

Direction générale de l'agilité et de la performance

NOTE

DESTINATAIRE : M. Karl Malenfant
Vice-président aux technologies de l'information et
chef de projet CASA

DATE : Le 22 mai 2020

OBJET : **DAP – Rapatriement des ressources hors site – Conversion et
sécurité**

CONTEXTE

Lors de l'exécution des travaux du lot 4, soit les travaux de la phase de réalisation de la Livraison 1, des préoccupations ont été soulevées concernant l'attribution de travaux de conversion et de sécurité à des ressources travaillant en Inde impliquant la manipulation de données nominatives confidentielles ou la création de rôles de sécurité pouvant octroyer l'accès à des données nominatives. À ce moment, l'outil permettant l'anonymisation des données nominatives n'était pas encore en fonction, ce qui n'est plus le cas maintenant. Après analyse, la Société avait évalué que le risque relié à la manipulation ou à l'accès à des données nominatives confidentielles, concernant plusieurs millions de Québécois, par des ressources localisées à l'extérieur du Québec, de même que l'impact qu'un tel incident pourrait avoir sur la perception de la Société par la population, était très élevé.

Afin de mitiger le risque induit par la manipulation et l'accès à des données nominatives pour des travaux effectués à l'extérieur du Québec, le chef de projet CASA a exigé de l'Alliance que les travaux de conversion et de sécurité soient rapatriés au Québec.

L'annexe C du Contrat de Services professionnels et de vente d'équipements encadre les modalités relatives à la tarification des services professionnels et l'annexe C-2 précise les taux horaires facturables par grand profil contractuel par période. Les ressources effectuant des travaux de conversion et de sécurité sont incluses dans le profil Équipier Intégration technologique qui regroupe une multitude de ressources œuvrant dans des domaines diversifiés et travaillant outre-mer. Le taux était alors de 82 \$. Ce taux a été ajusté temporairement à 195 \$ pour la période du 1^{er} janvier au 31 mars 2018 et à 197 \$ pour la période du 1^{er} avril 2018 au 31 mars 2019 afin de s'harmoniser à un taux similaire au marché québécois, même si ce taux n'existe pas au Contrat. Cet ajustement temporaire est encadré dans l'Entente du lot 4 signée par les deux parties en vigueur jusqu'au 30 octobre 2018, ou jusqu'à l'acceptation définitive du lot. Cet ajustement a également été documenté dans la DAP 35 et a été approuvé par le comité de direction lors de la séance du 27 février 2018. Le lot 4 est maintenant fermé.

Les travaux de la Livraison 2 ont débuté le 1^{er} novembre 2018. Puisqu'il s'agissait d'une entente à durée déterminée, le taux appliqué aux ressources qui exécutent des travaux de conversion et de sécurité est celui du profil Intégration technologique prévu à l'annexe C-2 du Contrat des Services professionnels et de vente d'équipements. Ce taux est actuellement de 85 \$.

Pour la Livraison 2, l'Alliance souhaite reconduire la DAP 35. L'impact monétaire de cette reconduction se chiffrerait, selon l'Alliance, à 16 M\$.

Au Québec, c'est la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels qui encadre l'accès et l'utilisation des renseignements nominatifs et plus particulièrement l'article 70.1 :

« Avant de communiquer à l'extérieur du Québec des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi.

Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte. »

Plusieurs dispositions contractuelles sont prévues afin de s'assurer du respect de cette Loi dans l'exécution du Contrat (voir références en annexe) :

- Article 16.1 du Contrat cadre : *« Ce Contrat cadre est régi par les lois applicables au Québec »;*
- Article 2.7 du Contrat de Services professionnels : *« L'Intégrateur s'engage à respecter, dans l'exécution du Contrat de Services professionnels, les lois et règlements en vigueur au Québec applicables à l'exécution du présent Contrat de Services professionnels »;*
- Article 1.2.12 de l'annexe N du Contrat de Services professionnels – Protection des renseignements personnels et confidentiels : *« Obtenir l'autorisation écrite de la Société avant de communiquer ou de transférer quelque donnée que ce soit, même à des fins techniques, hors Québec »;*

De plus, l'article 31 du Contrat de Services professionnels précise que ne pas exiger la stricte exécution d'un engagement contenu au contrat ne doit pas être considéré comme une renonciation.

Lors de la révision du bordereau à des fins de production de la version amendée, aucune demande d'autorisation écrite n'a été formulée par l'Alliance pour des travaux exécutés à l'extérieur du Québec impliquant la manipulation de données nominatives confidentielles ou la création de rôles de sécurité pouvant octroyer l'accès à des données nominatives. Le bordereau amendé décrit de façon détaillée la proportion de ressources sur site et hors site ainsi que les taux demandés pour chaque profil de ressources.

Depuis la Livraison 1, l'outil d'anonymisation des données est maintenant en place, ce qui permet de restreindre le nombre de ressources nécessitant l'accès à des données nominatives. À ce jour, les ressources qui exécutent des travaux de conversion et de sécurité nécessitant des accès à des données nominatives, qui nécessitent des comptes de sécurité privilégiés ou qui peuvent octroyer de tels comptes sont réparties comme suit :

- Conversion : 8 ressources au CIC de Montréal. Ces ressources nécessitent des accès à des données nominatives dans le cadre de leurs fonctions.
- Sécurité : 9 ressources au Québec. Ces ressources détiennent des comptes de sécurité privilégiés et peuvent octroyer de tels comptes. La détention de ce type de compte est essentielle dans le cadre de leurs fonctions.

RECOMMANDATION

Considérant que :

- L'Alliance aurait dû obtenir l'autorisation écrite de la Société afin de faire exécuter des travaux impliquant la manipulation de données nominatives confidentielles ou la création de rôles de sécurité pouvant octroyer l'accès à des données nominatives à l'extérieur du Québec;
- Une telle autorisation n'a pas été demandée par l'Alliance;
- L'Alliance avait l'occasion de modifier la proportion des ressources sur site et hors site dans son bordereau amendé ainsi que les taux afférents à chacun des profils.
- L'annexe C-2 du Contrat de Services professionnels encadre les taux payables par profils;
- L'entente contenue dans la DAP 35 et dans l'Entente de lot 4 était à durée limitée et que cette entente est échue;
- Le fait de ne pas avoir appliqué le taux prévu à l'annexe C du Contrat de Services professionnels pour la Livraison 2 ne constitue pas une renonciation à l'exigence du contrat;
- L'outil d'anonymisation est maintenant fonctionnel, ce qui permet de restreindre le nombre de ressources ayant accès à des données nominatives confidentielles;

Il est recommandé de ne pas reconduire le taux de la DAP 35 et de poursuivre l'application du taux prévu à l'annexe C-2 du Contrat pour ressources qui exécutent des travaux de conversion et de sécurité rapatriés au Québec.

IMPACT BUDGÉTAIRE

Il n'y a aucun ajout budgétaire.

Le directeur général de l'agilité et de la performance,

Sylvain Cloutier

p. j. Annexes

ANNEXES

EXTRAITS DE LA LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

🕒 **67.2.** Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme.

Dans ce cas, l'organisme public doit:

1° confier le mandat ou le contrat par écrit;

2° indiquer, dans le mandat ou le contrat, les dispositions de la présente loi qui s'appliquent au renseignement communiqué au mandataire ou à l'exécutant du contrat ainsi que les mesures qu'il doit prendre pour en assurer le caractère confidentiel, pour que ce renseignement ne soit utilisé que dans l'exercice de son mandat ou l'exécution de son contrat et pour qu'il ne le conserve pas après son expiration. En outre, l'organisme public doit, avant la communication, obtenir un engagement de confidentialité complété par toute personne à qui le renseignement peut être communiqué, à moins que le responsable de la protection des renseignements personnels estime que cela n'est pas nécessaire. Une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service visé au premier alinéa doit aviser sans délai le responsable de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué et doit également permettre au responsable d'effectuer toute vérification relative à cette confidentialité.

Le deuxième alinéa ne s'applique pas lorsque le mandataire ou l'exécutant du contrat est un membre d'un ordre professionnel. De même, le paragraphe 2° du deuxième alinéa ne s'applique pas lorsque le mandataire ou l'exécutant du contrat est un autre organisme public.

1985, c. 30, a. 8; 1990, c. 57, a. 16; 1994, c. 40, a. 457; 2006, c. 22, a. 40.

🕒 **67.3.** Un organisme public doit inscrire dans un registre toute communication de renseignements personnels visée aux articles 66, 67, 67.1, 67.2, 68 et 68.1, à l'exception de la communication d'un renseignement personnel requis par une personne ou un organisme pour imputer, au compte d'un membre d'un organisme public, de son conseil d'administration ou de son personnel, un montant dont la loi oblige la retenue ou le versement.

Un organisme public doit aussi inscrire dans ce registre une entente de collecte de renseignements personnels visée au troisième alinéa de l'article 64, de même que l'utilisation de renseignements personnels à d'autres fins que celles pour lesquelles ils ont été recueillis visées aux paragraphes 1° à 3° du deuxième alinéa de l'article 65.1.

Dans le cas d'une communication d'un renseignement personnel visée au premier alinéa, le registre comprend:

- 1° la nature ou le type de renseignement communiqué;
- 2° la personne ou l'organisme qui reçoit cette communication;
- 3° la fin pour laquelle ce renseignement est communiqué et l'indication, le cas échéant, qu'il s'agit d'une communication visée à l'article 70.1;
- 4° la raison justifiant cette communication.

Dans le cas d'une entente de collecte de renseignements personnels, le registre comprend:

- 1° le nom de l'organisme pour lequel les renseignements sont recueillis;
- 2° l'identification du programme ou de l'attribution pour lequel les renseignements sont nécessaires;
- 3° la nature ou le type de la prestation de service ou de la mission;
- 4° la nature ou le type de renseignements recueillis;
- 5° la fin pour laquelle ces renseignements sont recueillis;
- 6° la catégorie de personnes, au sein de l'organisme qui recueille les renseignements et au sein de l'organisme receveur, qui a accès aux renseignements.

Dans le cas d'utilisation d'un renseignement personnel à une autre fin que celle pour laquelle il a été recueilli, le registre comprend:

- 1° la mention du paragraphe du deuxième alinéa de l'article 65.1 permettant l'utilisation;
- 2° dans le cas visé au paragraphe 3° du deuxième alinéa de l'article 65.1, la disposition de la loi qui rend nécessaire l'utilisation du renseignement;
- 3° la catégorie de personnes qui a accès au renseignement aux fins de l'utilisation indiquée.

1985, c. 30, a. 8; 1990, c. 57, a. 17; 2006, c. 22, a. 41.

