TITRE Document explicatif de la Politique et des directives de sécurité de l'information pour Consultants, Partenaires et Fournisseurs	**NO. CONTRÔLE**
DIVISION PRINCIPALE Service de Sécurité de l'information / Service de l'Innovation et des technologies	**ÉMISE LE** 2020-01-16
PROPRIÉTAIRE DE LA DIRECTIVE Amar Haicheur, Assistant-directeur, Gouvernance intégrée et services partagés TI	**En vigueur depuis** 2020-04-29

1. Objectifs, champs d'application et personnes visées

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.

Cette directive se veut explicative et ciblée pour les consultants, partenaires et 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

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

- Sécurité physique des infrastructures de la Ville ;
- Accès et gestion des ressources informationnelles de la Ville;
- Traitement des incidents de sécurité ;

2. Conditions d'utilisation et comportements interdits

2.1. Sécurité physique

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

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

c. 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.

d. Les bureaux doivent faire l'objet d'un « bureau propre », ce qui signifie qu'il doit être exempt de documents et de papier. Tout document et matériel sensible doivent être conservés sous clé.

e. Les corbeilles à papier, à recyclage et autres contenants doivent être exempts d'information sensible. Toute information sensible pouvant se trouver sur des documents de toute forme doit être mis dans les boîtes sécurisées destinées à la destruction des documents ou dûment déchiquetés. Ces boîtes sont disposées sur les étages de chaque édifice de la Ville.

f. 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

2.2.1. Identifiant et mot de passe

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

b. Les identifiants et mot de passe sont nécessaires pour accéder aux ressources informationnelles numériques.

c. Les identifiants et mot 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.

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

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

f. 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), tel que mentionné dans la *Directive sur les incidents de sécurité*.

2.2.2. Demandes d'accès

a. 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 seul les accès requis soient attribués.

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

c. 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.

d. 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, rôle et mandat.

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

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

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

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

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

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

k. Le consultant, partenaire et fournisseur a la responsabilité de s'assurer que dans la mesure où l'un de ses 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

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

b. 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

a. Les employés, consultants, partenaires, 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.

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

c. Tout vol, perte, vandalisme sur des actifs informationnels, incluant équipement informatique et 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

a. Les ordinateurs, mobiles et 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.

b. 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

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

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

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

2.7. Accès sans-fil sécurisé

a. 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.

b. 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

a. Les entrées et 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 applications de la Ville de Laval.

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

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

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

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

f. 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.

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

h. 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.

i. Dans le cadre de leurs mandats, les consultants, partenaires et fournisseur doivent s'assurer que les données et documents qu'ils produisent sont sauvegardés et demeurent sur des supports de donnée 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.

j. 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.

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

2.9. Courrier électronique

a. 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

a. 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.

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

2.11. Échange de documents électroniques

a. 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, partenaires et fournisseurs doivent faire approuver les échanges de documents électroniques par le donneur d'ordres.

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

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

d. Le consultant, partenaire et fournisseur a la responsabilité de s'assurer que les documents qu'il transmet sont considérés intacts, sans menace attachée ou intégrée. Il doit s'assurer d'avoir les outils de détection et de procéder systématiquement à la validation avant tout échange avec la Ville. S'il constate une irrégularité, il est de son devoir de déclarer cet incident de sécurité.

2.12. Propriétés matérielles, logicielles et progicielles

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

2.13. Utilisation de l'accès Internet de la Ville

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

b. 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.

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

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

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

f. Le téléchargement de partagiciels et de gratuiciels sont interdits sur les postes de la Ville. Le consultant, partenaire, 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.

g. 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 autorisé par le SIT.

2.14. Incidents de sécurité

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

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

a) 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 :
    a. Vol d'identité numérique et utilisation de l'identité d'un tiers;
    b. Piratage et intrusion ;
    c. Distribution d'information à des destinataires qui n'ont pas les autorisations requises ;
    d. Accès illicite au réseau ;

b) Constat d'une brèche de sécurité dans un système d'exploitation, un service normalisé, d'une application ou d'un progiciel ou bien des combinaisons de certaines de ces composantes;

c) Comportement d'un utilisateur qui n'est pas conforme à la Politique, au cadre de gestion et aux autres directives émise par le SIT;

2.14.1. Sensibilisation

a. Les consultants, partenaires et 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.

2.14.2. Déclaration des incidents de sécurité

a. Dès que le consultant, le fournisseur, 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.

b. Contactez-le (450) 978-6888, extension 4000 pour déclarer l'incident de sécurité.

