

2.2 Authentification

Identifiant et mot de passe

Toute personne doit être munie d'un identifiant qui lui est unique, propre à son profil. Le partage des identifiants et des mots de passe n'est pas permis.

Les identifiants et les mots de passe sont nécessaires pour accéder aux ressources informationnelles numériques.

Les identifiants et les mots de passe doivent être strictement valides selon les standards pour la période d'emploi au sein de la Ville, de la durée du contrat avec la Ville ou la durée de la relation d'affaires.

Les mots de passe doivent être changés à intervalles réguliers selon le standard de la Ville et ne peuvent être identiques aux précédents.

Il n'est pas permis de conserver les identifiants et les mots de passe sur papier.

Si l'utilisateur s'aperçoit que ses accès ont été utilisés par une tierce personne, il doit absolument déclarer l'incident de sécurité auprès du service à la clientèle SIT (se référer à la section 2.14.2), comme mentionné dans la Directive sur les incidents de sécurité.

Demandes d'accès

Les demandes d'accès doivent être basées sur le principe de la nécessité d'accès dans le cadre de la fonction du demandeur. Le propriétaire est responsable de s'assurer que seuls les accès requis sont attribués.

Le SIT se réserve le droit de refuser des demandes d'accès qui seraient jugées au-delà des privilèges requis.

Le SIT fera une revue périodique sur toutes les demandes d'accès qui ont été accordées. Les accès seront révoqués si l'utilisateur n'exerce plus un rôle pour lequel ces accès pourraient être requis.

Les demandes d'accès doivent être granulaires, c'est-à-dire en fonction de ce que les utilisateurs ont réellement besoin pour exercer leur emploi, leur rôle et leur mandat.

Toute demande d'accès est sujette à l'approbation du donneur d'ordres responsable à la Ville, puis du propriétaire de l'actif avant que ces accès soient conférés. Cela inclut aussi l'accès aux applications de la Ville.

Les accès sont octroyés aux employés, aux consultants, aux partenaires et aux fournisseurs dans le cadre de leurs fonctions. Tout accès par une autre personne est proscrit, y compris les membres de la famille.

Pour tout accès à des services existants et à de nouveaux services nécessaires à l'exécution de son mandat, une demande doit être faite au SIT et approuvée par le donneur d'ordres, soit un cadre de la Ville, répondant pour le demandeur.

Les accès et les comptes des utilisateurs doivent être révoqués à la fin du mandat du demandeur.

Les habilitations sécuritaires (avec le BIEL) requises pour ces accès doivent avoir été préalablement validées et vérifiées avant que les accès soient octroyés.

Dans l'alternative où le demandeur ne parvient pas à obtenir l'habilitation sécuritaire correspondante aux ressources qui sont requises pour accomplir son travail, le demandeur ne pourra ni accéder, ni recevoir, ni transiger l'information.

Le consultant, le partenaire et le fournisseur ont la responsabilité de s'assurer que dans la mesure où l'un de leurs employés quitte l'entreprise et qui n'est plus à l'emploi, a migré vers d'autres fonctions, d'aviser la Ville pour que les droits de cet employé soient traités en conséquence.

2.3 Gestion des sessions de travail

L'utilisateur a la responsabilité de verrouiller sa session de travail s'il s'absente de son ordinateur.

Lorsque l'utilisateur a terminé sa journée de travail, il doit s'assurer de fermer sa session de travail.

2.4 Gestion des actifs informationnels

Les employés, les consultants, les partenaires et les fournisseurs ont l'obligation de collaborer à la prise des inventaires des actifs informationnels de la Ville de Laval. Tout changement doit être signalé auprès du SIT.

Tous les actifs informationnels TI appartenant à la Ville doivent être déclarés, pris en stock et revalidés annuellement.

Tout vol, toute perte et tout vandalisme sur des actifs informationnels, y compris de l'équipement informatique et des téléphones intelligents, doivent être signalés au SIT dès qu'ils sont constatés pour qu'il y ait une prise en charge de l'incident de sécurité.