🕒 **70.1.** Avant de communiquer à l'extérieur du Québec des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public doit s'assurer qu'ils bénéficieront d'une **protection** équivalant à celle prévue à la présente loi.

Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une **protection** équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.

2006, c. 22, a. 47.

EXTRAITS DU CONTRAT CADRE

16. DROIT APPLICABLE ET RÈGLEMENT DES DIFFÉRENDS

16.1 Ce Contrat cadre est régi par les lois applicables au Québec.

EXTRAITS DU CONTRAT DE SERVICES PROFESSIONNELS ET DE VENTE D'ÉQUIPEMENTS

1.2 Définitions

À moins que le contexte n'exige un sens différent, les définitions stipulées au Contrat cadre s'appliquent à ce Contrat de Services professionnels.

Les termes et expressions qui suivent, lorsqu'ils apparaissent dans le Contrat ou dans toute annexe liée à celui-ci, s'interprètent à moins d'une dérogation implicite ou explicite dans le texte, en fonction des définitions qui leur sont attribuées ci-après. Si la compréhension du texte le requiert, un mot exprimé avec le genre masculin comprend le féminin et vice versa; il en va de même pour un mot exprimant un nombre en ce dont le singulier comprend le pluriel et vice versa.

« **Accès informatiques privilégiés** » désigne notamment les accès informatiques qui octroient des pouvoirs d'intervention supplémentaires aux actifs informationnels numériques de la Société à certains intervenants de la Société, lesquels sont notamment décrits au Plan Qualité Programme (PQP):

« **Attestation d'antécédents judiciaires** » désigne une lettre ou un certificat émis par un

2

CT 19000010
P22899

corps policier ou toute autorité gouvernementale démontrant qu'une personne possède ou non des antécédents judiciaires.

2. REPRÉSENTATIONS ET GARANTIES DE L'INTÉGRATEUR

L'Intégrateur fait les représentations et garanties suivantes au bénéfice de la Société :

2.1 Statut

L'Intégrateur a été dûment constitué et il s'est conformé, initialement et annuellement, aux exigences de la *Loi sur la publicité légale des entreprises* (Québec) par l'envoi de sa déclaration initiale et, chaque année subséquente, de sa déclaration annuelle au Registraire des entreprises.

2.2 Permis d'exploitation

L'Intégrateur possède tous les permis requis en relation avec ses activités.

2.3 Capacité juridique

L'Intégrateur a tous les pouvoirs requis par la loi et a pris toutes les mesures légales nécessaires pour être autorisé à signer les présentes. L'Intégrateur a également tous les pouvoirs nécessaires afin de poursuivre toute entreprise dans laquelle il est engagé au jour de la signature du Contrat de Services professionnels, d'exercer les droits lui revenant et de se soumettre aux obligations lui incombant en vertu du Contrat de Services professionnels.

2.4 Ressources

L'Intégrateur dispose ou s'engage à obtenir l'ensemble des ressources humaines et matérielles nécessaires à l'exécution du Contrat de Services professionnels.

2.5 Liberté contractuelle de l'Intégrateur

L'Intégrateur n'est lié à aucune entente ou obligation précédente qui pourrait être en conflit avec le Contrat de Services professionnels ou qui pourrait lui interdire ou limiter l'exécution du Contrat de Services professionnels et il peut exécuter les obligations

stipulées au Contrat de Services professionnels, sans qu'il soit nécessaire d'obtenir de licence, de renonciation, de consentement ou d'approbation qu'il ne détiendrait pas à la Date d'entrée en vigueur du Contrat de Services professionnels.

2.6 Propriété intellectuelle

L'Intégrateur détient, selon le cas à titre de propriétaire ou de titulaire de droits de licence ou autre, tous les droits, titres et intérêts de propriété intellectuelle requis aux fins de l'exécution de ce Contrat de Services professionnels.

2.7 Respect des lois et règlements

L'Intégrateur s'engage à respecter, dans l'exécution du Contrat de Services professionnels, les lois et règlements en vigueur au Québec applicables à l'exécution du présent Contrat de Services professionnels.

2.8 Certification

2.8.1 L'Intégrateur doit maintenir sa certification ISO 9001:2008 ou la version courante à venir, durant toute la durée du Contrat de Services professionnels.

2.9 Collaboration

L'Intégrateur s'engage à collaborer entièrement avec la Société dans l'exécution du Contrat de Services professionnels et à tenir compte de toutes les recommandations de la Société relatives à la façon de préparer et d'exécuter le travail confié.

7.5.3 Lieu de travail

L'équipe de projet travaillera dans des locaux au siège social de la Société à Québec. Pour certains travaux spécifiques réalisés par l'Intégrateur, la Société est ouverte à ce que ces travaux se réalisent à l'extérieur des locaux de la Société. Ces travaux devront être identifiés dans les Ententes de lots.

7.6 Éthique et sécurité de l'information

L'Intégrateur s'engage à respecter et appliquer et se porte garant du respect et de l'application par les Ressources de l'Intégrateur des règles, procédures et mesures de sécurité décrites au guide joint comme annexe J.

8. RESSOURCES HUMAINES

8.1 Lien d'emploi

- 8.1.1** L'Intégrateur est entièrement responsable à l'égard de l'ensemble des Ressources de l'Intégrateur affecté à l'exécution du Contrat de Services Professionnels, à l'exclusion du personnel de la Société, et il devra en assumer tous les droits, obligations et responsabilités. L'Intégrateur devra notamment se conformer aux lois régissant les accidents du travail et à celles régissant les conditions de travail.

13

- 8.1.2** Les ressources des sous contractants de l'Intégrateur impliquées dans l'exécution du Contrat de Services Professionnels sont sous l'entière responsabilité de l'Intégrateur qui en assume toutes les obligations.

8.4 Attestation de sécurité

8.4.1 Chaque Ressource de l'Intégrateur, selon le cas,

- qui est susceptible d'obtenir des Accès informatiques privilégiés; ou,
- dont le mandat est sous la responsabilité de l'équipe de la sécurité informatique;

ne doit pas avoir été déclarée coupable, dans les cinq (5) dernières années précédant la Date d'entrée en vigueur du Contrat de Services professionnels, d'une infraction pénale ou criminelle concernant les infractions ayant un lien avec l'objet du présent mandat, à moins d'en avoir obtenu le pardon ou la réhabilitation. Sont notamment considérés incompatibles avec les activités que la ressource sera appelée à réaliser dans le cadre du mandat, les actes criminels et les infractions figurant à l'annexe L, le tout conformément à l'article 18.2 de la *Charte des droits et libertés de la personne*.

8.4.2 La Société se réserve le droit de demander à l'Intégrateur de lui remettre une Attestation d'antécédents judiciaires pour chaque ressource visée au paragraphe précédent. L'Intégrateur devra alors fournir à la Société l'original de l'attestation au plus tard trois (3) jours ouvrables avant la date prévue d'entrée en fonction de la ressource. Pour être recevable, l'attestation devra de plus avoir été émise depuis moins de trois (3) mois de la date de la demande de la Société. Elle devra être transmise à la Société sous enveloppe cachetée avec la mention « PERSONNEL ET CONFIDENTIEL ». L'enveloppe sera confiée exclusivement, aux fins de vérification et de conservation, au gestionnaire ou au directeur concerné.

8.4.3 Toutes les exigences prévues au présent article s'appliquent également au remplaçant d'une ressource visée par le paragraphe 8.4.1 du présent article et devront être respectées tout au long du Contrat de Services professionnels.

8.4.4 L'Intégrateur est tenu d'informer préalablement les personnes concernées de ces

exigences et de recueillir auprès de ces personnes les renseignements et autorisations nécessaires à la vérification et à la communication des résultats à la Société.

- 8.4.5 De plus, l'Intégrateur devra aviser la Société dans les plus brefs délais, de tout événement pouvant entraîner une modification au résultat de la vérification d'antécédents judiciaires obtenue préalablement à l'entrée en fonction de la ressource.
- 8.4.6 Si l'Intégrateur ne répond pas à ces exigences, la Société se réserve le droit de résilier le Contrat de Services professionnels conformément à l'article 25.
- 8.4.7 L'Intégrateur assume tous les frais inhérents à l'émission des attestations d'antécédents judiciaires.

11. PRIX

- 11.1 La Société s'engage à verser à l'Intégrateur la somme maximale de 370 602 829\$ excluant les taxes applicables (le « Prix maximal »), incluant toute somme payée dans le cadre de l'exécution de l'Entente de principe et des Avenants, à titre de considération pour la vente des Équipements et la prestation des Services professionnels, laquelle est ventilée conformément à l'annexe C.
- 11.2 La tarification applicable aux Services professionnels est décrite à l'annexe C.

18. CONFIDENTIALITÉ

L'Intégrateur s'engage à ce que ni lui ni aucune des Ressources de l'Intégrateur ne divulgue, sans y être dûment autorisé par la Société, les données, analyses ou résultats inclus dans les Biens livrables cédés, les Développements SAAQ, ou autres documents réalisés dans le cadre de l'exécution du Contrat de Services professionnels ou, généralement, quoi que ce soit dont il aurait eu connaissance dans l'exécution de celui-ci.

19. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

19.1 L'Intégrateur s'engage à se conformer aux obligations relatives à la protection des renseignements personnels stipulées à l'annexe N.

19.2 Les Ressources de l'Intégrateur assignés à l'exécution de ce Contrat de Services professionnels devront signer l'engagement de confidentialité prévu à l'annexe N.

31. ABSENCE DE RENONCIATION

Le fait pour une Partie de ne pas appliquer un article ou de ne pas exiger la stricte exécution d'un engagement contenu au Contrat de Services professionnels ou de ne pas exercer un droit ne doit pas être considéré comme une renonciation à une telle exigence ou à un tel droit.