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

1- **Qui** : l'utilisateur ou tous les utilisateurs, les parties impliquées ;
2- **Quoi** : ce qui s'est passé et quels sont les dommages qui sont constatés;
3- **Quand** : chronologie des événements selon le constat, à quel moment est-ce que cela a été constaté;
4- **Comment** : de quelle façon vous avez pris connaissance de cet incident ;
5- **Où** : sur quel actif informationnel de la Ville, (ex : ordinateur, application);
6- **Pourquoi** : si l'on connaît la cause (ex : virus identifié par l'anti-virus).

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

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

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

2.15. Conséquence du non-respect

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

3. Définitions

Accès à distance : Lorsqu'à partir d'un ordinateur, il est possible de rejoindre un service, une infrastructure ou même des applications.

Accès filaire : Branchement réseau à partir d'un câble réseau entre un ordinateur et une prise.

Accès sans-fil : Branchement réseau à partir d'ondes entre un ordinateur et une infrastructure.

Actif informationnel : Une information, quel que soit son canal de communications ou son support, une Plateforme technologique et Solution d'affaires TI ou une Technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par la Ville et sous sa responsabilité.

Application : Ensemble de programmes dont se servent les utilisateurs afin d'accomplir une tâche ou une activité particulières.[1]

Authentification : Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel[2].

Authentification à deux facteurs : Dans ce cas précis, authentification requérant à la fois ce que l'on connaît, donc un mot de passe, mais aussi ce que l'on possède, un périphérique externe.

Autorisation : Attribution à une personne ou à une entité d'un droit d'accès, complet ou restreint, à une ressource.

Catégorisation des actifs : Processus par lequel les actifs se voient conférer un indice basé sur les critères de disponibilité, d'intégrité et de confidentialité**.**

Confidentialité : propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Consultant : Personne extérieure à une entité qui assiste les dirigeants dans un domaine délimité sans assumer la responsabilité de la décision proposée[3].

Disponibilité : propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Fournisseur : Personne physique ou morale qui fournit un produit ou un service à l'organisation de l'évènement et pour lesquels elle obtient une compensation[4].

Gouvernance de sécurité : validation des activités, fonctions, rôles, processus et les relations établies entre ces derniers pour une saine gestion de la sécurité de l'information.

---

[1] Grand dictionnaire terminologique
[2] Ibid.
[3] Ibid.
[4] Grand dictionnaire terminologique.

Incident de sécurité : c'est lorsqu'un risque se concrétise et peut avoir des impacts sur les citoyens, le service ou les utilisateurs**.**

Infonuagique : Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation.[5]

Information numérique : information dont l'utilisation n'est possible qu'au moyen des technologies de l'information.

Intégrité : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'Intégrité fait référence à l'exactitude et à la complétude.

Journalisation : Enregistrement dans un journal d'événements qui se produisent dans une infrastructure, une application ou un service.

Logiciel : Ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données.[6]

Outil de collaboration : Outil informatique qui favorise le travail collaboratif et qui répond à des besoins de communication, de coordination et de production.[7]

Partenaire : Organisation avec laquelle une autre organisation collabore pour atteindre des objectifs.[8]

Progiciel : Ensemble complet et intégré de programmes ou modules, paramétrables, à usage professionnel, accompagné de services et de documentation, conçu pour plusieurs utilisateurs simultanés, en vue d'une application commune**.**[9]

Utilisateur : Toute personne physique ou morale qui, par engagement contractuel ou autrement, fait usage ou a accès à tout Actif informationnel sous la responsabilité de la Ville. Son notamment des Utilisateurs les employés municipaux sans égard à leur catégorie d'emploi ou leur statut, les citoyens, les élus, les fournisseurs, les partenaires ainsi que toute personne ayant recours aux services de la Ville.

[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.

4. Approbation et version

RESPONSABLE DE LA DIRECTIVE Amar Haicheur	SIGNATURE
TITRE Assistant-directeur, Gouvernance intégrée et services partagés TI	DATE D'APPROBATION 2020-04-29

Version	Rédacteur	Commentaires/mises à jour	Date
0.1	Helene Decelles	Version initiale	2019-10-18
0.2	Helene Decelles	Révision	2019-10-23
1.0	Helene Decelles	Version révisée juridique	2020-01-16
1.1	Joel Moreault	Ajustements mineurs	2020-04-08
1.2	Joel Moreault	Révision de la direction - Ajustements	2020-04-29