2.5 Mobilité

Les ordinateurs, les mobiles et les tablettes contenant de l'information de la Ville ne doivent pas être laissés sans surveillance dans les endroits publics. Ce même poste de travail doit être verrouillé physiquement de façon sécuritaire.

L'utilisateur doit s'assurer d'utiliser son poste de travail dans des conditions qui visent à préserver la confidentialité des informations auxquelles il a accès.

2.6 Accès à distance

Tout accès à distance est assujéti aux directives portant sur l'authentification et sur les demandes d'accès.

L'accès à distance des consultants, des partenaires et des fournisseurs est défini dans le contrat qui est conclu avec la Ville. Lorsque le contexte s'y prête, les habilitations sécuritaires requises doivent être demandées préalablement et doivent être valides.

Les consultants, les partenaires et les fournisseurs doivent accepter les conditions associées à l'utilisation des ressources.

2.7 Accès sans-fil sécurisé

L'accès au réseau est limité dans l'exercice d'un mandat bien précis, aux ressources qui sont strictement nécessaires à la réalisation du mandat.

L'accès au réseau à distance doit être encadré dans le contrat octroyé, et ce, selon les termes d'une entente-cadre. Ces accès ne seront disponibles que pour la durée des interventions par individu. Le partage des comptes et des accès n'est pas permis.

2.8 Stockage, manipulation et transfert des données de la Ville

Les entrées et les sorties de données et de documents de toute forme font l'objet d'une surveillance de la part du SIT pour toutes les infrastructures et les applications de la Ville de Laval.

Les méthodes de transfert de données, la manipulation et le stockage de données doivent être préalablement approuvés par le responsable de la sécurité du SIT.

Le transfert des données d'un support informatique à un autre doit être préalablement validé pour protéger les données d'accès inopportun.

La destruction de données et de documents électroniques telle que prescrite dans le plan de conservation de la Ville doit être encadrée de façon à ce que ces données ne puissent être récupérées de quelque façon que ce soit.

Le transfert de l'information d'un endroit à un autre sur des médias électroniques doit être sécurisé.

L'entreposage des sauvegardes des données doit être conservé dans un endroit à accès restreint et dont les personnes qui accèderont ont l'habilitation sécuritaire requise.

Pour les consultants, les fournisseurs et les partenaires, l'information ayant trait à la Ville de Laval, produite en vertu d'un contrat signé, doit être hébergée sur le service de stockage normalisé de la Ville.

Pendant la durée de l'hébergement de l'information par le consultant, le partenaire ou le fournisseur, selon le cas, a la responsabilité de s'assurer que l'intégralité de cette information n'est pas affectée. Dans le cas où il constate une altération, il doit absolument contacter le SIT et déclarer un incident de sécurité.

Dans le cadre de leurs mandats, les consultants, les partenaires et les fournisseurs doivent s'assurer que les données et les documents qu'ils produisent sont sauvegardés et demeurent sur des supports de données appartenant à la Ville. Les responsables de SIT doivent avoir confirmé le retour et l'intégralité de l'information avant la destruction de la copie hébergée chez le consultant, le partenaire ou le fournisseur.

La destruction de l'information après la restitution et la confirmation doit être faite de façon à ce qu'elle ne puisse être restaurée d'une façon ou d'une autre.

L'information doit être manipulée de façon à être conforme aux lois, aux règlements et aux normes en vigueur.

2.9 Courrier électronique

Il est interdit de faire un renvoi automatique entre une adresse de courrier électronique de la Ville et un compte de courrier électronique personnel, d'entreprise ou d'organisme tiers.

2.10 Clavardage

La fédération avec d'autres entreprises et organismes doit être régie par un contrat en bonne et due forme qui stipule les responsabilités et les limites de chaque entreprise.

L'information sensible ne doit pas être acheminée par ce média.