EXTRAIT DES ANNEXES AU CONTRAT DE SERVICES PROFESSIONNELS ET DE VENTE D'ÉQUIPEMENTS

ANNEXE C – TAUX

CT19000010
P22899

Tarifs

Table des taux pour les 5 premières années

Livraison 0- Commun		Période de réalisation				
Domaine	Type_Ressources	Taux_Année 1	Taux_Année 2	Taux_Année 3	Taux_Année 4	Taux_Année 5
Formation initiale au projet	Ressources de l'alliance	235 \$	238 \$	241 \$	244 \$	247 \$
Planification du projet	Ressources de l'alliance	235 \$	238 \$	241 \$	244 \$	247 \$
Conception de la solution	Ressources de l'alliance	235 \$	238 \$	241 \$	244 \$	247 \$
Conception du modèle d'organisation du Centre d'expertise	Ressources de l'alliance	235 \$	238 \$	241 \$	244 \$	247 \$
Autres livraisons/ soutien, maintenance et exploitation		Période de réalisation				
Domaine	Type_Ressources	Taux_Année 1	Taux_Année 2	Taux_Année 3	Taux_Année 4	Taux_Année 5
Intégration fonctionnelle	Ressources de l'alliance	150 \$	152 \$	154 \$	156 \$	158 \$
	Team lead (ressources de l'alliance)	272 \$	276 \$	280 \$	284 \$	288 \$
Intégration technologique	Ressources de l'alliance	82 \$	83 \$	84 \$	85 \$	86 \$
	Team lead (Ressources de l'alliance)	272 \$	276 \$	280 \$	284 \$	288 \$
Gestion du changement	Ressources de l'alliance	140 \$	142 \$	144 \$	146 \$	148 \$
	Team lead (ressource de l'alliance)	272 \$	276 \$	280 \$	284 \$	288 \$
Communication	Ressources de l'alliance	140 \$	142 \$	144 \$	146 \$	148 \$
	Team lead (0 ressource)	272 \$	276 \$	280 \$	284 \$	288 \$
Formation	Ressources de l'alliance	140 \$	142 \$	144 \$	146 \$	148 \$
	Team lead (0 ressource)	272 \$	276 \$	280 \$	284 \$	288 \$
Assistance à la gestion, bureau de programme, intégration et assurance qualité	Coach (Ressources de l'alliance)	367 \$	372 \$	377 \$	382 \$	387 \$
	Expertise de pointe	350 \$	355 \$	360 \$	365 \$	370 \$
	Ressources de l'alliance	115 \$	116 \$	118 \$	120 \$	122 \$
	Team lead (Ressources de l'alliance)	272 \$	276 \$	280 \$	284 \$	288 \$

ANNEXE J

Guide à l'intention des consultants qui accomplissent un mandat à la Société

Ce guide, à l'usage des consultants qui accomplissent un mandat à la Société, se veut un rappel des obligations en matière d'éthique, de sécurité de l'information et de protection des renseignements personnels. Il est important de noter que les obligations présentées dans ce guide ne se substituent pas aux obligations légales ou contractuelles auxquelles sont soumis les consultants.

L'ÉTHIQUE

L'éthique est une façon de diriger nos comportements en faisant appel à notre jugement et à notre sens des responsabilités. Elle met l'accent sur les valeurs pour donner un sens à nos décisions et à nos actions. Ainsi, les valeurs apportent un éclairage dans la réflexion préalable à la prise de décisions. L'enjeu premier de l'éthique pour une organisation de services publics est de maintenir et de renforcer collectivement la confiance que les citoyens ont envers elle.

Ainsi, le consultant qui travaille à la Société est incité à appuyer ses actions et ses décisions sur les valeurs de l'organisation, soit l'engagement, la rigueur, la cohérence et le respect.

1. Chacun témoigne de son engagement en adhérant à la vision, à la mission et aux valeurs de la Société et en s'en inspirant quotidiennement.

Manifester son engagement c'est :

- faire preuve de leadership et influencer le milieu de travail par son comportement exemplaire, son sens critique et le dialogue;
- établir des relations interpersonnelles constructives visant le maintien d'un bon climat de travail;
- mettre en commun les efforts et prendre en compte les compétences particulières et les préoccupations des autres dans la réalisation de la mission de l'organisation.

L'engagement suppose une motivation du consultant à mettre ses idées et ses habiletés au service de la mission de l'organisation.

2. Chacun agit avec rigueur, c'est-à-dire avec professionnalisme, intégrité et équité.

Agir avec professionnalisme, c'est :

- S'assurer de respecter les délais prévus, avec tout le soin et toute l'attention nécessaires à un travail de qualité ;
- Chercher à tenir à jour et à améliorer ses connaissances ;
- Mettre à profit son habileté et son expérience pour atteindre les résultats visés.

Agir avec intégrité, c'est :

- Travailler avec honnêteté ;
- Utiliser de façon judicieuse l'information ou le matériel disponible pour l'exécution de son contrat, et non à des fins personnelles ou au profit d'un tiers ;
- Préserver son objectivité, son impartialité et sa crédibilité :
 - En s'abstenant d'accorder, de solliciter ou d'accepter toute faveur ou tout avantage indu pour soi-même ou pour une autre personne (par exemple, s'abstenir de communiquer avec un membre du comité de sélection d'adjudication de contrats afin d'influencer le processus d'adjudication ou de tenter d'obtenir plus de détails quant au résultat d'adjudication);
 - En évitant toute situation de conflit d'intérêts, réel ou apparent, et si une telle situation se présente, en informer immédiatement la Société.

Agir avec équité, c'est :

- Apprécier avec justesse ce qui est dû à chacun, en faisant preuve :
 - D'égalité de traitement (égalité devant la loi);
 - D'impartialité (intervenir sans préjugé, ni discrimination);
 - De jugement (reconnaître les particularités et les différences de certaines personnes pour assurer un juste traitement de leur dossier).

3. Chacun agit en toute cohérence avec la Société.

Agir avec cohérence, c'est :

- Favoriser l'esprit d'équipe ;
- Communiquer efficacement afin de favoriser la coordination des interventions et la production de services de qualité au meilleur coût ;
- Être responsable, c'est-à-dire :
 - Respecter les lois et les normes applicables au travail confié ;
 - Arrêter ses choix en considérant les conséquences sur les parties impliquées;
 - Pouvoir justifier ses décisions et en assumer les conséquences.

4. Chacun agit avec respect en maintenant une relation de confiance.

Agir avec respect, c'est :

- Être poli et courtois dans ses gestes et ses paroles ;
- Faire preuve de transparence et d'écoute ;
- Faire preuve de discrétion et de retenue ;
- S'abstenir de toute violence ou de tout harcèlement ;
- Dans ses communications, se présenter en précisant son statut et son mandat, y compris lors des réunions ;
- Permettre au personnel de la Société de respecter ses obligations de confidentialité et de protection des renseignements personnels ;
- Permettre aux professionnels de la Société de respecter leur obligation au secret professionnel ;
- Si un avis juridique est requis, demander au gestionnaire responsable de son contrat de faire une demande à la Direction des affaires juridiques.

LA SÉCURITÉ DE L'INFORMATION

La Société a mis en place diverses mesures de sécurité pour s'assurer de la confidentialité, de l'intégrité et de la disponibilité de l'information qu'elle détient. Il est de votre responsabilité de respecter ces mesures tout au long de votre mandat.

UTILISATION DE VOTRE CODE D'UTILISATEUR

Ce code sert à établir votre identité et à vous permettre d'accéder aux données dont vous avez besoin pour effectuer votre mandat. Il vous est attribué lors de votre entrée en fonction à la Société et est à votre usage exclusif. Vous êtes responsable des accès effectués sous votre code d'utilisateur.

Il est essentiel de verrouiller votre session lorsque vous vous absentez de votre poste de travail.

UTILISATION DE VOTRE MOT DE PASSE

Le mot de passe sert à valider votre identité. Il est important de le garder secret, sans quoi une personne qui le connaît pourrait usurper votre identité. Elle pourrait ainsi consulter, modifier ou même détruire des données et effectuer des opérations qui vous seraient imputées.

Si vous croyez que quelqu'un connaît votre mot de passe, vous devez immédiatement le changer.

UTILISATION DE VOTRE MICRO-ORDINATEUR

Si vous utilisez votre propre micro-ordinateur lors de l'exécution de votre mandat à la Société, vous devez vous assurer en tout temps de respecter les exigences mentionnées à votre contrat à cet égard (antivirus, système d'exploitation, mise à jour de logiciels, etc.). De l'information sur le sujet est également accessible dans l'[intranet](#) de la Société.

UTILISATION D'UNE CLÉ USB

Si vous devez utiliser une clé USB pour le transport d'informations, vous êtes tenu d'utiliser une clé USB sécuritaire, qui :

- Est pourvue d'un mécanisme de chiffrement ;
- Permet le chiffrement automatique de toutes données copiées sur la clé ;
- Est dotée d'un algorithme de chiffrement robuste (AES 256 bits au minimum).

À titre d'exemple, la clé USB « Kingston Data Traveler 4000 » répond aux exigences de sécurité de la Société.

UTILISATION DU COURRIEL

Seule l'adresse de courriel se terminant par « @saaq.gouv.qc.ca » doit être utilisée lors de communications effectuées au nom de la Société.

Il est interdit de transmettre à l'extérieur de la Société – par courriel, par collecticiel, par Internet ou par un autre moyen – tout renseignement de nature confidentielle qui n'a pas fait l'objet d'un chiffrement.

Vous ne devez jamais rediriger un « courriel SAAQ » sur un réseau non protégé (par exemple sur un téléphone intelligent, à votre entreprise, à un autre ministère ou organisme, ou à votre domicile). De même, vous ne devez jamais inciter un employé de la Société à vous transmettre des documents confidentiels sur des réseaux externes.

Toute information stockée ou consignée sur l'équipement électronique de la Société à l'aide d'un courriel, d'un collecticiel, d'Internet, ou par tout autre moyen, est réputée constituer une information à laquelle la Société a accès. Ainsi, la Société peut récupérer le contenu des boîtes de courriel si elle le juge opportun.

Enfin, au terme de votre mandat, vous devez effacer de votre boîte de courriel les renseignements personnels et les autres informations qui vous appartiennent. L'utilisation du courriel est un privilège qui peut vous être enlevé en tout temps, pour tout motif jugé raisonnable.

UTILISATION D'INTERNET

L'utilisation d'Internet est permise uniquement pour l'accomplissement de votre mandat à la Société.

La Société tient un registre quotidien des sites Internet visités par chaque utilisateur. Rappelez-vous que certains sites recueillent l'adresse de leurs visiteurs et publient parfois des statistiques à ce sujet. La *Politique d'utilisation du courriel et des services d'Internet de la Société* précise que : « les outils électroniques rendent possible l'identification de la Société par un interlocuteur externe et il faut en tenir compte lors de leur utilisation ».

Pour plus d'information, consultez la [Politique d'utilisation du courriel et des services d'Internet de la Société](#) (réf. : 08.11.0) dans l'intranet de la Société (Accueil>Outils spécialisés>Gestion-Soutien administratif>Cadre de gestion>Politiques et procédures).

SIGNALEMENT DES INCIDENTS

Vous devez rapporter rapidement tout problème de sécurité informatique (code malveillant, virus informatique, etc.) au centre d'assistance de la Société (tél. : 3210).

CONFIDENTIALITÉ DE L'INFORMATION

L'information communiquée par la Société est confidentielle, de même que celle que vous devez produire dans le cadre de votre mandat. À titre d'exemple, il peut s'agir de documentation ou d'information concernant des projets de développement, des plans d'action, des façons de faire actuelles ou envisagées, des mécanismes de sécurité, des contrôles ou des problèmes à corriger. Sauf si votre contrat de service prévoit le contraire ou si vous obtenez l'autorisation d'un représentant de la Société, cette information appartient à la Société et doit demeurer dans ses bureaux.

- Vous ne pouvez pas utiliser cette information à d'autres fins que la réalisation de votre mandat.
- Il vous est interdit de faire des copies des documents, que ce soit pour un usage personnel ou professionnel, ou pour une référence future.
- Vous ne pouvez pas communiquer l'information à d'autres personnes, à moins que cela ne soit requis pour l'exécution du mandat.

CONFIDENTIALITÉ DES DONNÉES INFORMATIQUES

La Société détient de nombreux renseignements sur ses usagers, son personnel et ses fournisseurs. Tous les renseignements se rapportant à des personnes physiques sont des renseignements personnels et confidentiels. Les renseignements se rapportant à des personnes morales et les autres données inscrites dans les systèmes informatiques de la Société sont aussi des renseignements confidentiels, même s'ils ne sont pas des renseignements personnels.

- La Société effectue des vérifications quotidiennes des consultations faites dans ses systèmes d'information.
- Il vous est strictement interdit de consulter et d'utiliser ces renseignements à d'autres fins que la réalisation de votre mandat.
- Avant de pouvoir accéder à des renseignements confidentiels sur les clientèles, le personnel ou les fournisseurs de la Société, vous devez signer un formulaire d'engagement à la confidentialité.
- Vous devez utiliser des données fictives pour les essais de système et les autres tests.

PROTECTION DES RENSEIGNEMENTS PERSONNELS

Afin d'assurer la confidentialité des renseignements personnels, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* énonce des règles précises. La Société les met en œuvre à l'aide des politiques et des procédures de son cadre de gestion, accessible dans l'intranet.

Ces règles concernent :

1. L'ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Toute personne physique a droit à la confidentialité des renseignements qui la concernent. Elle (ou son représentant autorisé) a le droit d'y accéder, d'en demander copie, ou de les faire rectifier.

Remarque : Vous n'êtes pas autorisé à traiter les demandes d'accès ou de rectification. Elles doivent être adressées à la Société le plus rapidement possible.

2. LA COLLECTE DE RENSEIGNEMENTS PERSONNELS

Lorsque votre contrat de service vous autorise à recueillir des renseignements personnels pour le compte de la Société, vous ne pouvez le faire que si ces renseignements sont nécessaires au traitement du dossier de la personne concernée ou à l'exécution de votre contrat.

La personne à qui l'on demande un renseignement personnel doit être informée :

- Du nom et de l'adresse de la Société ;
- Des fins pour lesquelles ce renseignement est recueilli ;
- Des catégories de personnes qui auront accès à ce renseignement ;

- Du caractère obligatoire ou facultatif de la demande ;
- Des conséquences en cas de refus de répondre à la demande ;
- Des droits d'accès et de rectification.

Un avis à cette fin doit être inclus dans tout formulaire de collecte de renseignements personnels, ou joint à celui-ci. Son contenu doit être approuvé par la Société.

3. L'UTILISATION DES RENSEIGNEMENTS PERSONNELS AU SEIN DE LA SOCIÉTÉ

L'utilisation de renseignements personnels sans le consentement de la personne concernée est strictement encadrée.

- Seules les personnes préalablement autorisées par la Société peuvent accéder aux renseignements personnels nécessaires à l'exercice de leurs fonctions, selon les accès qui leur sont attribués.
- Vous ne devez ni prendre connaissance ni utiliser les renseignements personnels détenus par la Société, sauf lorsqu'ils sont nécessaires à l'exercice des fonctions et des tâches qui vous sont confiées.
- La curiosité ou l'intérêt personnel ne justifient pas la consultation ou l'utilisation de renseignements personnels.
- Les renseignements personnels que vous utilisez pour rendre une décision au sujet d'une personne physique doivent être versés au dossier de cette personne, quel que soit le support sur lequel ces renseignements sont regroupés.
- Les renseignements personnels détenus par la Société doivent être à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été recueillis.

4. LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À UN TIERS

Lorsque votre contrat de service exige que vous communiquiez des renseignements personnels à des tiers, vous devez d'abord obtenir l'autorisation de la personne concernée. Cette autorisation doit être claire, donnée à des fins précises, et pour une durée déterminée.

En l'absence du consentement de la personne concernée, la communication de renseignements personnels à des tiers doit être préalablement approuvée par la Société et respecter les exigences administratives et de sécurité fixées par la Société.

5. LA CONSERVATION ET LA DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Les exigences de la Société relatives à la conservation et à la destruction des documents sont indiquées dans votre contrat de service. Nous tenons toutefois à vous rappeler que :

Vous ne pouvez pas utiliser à des fins personnelles des documents qui contiennent des renseignements personnels ou des informations confidentielles destinés à être jetés ou détruits. Le mode de destruction des documents contenant des renseignements personnels doit assurer la protection de la confidentialité.

Pour obtenir plus d'information, consultez le guide qui est joint à votre contrat de service.

6. L'UTILISATION DU TÉLÉCOPIEUR

Lorsque vous avez à transmettre par télécopieur des documents contenant des renseignements personnels, vous devez respecter les règles contenues dans la *Procédure pour l'envoi de documents confidentiels par télécopieur*. Avant d'entreprendre une communication par télécopieur, il est nécessaire de s'assurer que le destinataire est autorisé à obtenir les renseignements devant lui être communiqués.

Référence : [Procédure sur l'envoi de documents confidentiels par télécopieur](#) (réf. : 04.02.3) accessible dans l'intranet de la Société (Accueil>Outils spécialisés>Gestion-Soutien administratif>Cadre de gestion>Politiques et procédures).

CONSÉQUENCES DU NON-RESPECT DE CES RÈGLES

Le non-respect de ces règles constitue un manquement aux obligations de confidentialité du consultant.

Un bris de confidentialité résultant du non-respect de ces règles aurait des conséquences néfastes pour la Société. Il en aurait aussi pour le consultant, qui s'exposerait à des poursuites civiles, voire pénales, dans le cas d'un bris intentionnel, en plus d'autres conséquences prévues au contrat.

ANNEXE L

¹ Art. 21.13 *Loi sur les contrats des organismes publics*² Art. 40.5 *Règlement sur les contrats de travaux de construction des organismes publics*³ Attestation de Revenu QuébecCT19000010
P22899

**Condammations criminelles et pénales incompatibles avec les activités des
Ressources de l'intégrateur dans le cadre de l'exécution du contrat de services
professionnels**

CODE CRIMINEL (L.R.C. (1985), CH. C-46)

PARTIE II	INFRACTIONS CONTRE L'ORDRE PUBLIC
52. (1)	Sabotage
57. (1)	Faux ou usage de faux en matière de passeport
58. (1)	Emploi frauduleux d'un certificat de citoyenneté
PARTIE II.1	TERRORISME
83.02	Fournir ou réunir des biens en vue de certains actes
83.03	Fournir, rendre disponibles, etc., des biens ou services à des fins terroristes
83.04	Utiliser ou avoir en sa possession des biens à des fins terroristes
83.12 (1)	Infraction – blocage des biens, communication ou vérification (à l'exception de l'article 83.11)
83.18 (1)	Participation à une activité d'un groupe terroriste
83.19 (1)	Facilitation d'une activité terroriste
83.2	Infraction au profit d'un groupe terroriste
83.21 (1)	Charger une personne de se livrer à une activité pour un groupe terroriste
83.22 (1)	Charger une personne de se livrer à une activité terroriste
83.23	Héberger ou cacher une personne ayant commis une activité terroriste
PARTIE IV	INFRACTIONS CONTRE L'APPLICATION DE LA LOI ET L'ADMINISTRATION DE LA JUSTICE
119 (1)	Corruption de fonctionnaires judiciaires, etc.
120.	Corruption de fonctionnaires
121. (1)	Fraudes envers le gouvernement
122.	Abus de confiance pour un fonctionnaire public
123. (1)	Actes de corruption dans les affaires municipales
123. (2)	Influencer un fonctionnaire municipal
130.	Prétendre faussement être un agent de la paix
134. (1)	Parjure
136. (1)	Témoignages contradictoires
137.	Fabrication de preuve
138.	Infractions relatives aux affidavits
139. (2)	Entrave à la justice
140.(1) et (2)	Méfait public
142.	Acceptation vénale d'une récompense pour le recouvrement d'effets
PARTIE V	INFRACTIONS D'ORDRE SEXUEL, ACTES CONTRAIRES AUX BONNES MŒURS, INCONDUITE
163.1 (2) (3) (4) (4.1)	Pornographie juvénile

PARTIE VI	ATTEINTES À LA VIE PRIVÉE
184. (1)	Interception
184.5 (1)	Interception de communications radiotéléphoniques
193. (1)	Divulgaration de renseignements
193.1	Divulgaration de renseignements obtenus par suite de l'interception d'une communication radiotéléphonique
PARTIE VIII	INFRACTIONS CONTRE LA PERSONNE ET LA RÉPUTATION
264. (1)	Harcèlement criminel
264.1 (1)	Proférer des menaces
271. (1)	Agression sexuelle
272. (1)	Agression sexuelle armée, menaces à une tierce personne ou infraction de lésions corporelles
273. (1)	Agression sexuelle grave
279. (1)	Enlèvement
279.1 (1)	Prise d'otage
280. (1)	Enlèvement d'une personne âgée de 16 ans et moins
281.	Enlèvement d'une personne âgée de 14 ans et moins
282. (1)	Enlèvement en contravention d'une ordonnance de garde
PARTIE IX	INFRACTIONS CONTRE LES DROITS DE PROPRIÉTÉ
322. (1)	Vol (valeur dépassant 5 000 \$)
326. (1) b)	Vol de service de télécommunication
328.	Vol par une personne ou d'une personne ayant un droit de propriété ou intérêt spécial
330. (1)	Vol par une personne tenue de rendre compte
331.	Vol par une personne détenant une procuration
336.	Abus de confiance criminel
337.	Employé public qui refuse de remettre des biens
340.	Destruction de titres
341.	Fait de cacher frauduleusement
342. (3)	Utilisation non autorisée de données relatives à une carte de crédit
342.01 (1)	Fabrication ou possession d'instruments destinés à fabriquer ou à falsifier des cartes de crédit
342.1 (1)	Utilisation non autorisée d'ordinateur
342.2 (1)	Possession de moyens permettant d'utiliser un service d'ordinateur
346. (1)	Extorsion
353. (1)	Fait de vendre, etc., un passe-partout d'automobile
354. (2)	Possession d'un véhicule à moteur dont le numéro d'identification a été oblitéré
363.	Obtention par fraude de la signature d'une valeur
366. (1) et 367	Faux
369. b) c)	Papier de bons du Trésor, sceaux publics, etc.
372. (1)	Faux messages
374.	Rédaction non autorisée d'un document
375.	Obtenir, etc., au moyen d'un instrument fondé sur un document contrefait
376. (2)	Contrefaçon d'une marque
377. (1)	Documents endommagés
378.	Infractions relatives aux registres