2.11 Échange de documents électroniques

Une attention particulière doit être portée à la classification de l'information en fonction des interlocuteurs avec lesquels l'employé échange. En cas de doute, l'employé doit vérifier avec son supérieur immédiat. Les consultants, les partenaires et les fournisseurs doivent faire approuver les échanges de documents électroniques par le donneur d'ordres.

Au préalable, l'information contenue dans les documents électroniques doit avoir été approuvée pour être échangée avec l'externe, qu'il s'agisse de consultants, de partenaires et/ou de fournisseurs par un cadre de la Ville.

Dans la nécessité d'échanger avec l'externe, seuls les services normalisés de la Ville sont autorisés. Les accès seront journalisés.

Le consultant, le partenaire et le fournisseur ont la responsabilité de s'assurer que les documents qu'ils transmettent sont considérés comme étant intacts, sans menace attachée ou intégrée. Ils doivent s'assurer d'avoir les outils de détection et de procéder systématiquement à la validation avant tout échange avec la Ville. S'ils constatent une irrégularité, il est de leur devoir de déclarer cet incident de sécurité.

2.12 Propriétés matérielles, logicielles et progicielles

Les consultants, les partenaires et les fournisseurs doivent s'assurer d'être détenteurs en règle des équipements, des licences, des logiciels et des progiciels qu'ils utilisent sur leurs ordinateurs, leurs mobiles et leurs services en infonuagique pour offrir leurs services à la Ville de Laval.

2.13 Utilisation de l'accès Internet de la Ville

Les consultants, les partenaires, les fournisseurs et leurs sous-traitants peuvent utiliser l'accès Internet dans le cadre des tâches qui leur sont confiées pendant les heures requises par la Ville et dans le cadre de leurs mandats.

Le portail d'échange documentaire externe de la Ville doit être utilisé pour transiger avec la Ville. Des dérogations sont possibles, mais elles doivent être approuvées par le SIT.

L'utilisation des outils de collaboration qui permettrait la connectivité entre la Ville et un consultant, un partenaire, un fournisseur et leurs sous-traitants doit avoir été définie au contrat.

Les accès à distance, le support applicatif et technologique, doivent être prévus au contrat entre la Ville de Laval et leurs consultants, leurs partenaires ou leurs fournisseurs ou leurs sous-traitants impliqués.

L'utilisation des applications, des plateformes, des solutions d'affaires, des infrastructures et des autres services en infonuagique mis à la disposition des consultants, des partenaires, des fournisseurs et des sous-traitants dans le cadre des ententes avec la Ville doit être prévue au contrat.

Le téléchargement de logiciels et de gratuits est interdit sur les postes de la Ville. Le consultant, le partenaire, le fournisseur et leurs sous-traitants doivent s'assurer d'avoir les licences en vigueur sur leurs postes, lorsque permis, pour produire les livrables dans le cadre de leur mandat.

Tout accès à distance à d'autres réseaux d'entreprises n'est permis que par l'accès Internet public. Ces accès doivent avoir été prévus au contrat et autorisés par le SIT.

2.14 Incidents de sécurité

Les employés, les consultants, les partenaires, les fournisseurs, les citoyens et les visiteurs ont l'obligation de rapporter tout incident de sécurité informatique dont ils ont connaissance en regard des actifs de la Ville de Laval.

Cela s'applique à tout ce qui a trait aux actifs informationnels de la Ville de Laval dans les cas suivants :

- Constat de tentative ou d'accès, d'utilisation, de manipulation, d'altération, de distribution ou de destruction d'information à des fins malveillantes, par exemple :
 - Vol d'identité numérique et utilisation de l'identité d'un tiers
 - Piratage et intrusion
 - Distribution d'information à des destinataires qui n'ont pas les autorisations requises
 - Accès illicite au réseau
- Constat d'une brèche de sécurité dans un système d'exploitation, un service normalisé, une application ou un logiciel ou bien des combinaisons de certaines de ces composantes;
- Comportement d'un utilisateur qui n'est pas conforme à la Politique, au cadre de gestion et aux autres directives émises par le SIT.