PARTIE X	OPÉRATIONS FRAUDULEUSES EN MATIÈRE DE CONTRATS ET DE COMMERCE
380. (1)	Fraude
392.	Aliénation de biens avec l'intention de frauder des créanciers
397. (1)	Livres et documents
397. (2)	Pour frauder ses créanciers (contribue à l'accomplissement d'une infraction visée au paragraphe 1)
403.	Supposition intentionnelle de personne
405.	Reconnaissance d'un instrument sous un faux nom
407.	Contrefaçon d'une marque de commerce
409. (1)	Instruments pour contrefaire une marque de commerce
417. (1)	Application ou enlèvement de marques sans autorisation
417. (2)	Opérations illicites à l'égard d'approvisionnements publics
418. (1)	Vente d'approvisionnements défectueux à Sa Majesté
418. (2)	Infractions (au paragraphe 1) par dirigeants et employés de personnes morales
423. (1)	Intimidation
423.1 (1)	Intimidation d'une personne associée au système judiciaire ou d'un journaliste
424.	Menaces de commettre une infraction contre une personne jouissant d'une protection internationale
426. (1)	Commissions secrètes
426. (2)	Fait de contribuer à l'infraction (visée au paragraphe 1)
PARTIE XI	ACTES VOLONTAIRES ET PROHIBÉS CONCERNANT CERTAINS BIENS
430. (1)	Méfait (bien – valeur dépassant 5 000 \$)
430. (1.1)	Méfait concernant des données
431.	Attaque contre les locaux officiels, le logement privé ou les moyens de transport d'une personne jouissant d'une protection internationale
431.1	Attaque contre les locaux officiels, le logement privé ou les moyens de transport du personnel des Nations Unies ou du personnel associé
PARTIE XII	INFRACTIONS RELATIVES À LA MONNAIE
457. (3)	Infraction (au paragraphe 1 : Chose ressemblant à un billet de banque)
PARTIE XII.2	PRODUITS DE LA CRIMINALITÉ
462.31 (1)	Recyclage des produits de la criminalité
463.	Punition de la tentative et de la complicité
464.	Conseiller une infraction qui n'est pas commise
465. (1)	Complot
465. (3)	Complot en vue de commettre une infraction
467.11 (1)	Participation aux activités d'une organisation criminelle
467.12 (1)	Infraction au profit d'une organisation criminelle
467.13 (1)	Charger une personne de commettre une infraction

LOI RÉGLEMENTANT CERTAINES DROGUES ET AUTRES SUBSTANCES (L.C. 1996, CH. 19)

Les articles retenus visent le trafic, l'importation, l'exportation et la production de substances, art. 5, 6 et 7.

ANNEXE N

Protection des renseignements personnels et confidentiels

1. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

1.1 Définitions

« **Renseignement personnel** » : tout renseignement qui concerne une personne physique et qui permet de l'identifier.

« **Renseignement confidentiel** » : tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la Loi sur l'accès, notamment un renseignement ayant des incidences sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques ou sur la vérification.

1.2 L'Intégrateur s'engage envers la Société à respecter chacune des dispositions applicables aux renseignements personnels et confidentiels ci-dessous énumérées; que ces renseignements lui soient communiqués dans le cadre de l'exécution de ce Contrat ou soient générés à l'occasion de son exécution.

1.2.1 Informer son personnel des obligations stipulées aux présentes dispositions et diffuser à cet égard toute l'information pertinente.

1.2.2 Rendre accessibles les renseignements personnels, au sein des membres de son personnel, uniquement à ceux qui ont qualité pour les recevoir, lorsqu'ils sont nécessaires à l'exercice de leurs fonctions et sont utilisés aux fins pour lesquelles ils ont été recueillis ou que la loi autorise leur utilisation.

1.2.3 Faire signer aux membres de son personnel, préalablement à l'accès à des renseignements personnels et confidentiels, des engagements au respect de la confidentialité de ces renseignements selon l'Engagement de confidentialité joint au présent document et les transmettre aussitôt à la Société, sous peine de se voir refuser l'accès aux locaux, à l'équipement de la Société ou aux données à être transmises par celle-ci, le cas échéant.

1.2.4 Ne pas communiquer les renseignements personnels, sans le consentement de la personne concernée, à qui que ce soit, sauf dans le cadre d'un sous-contrat et selon les modalités prévues au paragraphe 1.12.13, et le cas échéant, soumettre à l'approbation de la Société le formulaire de consentement à la communication de renseignements personnels de la personne concernée.

1.2.5 Utiliser les renseignements personnels uniquement pour la réalisation du Contrat.

- 1.2.6 Recueillir un renseignement personnel au nom de la Société, dans les seuls cas où cela est nécessaire à la réalisation du Contrat et informer préalablement toute personne visée par cette cueillette de l'usage auquel ce renseignement est destiné, ainsi que des autres éléments mentionnés à l'article 65 de la Loi sur l'accès.
- 1.2.7 Prendre toutes les mesures de sécurité propres à assurer la confidentialité des renseignements personnels et confidentiels à toutes les étapes de la réalisation du Contrat et, le cas échéant, les mesures identifiées à l'Engagement de confidentialité joint au présent document.
- 1.2.8 Ne conserver, à l'expiration du Contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, en les retournant à la Société dans les 60 jours suivant la fin du Contrat et remettre à la Société une confirmation que elle et les membres de son personnel ont retourné tous ces documents.
- 1.2.9 Informer, dans les plus brefs délais, la Société de tout manquement aux obligations prévues aux présentes dispositions ou de tout événement pouvant risquer de porter atteinte à la sécurité ou à la confidentialité des renseignements personnels ou confidentiels.
- 1.2.10 Fournir, à la demande de la Société, toute l'information pertinente au sujet de la protection des renseignements personnels et confidentiels et donner accès à toute personne désignée par la Société, à la documentation, aux systèmes, aux données et aux lieux physiques relatifs au Contrat afin de s'assurer du respect des présentes dispositions.
- 1.2.11 Se conformer aux objectifs et aux exigences de sécurité de l'information définis par la Société.
- 1.2.12 Obtenir l'autorisation écrite de la Société avant de communiquer ou de transférer quelque donnée que ce soit, même à des fins techniques, hors du Québec.
- 1.2.13 Lorsque la réalisation du présent Contrat est confiée à un sous-contractant et qu'elle comporte la communication de renseignements personnels et confidentiels par l'Intégrateur au sous-contractant ou la cueillette de renseignements personnels et confidentiels par le sous-contractant :
 - soumettre à l'approbation de la Société la liste des renseignements personnels et confidentiels communiqués au sous-contractant;
 - conclure un contrat avec le sous-contractant stipulant les mêmes obligations que celles prévues aux présentes dispositions;
 - exiger du sous-contractant qu'il s'engage à ne conserver, à l'expiration du sous-contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support,

et à remettre à l'Intégrateur, dans les 60 jours suivant la fin de ce contrat, un tel document.

- 1.2.14 Transmettre de façon sécuritaire les renseignements personnels ou confidentiels lorsque ceux-ci sont communiqués par courriel ou Internet. Ces renseignements doivent nécessairement faire l'objet d'un chiffrement ou être protégés par un dispositif de sécurité éprouvé. Si les renseignements personnels ou confidentiels sont acheminés par télécopieur, l'émetteur du document doit s'assurer que le récepteur est habilité à le recevoir et qu'il prendra toutes les mesures nécessaires à la protection de ces renseignements. Toutefois, les parties peuvent convenir entre elles de tout autre moyen (à l'exception d'une clé USB), telle la remise en mains propres, la messagerie ou la poste recommandée en indiquant toujours sur l'enveloppe la mention « personnel et confidentiel ».
- 1.3 La fin du Contrat ne dégage aucunement l'Intégrateur et le sous-contractant de leurs obligations et engagement relatifs à la protection des renseignements personnels et confidentiels.
- 1.4 La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels peut être consultée à l'adresse suivante : <http://www.publicationsduquebec.gouv.qc.ca>.

ANNEXE N
ENGAGEMENT DE CONFIDENTIALITÉ

Je, soussigné(e), _____, exerçant mes fonctions au sein de

(Nom de la personne)

_____, déclare formellement ce qui suit.

(Nom de l'alliance)

Je suis un(e) employé(e) de cette entreprise et, à ce titre, j'ai été affecté(e) à l'exécution du contrat de services concernant _____

(Objet du contrat)

entre la Société de l'assurance automobile du Québec et mon employeur en date du

_____.
(Date)

Je m'engage, sans limite de temps, à garder le secret le plus entier, à ne pas communiquer ni permettre que soit communiqué à quiconque quelque renseignement ou document, quel qu'en soit le support, qui me sera communiqué ou dont je prendrai connaissance dans l'exercice ou à l'occasion de l'exécution de mes fonctions, à moins d'avoir été dûment autorisé(e) à ce faire par la Société de l'assurance automobile du Québec ou par l'un de ses représentants autorisés.

Je m'engage également, sans limites de temps, à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre des rapports contractuels entretenus entre mon employeur et la Société de l'assurance automobile du Québec.

J'ai été informé(e) que le défaut par le (la) soussigné(e) de respecter tout ou partie du présent engagement de confidentialité m'expose ou expose mon employeur à des recours légaux, des réclamations, des poursuites et toutes autres procédures en raison du préjudice causé pour quiconque est concerné par le contrat précité.

Facultatif

Je reconnais avoir lu les règles relatives à l'éthique et à la sécurité de l'information décrites dans le « Guide à l'intention des consultants qui accomplissent un mandat à la Société de l'assurance automobile du Québec » (à l'annexe 8) et m'engage à les respecter.

Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.

ET J'AI SIGNÉ À _____ CE _____ JOUR DU MOIS DE _____ DE L'AN _____

(Signature du déclarant ou de la déclarante)

ADDENDA

N° 7

Question 77 :

Par ailleurs, considérant que l'entente de confidentialité généralement est à remettre avant la signature du contrat, nous sommes d'avis qu'une note de particularité est manquante à la page 4 du cahier réponse, annexe 9, point 9 — « Engagement de confidentialité ».

Pouvez-vous ajouter la particularité « (1) : À remettre avant la signature du contrat » à la page 4 du cahier réponse, annexe 9, point 9 — « Engagement de confidentialité »?