Sensibilisation

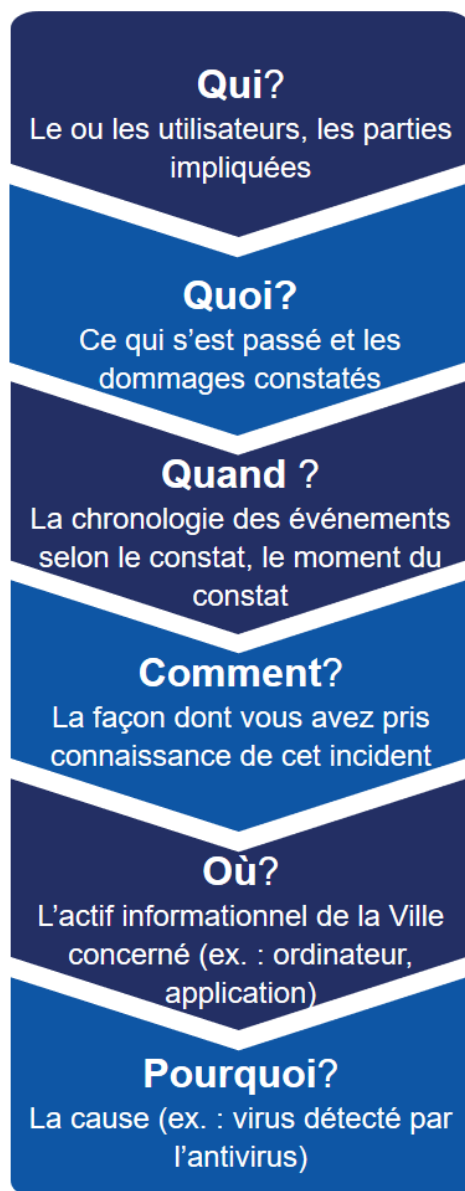
Les consultants, les partenaires et les fournisseurs doivent prendre connaissance de la Politique de sécurité de l'information, du cadre de gestion et des directives de sécurité au début de leur mandat. Ils doivent aussi s'engager, dans les termes du contrat, à s'y conformer.

Déclaration des incidents de sécurité

Dès que le consultant, le fournisseur ou le partenaire prend conscience d'un incident de sécurité, il doit obligatoirement le déclarer pour une prise en charge par l'équipe de sécurité de la Ville de Laval.

Composez le **450 978-6888, poste 4000**, pour déclarer l'incident de sécurité.

Afin d'accélérer le traitement de cette déclaration, vous devez avoir en main :



Cette information doit être la plus exacte possible. Vous devez fournir votre nom, votre courrier électronique, votre numéro de téléphone pour être joint.

Le responsable de la sécurité prendra en charge l'investigation avec le soutien de l'équipe opérationnelle TI.

Veuillez noter que les artefacts de cet incident doivent être conservés de façon intacte, ils peuvent être produits en cour, s'il y a matière à poursuite.

3. Renseignements supplémentaires

3.1 Conséquence du non-respect

En cas de violation ou de non-respect de ce guide, les sanctions mentionnées à la Politique de sécurité de l'information et au Cadre de gestion s'appliqueront.

3.2 Référence

- Politique de sécurité de l'information, Ville de Laval
- Cadre de gestion de la sécurité de l'information, Ville de Laval
- Directive – Gestion des actifs informationnels, Ville de Laval
- Directive – Gestion de la sécurité des ressources humaines, Ville de Laval
- Directive – Gestion des incidents, Ville de Laval
- Norme ISO/CEI 27002:2013 : Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information

3.3 Cas d'exception

Toute exception devra faire l'objet d'une demande de dérogation en bonne et due forme.

3.4 Acronymes

Acronyme	Description
BIEL	Bureau d'intégrité et d'éthique de Laval
CEI	Commission électrotechnique internationale
ISO	International Organization of Standardization
SIT	Service de l'innovation et des technologies