Réponse 77:

Tel que spécifié à l'article 6.9.2, l'entente de confidentialité doit être signée préalablement par le personnel de l'Alliance et/ou des fournisseurs qui auront accès à des renseignements personnels et confidentiels. Donc, toute ressource confirmée et acceptée par la Société devant réaliser des travaux dans le cadre du présent contrat devra signer l'annexe 9 avant son entrée en fonction à la Société, et ceci est valable pendant toute la durée du contrat.

Question 86 :

Dans les sections 2.x.4 « Bassin d'expertise » du cahier réponses, il est mentionné que « l'alliance doit démontrer qu'elle dispose d'un nombre suffisant de conseillers pour combler l'ensemble des postes requis. ». Nous comprenons que l'alliance doit présenter son bassin mondial de ressources ayant les compétences requises ainsi que celles aptes à travailler en français à Québec. Il nous est donc permis de croire que la Société permettra le travail hors Québec.

Sachant qu'au cours des dernières années d'autres organisations/ministères ont envisagé dans le cadre d'appel d'offres de permettre la prestation de services à distance à l'extérieur du Québec et que cela a toujours été remis en cause suite à des pressions politiques et/ou sociales. Nous aimerions savoir si nous pouvons envisager faire réaliser des travaux par des ressources à distance localisées dans des bureaux à l'extérieur du Québec? Si oui, dans quelle proportion les travaux pourront être faits par des ressources localisées au Québec versus à l'extérieur du Québec?

Réponse 86:

Nous vous confirmons qu'il est envisageable que des travaux soient réalisés à distance, et localisées dans des bureaux à l'extérieur du Québec. Toutefois tel que mentionné à la section '2.10.8 Modalités d'exécution du mandat', à la page 112 du document d'appel d'offres, la production des documents ainsi que les communications orales et écrites s'effectuent en français. Concernant la proportion des travaux réalisés hors Québec, il s'agit davantage de la nature des travaux à réaliser tels que :

- Des travaux de réalisation (aucune conception) comme du développement spécifique ou « sur mesure » ou encore du paramétrage TRÈS complexe. Dans un tel contexte, l'alliance devra s'assurer, en plus de fournir la documentation en français, du transfert de connaissance auprès des ressources de la Société;
- Le recours à des expertises de pointe pour un court laps de temps ce qui ne justifie pas un déplacement.

Et ce toujours dans le respect de la condition d'admissibilité 4.15.1.7, à la page 239 de l'appel d'offres, soit :

'La soumission doit être présentée par une alliance ou par des fournisseurs composant l'alliance dans le cas où l'alliance est non juridiquement organisée ayant, au Québec ou dans un des territoires visés par les accords intergouvernementaux applicables, un établissement où il exerce ses activités de façon permanente, clairement identifié à son nom et accessible durant les heures normales de bureau.'

APPEL D'OFFRES AMENDÉ

2.5.8 AO SECTION 2.10.12 - INTÉGRATION TECHNOLOGIQUE

Les détails inclus dans cette section représentent des précisions applicables à la section 2.10.12 du document d'appel d'offres.

2.5.8.1 AO SECTION 2.10.12.4 - Services requis

C. Domaine conception, réalisation et évolution de la solution informationnelle (BI)

Certaines responsabilités de ce domaine ont été transférées en intégration fonctionnelle du côté de l'intelligence d'affaires (Bâtons rouges). Les responsabilités maintenant associées au domaine de la conception, réalisation et évolution de la solution informationnelle BI (Bâtons bleus) sont entre autres :

- Élaboration de l'architecture technologique cible de la solution informationnelle;
- Paramétrage des composants techniques assurant l'intégration entre les composants de la solution informationnelle et :
 - les composants de la solution opérationnelle;
 - si requis, les systèmes patrimoniaux.

E. Domaine d'infrastructure technologique, exploitation et opérations

En introduction à la présente section, la Société désire signifier aux soumissionnaires son ouverture à un modèle de gestion des infrastructures caractérisé par une approche de type

service. Bien qu'à la base, la Société vise le déploiement, le soutien et l'exploitation de l'infrastructure technologique dans un mode de partenariat Société /Alliance, elle se dit disposée à considérer une offre clé en main. L'ouverture de la Société à ce chapitre est motivée par son souci de capitaliser sur toutes les opportunités qu'amènent l'évolution des technologies et les nouvelles pratiques en TI. Toutefois, la position de la Société face à la localisation physique des équipements demeure la même en ce sens, que l'on vise a priori un déploiement sur site.

Le soumissionnaire doit présenter, à même le cahier réponse, l'essence de sa proposition. Il doit aussi faire la démonstration des avantages que confère sa proposition notamment au plan commercial et en termes de la capacité à soutenir le plan de mise en œuvre du programme.

Dans le cadre d'une telle proposition, la Société aurait la responsabilité d'effectuer la gouvernance des services offerts ainsi que la reddition de compte et le suivi des niveaux de services. Conséquemment, la Société s'entend à ce que le soumissionnaire lui propose à même son offre tous les moyens nécessaires (cadre de gestion et outils) pour supporter cette gestion dans un contexte à la fois intègre et convivial.

Bien que la Société démontre de l'ouverture, elle se dit néanmoins soucieuse de la constitution de l'équipe et surtout de la localisation géographique de cette dernière. Cette équipe doit intervenir à la fois au plan de l'exploitation et en soutien aux équipes de réalisation du programme, sa proximité avec les équipes sur place revêt donc une grande importance.

La Société tient à préciser qu'une telle proposition ne doit en rien hypothéquer la vélocité des équipes de réalisation et le rythme de livraison du programme. En ce sens, la Société s'attend du soumissionnaire à ce qu'il dépose à même sa proposition un plan d'effectifs en infrastructure pour toute la durée du programme en identifiant leur localisation. Le nombre de spécialistes sur place doit être suffisant pour répondre aux impératifs de livraison du programme.

Dans sa proposition, le soumissionnaire doit aussi considérer le fait que la Société désire acquérir l'expertise nécessaire dans le domaine des infrastructures technologiques de manière à pouvoir interagir judicieusement avec les principaux intervenants de l'Alliance. En ce sens, la Société s'attend du soumissionnaire à ce qu'il lui propose des moyens ou des stratégies qui viendront supporter l'atteinte de cet objectif.

SOUSSION AMENDÉE

LGS-IBM/SAP

La Société désire obtenir de la part de l'Alliance les grandes lignes de son approche de sécurité qui soutiendra la consommation de services de type infonuagique. Les informations fournies doivent être suffisamment détaillées pour permettre à la Société d'apprécier la position de l'Alliance en vertu des risques et enjeux généralement rencontrés dans ce mode de consommation. Veuillez noter que cette rubrique est pour fins d'information seulement.

Réponse de l'Alliance

La stratégie de sécurité supportant la consommation de services de type infonuagique est basée sur la mise en place d'une extension du domaine de Sécurité de la Société. En effet outre l'aspect technique supportant l'interconnexion sécuritaire via l'utilisation de réseaux virtuels privés (VPN) permettant de sécuriser et d'isoler les échanges d'information entre le domaine interne de la Société et les infrastructures de service infonuagique, nous avons prévu la mise en place des processus, outils et approches de gestion supportant une utilisation sécuritaire des offres de services infonuagique.

Principes d'intégration de l'infonuagique :

- Sélection de fournisseurs reconnus supportant un contexte de sécurité équivalent ou supérieur aux exigences de la Société;
- Utilisation de canaux de communication entièrement sécurisés via les dernières technologies en matière de chiffrement;
- Utilisation des bases de sécurités basée sur le domaine interne de la société (Répertoire d'entreprise, solution de gestion, profil d'accès) pour l'accès et la gestion aux services d'infonuagique;
- Fonction de journalisation permettant de supporter les besoins de la Société en matière de traçabilité des actions;
- Intégration des pratiques et des outils de surveillance de la société;
- Intégration aux processus de gestion de la sécurité de la Société.

Notre approche d'utilisation des services Infonuagique supporte le niveau d'isolation, de segmentation et de sécurité nécessaire à la rencontre des requis de sécurité pour la SAAQ.

Notre solution pourra évoluer pour inclure davantage de services types infonuagiques ou vers des modes de types hybrides chez IBM ou autre partenaire, en fonction de la stratégie de la société ou du type d'utilisation. Par exemple, l'utilisation de service de type multientité (multitenant) pourrait être supportée pour l'intégration de certaines solutions infonuagique à des environnements de développement (SandBox, Dev) afin d'offrir des avantages visant une réduction des coûts d'utilisation des solutions infonuagique.

Chaque offre de type Infonuagique publiée via les ententes de service (SLA) les éléments de gouvernance, de sécurité, de conformité et les niveaux de responsabilités assumés par le fournisseur de service, ces documents ont fait l'objet d'une analyse préalable à la sélection de tout offre de type infonuagique afin de s'assurer que le service sélectionné rencontre ou dépasse les requis pour l'utilisation visée.

De façon générale notre approche de gestion des services de type infonuagique est fortement inspirée des guides et des recommandations produites par le Cloud Security Alliance. Le diagramme qui suit présente la vue globale des éléments adressés lors de la sélection et de l'utilisation d'une offre de service Infonuagique à notre solution.

Cahier réponse P2

1.05	Intégration du développement majeur fait par l'éditeur (CDP) dans la solution	Évaluation basée sur notre expérience d'intégration de développements similaires sur d'autres projets, la livraison du développement par l'éditeur a été un enjeu important pour les échéanciers.	3	4	Élevé	1	4	Faible	- Intégrer l'équipe du CDP aux sprints; - Réalisation à l'aide de sprints itératifs; - Intégrer la stratégie de livraison des lots et des CDP dès la livraison 0; - Définition détaillée des requis lors de la livraison 0; - Travailler étroitement avec l'éditeur tout au long du programme; - Prévoir la réalisation des cas d'essais à automatiser ainsi que des essais intégrés des processus de la solution déjà en opération; - Révision de la livraison du CDP à travers le Comité
------	---	---	---	---	-------	---	---	--------	--

Cahier réponses - P22899-3: Appel d'offres de suite de progiciels de gestion intégrés
Étape G: Sélection de la solution d'affaires et des services professionnels

©La Société de l'assurance automobile du Québec 2016

413

LGS-IBM/SAP

Facteur de risque		Évaluation - Dialogue				Niveau résiduel anticipé		
No	Description	Commentaires / Justification	Vulnérabilité actuelle	Impact actuel	Niveau de risque actuel	Vulnérabilité résiduelle	Impact résiduel	Niveau de risque résiduel
								d'intégration Technique et le Comité d'Assurance Qualité; • Faire appel aux experts SAP faisant partie du bassin d'expertise élargi de l'alliance, tels que les experts de domaine (« SAP - Subject Matter Expert »); • Prévoir des contrôles d'assurance qualité de l'éditeur; • Développer le CDP en approche Agile sur l'environnement de la Société; • Allouer une plage de temps réaliste dans le plan de livraison intégrée.

CAPACITE DE L'ALLIANCE A FOURNIR LES RESSOURCES REQUISES

L'envergure du programme de transformation de la Société requiert un grand nombre de ressources dans de nombreuses spécialités entourant le déploiement des logiciels SAP. L'alliance est consciente des exigences de disponibilité de ressources de ce type et est en mesure d'y faire face avec une grande vélocité grâce aux éléments suivants :

Vaste bassin de conseillers disponibles : En plus de la pratique Canadienne d'IBM sur SAP, l'alliance peut compter sur son bassin mondial de ressources (Global Delivery Centers). D'ailleurs, pour couvrir les pointes de ressources requises, l'alliance met déjà à contribution 3 de ses centres de développement, soit le nouveau centre de Montréal nouvellement ouvert le 29 novembre 2016, le centre d'Halifax en Nouvelle-Écosse et finalement celui de Kolkata en Inde. Cette capacité étendue permettra à l'alliance de pallier à toutes les périodes de pointes, planifiées ou non, au cours du déroulement du programme de transformation. L'alliance a également établi des ententes de partenariats stratégiques avec des firmes de consultation spécialisées dans la livraison de projets SAP afin d'augmenter son bassin de ressources disponibles pour la réalisation du programme de la Société.

Recrutement anticipé de ressources stratégiques : L'alliance a amorcé un processus d'embauche anticipée de ressources stratégiques afin de s'assurer que l'expertise requise au début des travaux soit disponible. À cet effet, l'alliance a organisé des campagnes de recrutement à travers le Canada et en France visant l'acquisition de talents pertinents aux domaines d'affaires de la Société. Ce processus fait l'objet de suivi très serré par le leadership de l'alliance afin d'atteindre les objectifs ciblés.

Accès aux experts de domaine de pointe : Au besoin, pour faire face à des problématiques pointues, l'alliance mettra à contribution des experts de domaine (SME – Subject Matter Experts) possédant une expérience étendue dans l'implantation des composants SAP. Bien que ces ressources ne soient pas nécessairement francophones, elles permettront, dans certains cas, de résoudre plus rapidement et plus efficacement les problèmes complexes qui pourraient survenir.

Cahier réponses - P22899-3: Appel d'offres de suite de progiciels de gestion intégrés
Étape G: Sélection de la solution d'affaires et des services professionnels

©La Société de l'assurance automobile du Québec 2016

447

LGS-IBM/SAP

Partenariat avec l'Université Laval : L'alliance a établi un partenariat avec l'Université Laval à Québec afin d'établir un programme de formation pour des ressources juniors. Cette approche permettra le développement d'un bassin de ressources locales francophones qui augmentera les effectifs permettant d'assurer la relève.

SOUMISSION

Pages 1207 à 1211

Un mécanisme bien rodé

Pour le volet intégration technologique, nous reprenons le mécanisme de recours au bassin de ressources de l'alliance décrit à la section 2.14.4, qui repose sur **un plan d'assignation** mis en place dès le départ, une **gestion par anticipation** pour grossir les rangs des spécialistes appelés sur les étapes successives, et **la croissance et formation** de ressources à potentiel, au travers du programme « *Consulting by Degrees* ».

Ici, il est utile de **rappeler les mécanismes de coordination et de cohésion avec les équipes du programme ainsi que les mécanismes d'interrelations entre les différentes équipes du chantier TI** décrits dans l'approche (Cf. 2.15.1). **Ce sont eux qui déclenchent celui de recours au bassin de ressources de l'alliance.**

Les tableaux suivants présentent le nombre d'employés recensés dans le système de ressources humaines de l'Alliance et de ceux de nos partenaires selon le bassin d'expertise en intégration technologique en lien avec l'organigramme présenté dans l'approche de cette section :

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : ARCHITECTURE ET INGÉNIERIE / Infrastructure					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	33	43	140	216	5
Alliance	25	33	105	162	4
Sous-contractants	8	11	35	54	1
Aptes à travailler à Québec en français	2	4	14	20	5
Alliance	1	3	11	15	4
Sous-contractants	1	1	4	6	1

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : ARCHITECTURE ET INGÉNIERIE / <u>Basis</u>					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	104	137	444	685	14
Alliance	78	103	333	514	10
Sous-contractants	26	34	111	171	4
Aptes à travailler à Québec en français	2	13	44	59	14
Alliance	1	10	33	44	10
Sous-contractants	1	3	11	15	4

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : ARCHITECTURE ET INGÉNIERIE / <u>Sécurité</u>					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	16	73	163	252	6
Alliance	12	55	123	190	5
Sous-contractants	4	18	41	63	1
Aptes à travailler à Québec en français	2	7	16	25	6
Alliance	1	5	12	18	5
Sous-contractants	1	2	4	7	1

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION OPÉRATIONNELLE / <u>ABAP</u>					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	124	562	1 261	1 947	40
Alliance	93	422	945	1 460	35
Sous-contractants	31	141	315	487	5
Aptes à travailler à Québec en français	12	56	126	195	20
Alliance	9	42	95	146	15
Sous-contractants	3	14	32	49	5

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION OPÉRATIONNELLE / <u> </u>					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	14	62	140	216	10
Alliance	10	47	105	162	8
Sous-contractants	3	16	35	54	2
Aptes à travailler à Québec en français	1	6	14	21	10
Alliance	1	5	11	17	8
Sous-contractants	0	2	4	5	2

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION OPÉRATIONNELLE / .Net					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	43	122	313	478	7
Alliance	20	47	105	172	5
Sous-contractants	23	75	208	306	2
Aptes à travailler à Québec en français	43	122	313	478	7
Alliance	20	47	105	172	5
Sous-contractants	23	75	208	306	2

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION OPÉRATIONNELLE / Opent text					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	14	62	140	216	5
Alliance	10	47	105	162	5
Sous-contractants	3	16	35	54	0
Aptes à travailler à Québec en français	1	6	14	21	5
Alliance	1	5	11	16	5
Sous-contractants	0	2	4	5	0

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION OPÉRATIONNELLE / Hybris					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	23	104	233	360	8
Alliance	17	78	175	270	6
Sous-contractants	6	26	58	90	2
Aptes à travailler à Québec en français	1	10	23	35	8
Alliance	1	8	18	26	6
Sous-contractants	0	3	6	8	2

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION OPÉRATIONNELLE / iXM					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	16	73	163	252	4
Alliance	12	55	123	189	3
Sous-contractants	4	18	41	63	1
Aptes à travailler à Québec en français	1	7	16	25	4
Alliance	1	5	12	19	3
Sous-contractants	0	2	4	6	1

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION OPÉRATIONNELLE / Essais					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	85	385	864	1 334	38
Alliance	64	289	648	1 000	30
Sous-contractants	21	96	216	333	8
Aptes à travailler à Québec en français	1	39	86	126	38
Alliance	1	29	65	95	30
Sous-contractants	0	10	22	31	8

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : SOLUTION INFORMATIONNELLE / Information de gestion					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	28	125	280	433	8
Alliance	21	94	210	324	6
Sous-contractants	7	31	70	108	2
Aptes à travailler à Québec en français	1	12	28	42	8
Alliance	1	9	21	31	6
Sous-contractants	0	3	7	10	2

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : CONVERSION / Master Data Governance					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	14	62	140	216	4
Alliance	10	47	105	162	3
Sous-contractants	3	16	35	54	1
Aptes à travailler à Québec en français	1	6	14	21	4
Alliance	1	5	11	16	3
Sous-contractants	0	2	4	5	1

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : CONVERSION / Expert conversion					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	32	146	327	505	10
Alliance	24	109	245	379	8
Sous-contractants	8	36	82	126	2
Aptes à travailler à Québec en français	1	15	33	48	10
Alliance	1	11	25	36	8
Sous-contractants	0	4	8	12	2

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : INFRASTRUCTURE ET EXPLOITATION / Infrastructure					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	34	156	350	541	11
Alliance	26	117	263	406	9
Sous-contractants	9	39	88	135	2
Aptes à travailler à Québec en français	1	16	35	52	11
Alliance	1	12	26	39	9
Sous-contractants	0	4	9	13	2

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : INFRASTRUCTURE ET EXPLOITATION / Basis					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	41	187	420	649	14
Alliance	31	141	315	487	10
Sous-contractants	10	47	105	162	4
Aptes à travailler à Québec en français	1	19	42	62	14
Alliance	1	14	32	47	10
Sous-contractants	0	5	11	15	4

Grille SP.3 - Bassin d'expertise en intégration technologique					
INTÉGRATION TECHNOLOGIQUE					
PROFIL : INFRASTRUCTURE ET EXPLOITATION / Sécurité/ITIL					
Nbre de conseillers	Seniors (plus de 10 ans d'expérience)	Intermédiaires (5 à 10 ans d'expérience)	Juniors (moins de 5 ans d'expérience)	Total	Équipe proposée en 1) Approche préconisée
Total	48	219	490	757	18
Alliance	36	164	368	568	16
Sous-contractants	12	55	123	189	2
Aptes à travailler à Québec en français	2	22	49	73	18
Alliance	1	16	37	54	16
Sous-contractants	1	5	12	19	2

*Réponse de l'alliance***A. Préoccupation de la santé financière de chacun des partenaires de l'alliance**

L'alliance LGS/IBM et SAP a été conçue avec des objectifs de solidité et de pérennité, pour assurer la livraison harmonieuse du projet de la Société. Elle est alignée sur le modèle d'affaires habituel de ses membres et sur des pratiques et méthodologies de travail conjoint qui ont fait leur preuve et évolué au fil des milliers de projets d'implantation qu'ils ont réalisés ensemble au cours des dernières décennies. Étant donné que le projet de la Société contient des particularités uniques, l'alliance comprend des adaptations spécifiques au contexte visant un alignement aux besoins et défis que présente ce projet.

L'entente créant l'alliance prévoit un départage précis et complet de l'ensemble des éléments de la portée à couvrir. Ainsi, chaque composante du projet se retrouve avec un représentant identifié et responsable. La répartition des responsabilités a été alignée sur les forces respectives de chaque membre qui se retrouve ainsi en terrain connu. En concentrant les activités de chaque membre sur des secteurs et contenus qu'il maîtrise, et qui se situent au cœur de ses orientations stratégiques actuelles et futures, on assure ainsi leur engagement maximal.

La santé et, conséquemment, la pérennité de l'alliance dépendent aussi fortement de la performance financière du projet. En ce sens, chaque membre a veillé, lors de l'établissement du prix des composantes sous sa responsabilité, à développer des scénarios basés sur des évaluations réalistes des travaux à compléter qui incluent suffisamment de contingences financières pour être en mesure d'assumer ses obligations, le tout à l'intérieur de balises de risques acceptables. Comme chaque membre dispose d'un vaste bassin de ressources dans le monde, dotées de capacités et de tarifs variés, il en résulte une proposition conjointe dont le prix est réaliste et les marges suffisantes pour justifier un intérêt d'affaires soutenu, malgré les risques inhérents à ce type de projet. Chaque membre s'engage dans l'alliance avec un dossier d'affaires intéressant et prometteur, sur lequel il peut s'engager avec confiance, compte tenu de sa maîtrise de la portée. Les conditions ont été mises en place pour créer un modèle gagnant, tant pour la Société que pour l'alliance.

L'entente prévoit que chaque partenaire ait l'entière responsabilité de sa portion de la solution. Du début à la fin du projet, les mécanismes de gouvernance acceptés et mis en place par les membres assurent un suivi du déroulement selon le calendrier et les balises financières prévues, ainsi que la qualité des livrables selon les critères de la Société décrits dans l'appel d'offres. Au niveau des équipes à l'œuvre, la méthodologie suivie, les mécanismes d'assurance qualité et les audits externes viennent renforcer le respect de chaque membre face à ses obligations. L'implication régulière des exécutifs de chaque membre assure l'engagement total et la mise en œuvre des correctifs requis, au besoin. Les différends qui pourraient survenir en cours de route seront aussi traités rapidement en impliquant lorsque requis, les exécutifs responsables de chaque membre selon un processus préétabli par l'alliance.

L'alliance prévoit des engagements formels pris par chaque membre. Par exemple, on retrouve des prix fermes assumés par chaque membre pour leur portion de travail respective, lesquels incluent la prise en charge des risques et coûts associés à la livraison de la solution. De plus, chacun assume sa part de responsabilité contractuelle relative aux éléments sous son contrôle, selon les termes qui seront convenus avec la Société. Enfin, l'alliance a aussi prévu l'ensemble des autres modalités qu'on retrouve généralement dans de tels cas, notamment au niveau de la propriété intellectuelle et du maintien de la capacité de contracter.

B. Maintien de la relation d'affaires et de la santé financière de l'alliance et de ses composantes

L'engagement de l'alliance est ferme pour la durée du contrat. Aucune clause de sortie (« opting out ») n'est prévue, à l'exception bien entendu de cas de force majeure empêchant un membre à poursuivre ses activités dans l'alliance. De fait, la pérennité de l'alliance repose principalement sur deux éléments majeurs : la santé financière de la portée du projet couverte par chaque membre pour toute la durée du projet et la capacité de gérer rapidement et équitablement les incidents ou conflits qui pourraient survenir au cours de la période de dix années prévue.

L'alliance a configuré les grands paramètres du projet pour assurer que les paiements reçus soient dans la mesure du possible alignés sur les coûts encourus, limitant ainsi les montants à financer et limitant ainsi les risques associés selon l'esprit du partage de risque suggéré par la Société. De plus, les marges bénéficiaires de chacun se situent à l'intérieur des limites que peuvent soutenir leurs opérations commerciales habituelles respectives. Ainsi, chaque membre de l'alliance s'engage dans un projet dont les paramètres financiers sont gérables et intéressants.

Même si on tente de tout prévoir, il est inévitable pour un projet de cette envergure d'une durée de dix années d'avoir à faire face en cours de route à des éléments imprévus, tels des ajustements à la portée des travaux résultant des nouveaux besoins de la Société. L'impact des changements rencontrés en cours de route peut être de nature mineure à sérieuse. C'est pourquoi nous avons prévu des mécanismes de gestion d'incidents ou de conflits, tels que décrit à la section précédente, qui seront d'enclenchés jusqu'aux plus hauts niveaux hiérarchiques de chaque membre de l'alliance pour assurer que la résolution s'exécute rapidement et mobilise l'ensemble des personnes concernées.

C. Qualité de la santé financière de chacun des partenaires impliqués

LGS, une filiale à part entière d'IBM, est une entreprise de services-conseils en affaires, technologies, développement et gestion de projets. Elle s'appuie sur des professionnels passionnés par leur domaine : la consultation en technologies de l'information (TI).

Fondée en 1979 par des entrepreneurs visionnaires, LGS regroupe aujourd'hui des centaines de professionnels à Québec, Montréal et Rimouski. Très présente dans le paysage québécois, elle fait également partie de la famille IBM. Elle donne ainsi un accès privilégié à une vaste expertise de haut niveau et à l'intelligence de spécialistes accessibles et aguerris aux réalités de la Société.

Modèle mondial de prestation – Approche de LGS/IBM à trois niveaux

LGS/IBM possède un vaste réseau mondial de prestation de services regroupant des dizaines de milliers de professionnels qui assurent les services de consultation, de processus d'affaires, de soutien à l'infrastructure et de gestion d'applications pour ses clients du monde entier. LGS/IBM utilise des outils et des processus standards basés dans ses centres pour créer une répartition plus efficace de la charge de travail, offrir des résultats plus uniformes et augmenter la productivité et la valeur pour ses clients.

Pour développer son modèle, LGS/IBM a commencé à établir des Centres d'innovation client (CIC) au Canada, aux États-Unis et en Europe afin d'offrir des services plus compétitifs dans le pays même ou à proximité pour assurer la prestation sur place et à l'étranger.

Les CIC de LGS/IBM appliquent une approche intégrée mondiale industrialisée pour offrir des services à haute valeur de développement d'applications, de maintenance des applications et d'intégration de systèmes pouvant répondre à la demande croissante en matière d'infonuagique, d'analytique, de mobilité, de sécurité et de médias sociaux (CAMSS).

Pour sa solution destinée à la Société, LGS/IBM préconise un modèle d'emplacement des ressources qui inclut des ressources sur site et hors site. C'est le modèle à trois niveaux que nous recommandons en fonction de notre expérience de soutien et de déploiement des applications SAP pour nos clients.

Avec une équipe de base d'experts sur place/à proximité, appuyée par une équipe à l'étranger de taille optimale et une « boîte à outils » éprouvée, nous offrons un programme de qualité pour le soutien et la maintenance des applications qui suit le modèle d'autres programmes de soutien réussis de LGS/IBM.

Dans le cadre du modèle LGS/IBM de capacité mondiale intégrée, notre Centre d'innovation client de Halifax soutient nos modèles de prestation à deux et à trois niveaux, en offrant une approche commune :

- Concept de type « usine »;
- Gouvernance mondiale et processus normalisés;
- Services et flux de travaux par composantes, indépendamment de l'emplacement;
- Utilisation des actifs et du capital intellectuel;
- Méthodes et outils automatisés qui augmentent la productivité de la prestation des services;
- Exploitation des capacités de SAP.

La figure 2.21-7 illustre le concept CIC à trois niveaux de LGS/IBM.

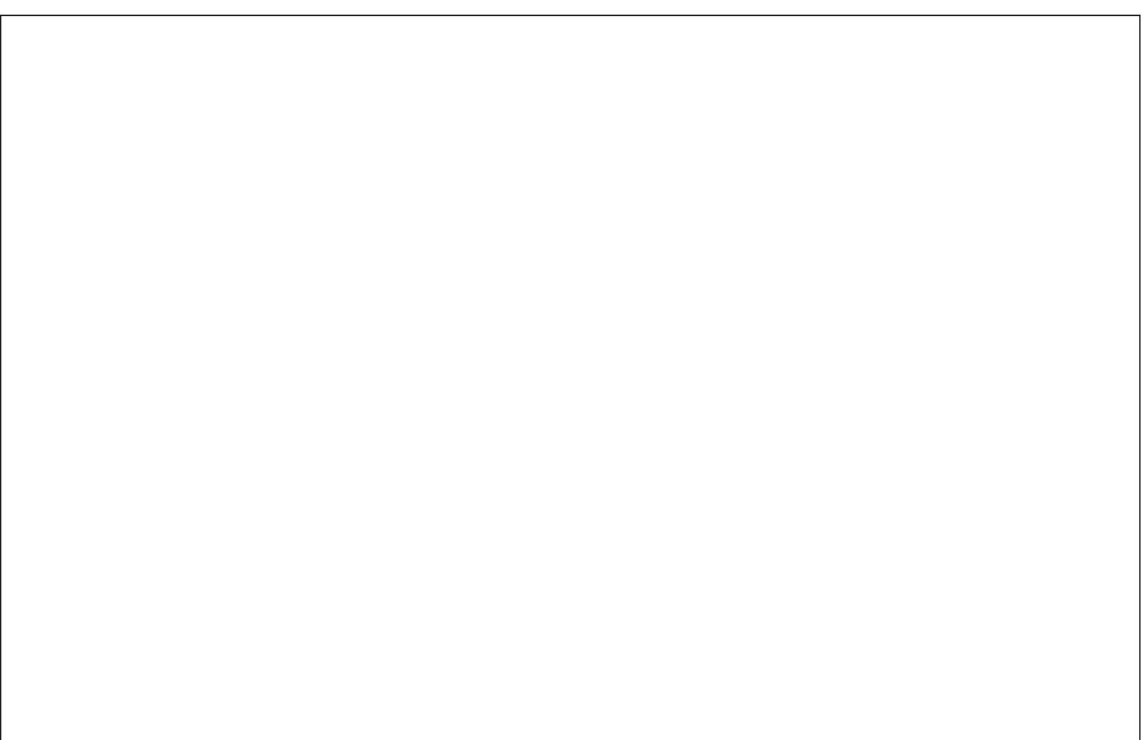


Figure 2.21.7 – Répartition géographique des services de LGS/IBM

Grâces aux politiques de déplacement mises en place par LGS/IBM, les ressources de proximité de Montréal ou du CIC d'Halifax ont la possibilité de se rendre sur les sites de ses clients à des fins de transfert essentiel des connaissances ou pour augmenter les équipes lors des phases de conception. Cela permet de fournir l'expertise appropriée au bon moment du mandat et au coût le plus faible possible.

Il faut préciser que LGS/IBM privilégie un modèle de prestation de services avec capacité fixe de base/complémentaire plutôt que celui à capacité fixe pris en considération dans cette soumission. Ce modèle de capacité fixe de base/complémentaire est détaillé à la section 2.21.2. « Information additionnelle de l'alliance » en plus d'informations complémentaires sur l'approche de transition et sur les outils et technologies utilisés dans le cadre de ce modèle.