# ÉNONCÉ DES TRAVAUX

## 1. TITRE

Système de gestion de l'information sur les intervenants d'Immigration, Réfugiés et Citoyenneté Canada (IRCC)

## 2. OBJECTIF

IRCC doit se procurer un service Web qui comprend une solution commerciale en vue de mettre en place un système de gestion de l'information sur les intervenants qui permettra aux utilisateurs d'IRCC de continuer à gérer efficacement divers renseignements électroniques concernant les intervenants ainsi que les interactions entre ceux-ci et IRCC.

## 3. CONTEXTE

IRCC emploie plus de 5 000 personnes au Canada et à l'étranger. Le Ministère élabore et gère des politiques et des programmes se rapportant à l'immigration, aux réfugiés, à la citoyenneté, à l'intégration et au Programme de passeport du Canada.

IRCC communique régulièrement avec des intervenants, d'autres ministères, des administrations provinciales et territoriales et le public canadien afin de les informer sur les politiques et les programmes existants et prévus, et de recueillir leurs commentaires à cet égard. Par ailleurs, une quarantaine de missions à l'étranger réalisent des activités de promotion et de recrutement au nom d'IRCC. À l'heure actuelle, cette information est sauvegardée dans une base de données Web de gestion des relations.

IRCC souhaite mettre en place un outil organisationnel centralisé pour éliminer la duplication, uniformiser la présentation et accroître l'exactitude des coordonnées des intervenants, poursuivre le travail de mobilisation du Ministère, et faciliter l'échange d'information et la communication avec les intervenants et les abonnés au bulletin. On s'attend également à ce que cet outil aide IRCC à réduire le temps et les ressources requises pour obtenir les données des intervenants et gérer les listes d'abonnés et d'intervenants.

## 4. PORTÉE DES TRAVAUX

La solution logicielle proposée pour le Système de gestion de l'information sur les intervenants est appelée ci-après « la solution ».

La solution livrée doit être un service Web géré auquel les employés d'IRCC peuvent accéder au moyen d'une connexion Internet sécurisée.

La solution doit répondre aux exigences obligatoires indiquées dans l'évaluation technique (pièce jointe 4.1) ou les dépasser.

## 5. EXIGENCES

### 5.1. SERVICES GÉRÉS

**Les services gérés doivent comprendre :**

5.1.1. Les plateformes matérielles et le stockage nécessaires pour prendre en charge la solution.

5.1.2. Tout logiciel ou service de réseautique, de sécurité et de plateforme (p. ex. systèmes d'exploitation, bases de données, répertoires, pare-feu) nécessaires pour prendre en charge la solution.

5.1.3. Les applications nécessaires pour prendre en charge la solution.

**Les services gérés doivent également comprendre :**

5.1.4. Les services nécessaires à la mise en œuvre et à la configuration de la solution, y compris l'importation des données dans la solution

5.1.5. Les services nécessaires pour la maintenance de la solution, y compris les nouvelles versions, les mises à jour et les corrections de bogues du logiciel au fur et à mesure qu'elles sont disponibles.

5.1.6. Le soutien technique de la solution, tel que décrit dans la section 9.3.

## 5.2. DISPONIBILITÉ DES LOGICIELS

5.2.1. La plus récente version commerciale de la solution doit être disponible à la date de clôture des soumissions.

5.2.2. La solution doit comprendre les nouvelles versions, les mises à jour et les corrections de bogues du logiciel au fur et à mesure qu'elles sont disponibles.

## 5.3. ENVIRONNEMENT TECHNIQUE

5.3.1. La solution et toutes les données sauvegardées doivent être hébergées sur un serveur protégé dédié situé au Canada, conformément aux exigences indiquées à l'annexe A.

5.3.2. La solution doit prévoir un contrôle de sécurité en temps réel et l'envoi d'avis par courriel à IRCC en cas d'incidents de sécurité, conformément aux exigences énoncées à l'annexe A.

5.3.3. La solution doit permettre la vérification et le suivi des actions des utilisateurs et des mesures administratives sélectionnées. La fonction de vérification doit fournir des détails sur qui a effectué des changements sur des champs précis d'un dossier, ainsi que la date et l'auteur de la dernière mise à jour d'un dossier.

5.3.4. La solution doit permettre l'interopérabilité des données avec Microsoft Outlook (2013), Service pack 1, et doit être compatible avec les versions ultérieures de Microsoft Outlook.

5.3.5. La solution doit permettre l'interopérabilité des données avec Microsoft Outlook 2007 (12.0.6680.5000), Service pack 3, et doit être compatible avec les versions ultérieures de Microsoft Outlook.

5.3.6. La solution doit être compatible avec la version de Windows Internet Explorer en usage à IRCC - version 11, protocole TLS version 1.2, chiffrement AES 256 bits -, ainsi qu'avec les versions ultérieures d'Internet Explorer et d'autres navigateurs Internet (p. ex. Firefox, Chrome).

5.3.7. La solution doit permettre – ou être configurée de façon à permettre – l'utilisation de fichiers dans les formats suivants : jpg, jpg2000, tiff, bmp, xls, xlsx, xlsm, ppt, rtf, mso, txt, pdf, pptx, doc, docx et docm.

5.3.8. La solution doit pouvoir être offerte à au moins 500 utilisateurs et la capacité doit pouvoir être augmentée.

## 5.4. ADMINISTRATION DU SYSTÈME

5.4.1. La solution doit permettre aux administrateurs de compte d'IRCC d'attribuer un droit d'accès à un employé ou à un groupe d'employés.

5.4.2. La solution doit bloquer l'exécution d'opérations sur des objets de la base de données à moins que l'utilisateur n'ait l'autorisation nécessaire.

5.4.3. La solution doit permettre de contrôler divers types de droits d'accès des utilisateurs, notamment :

**5.4.3.1.** lecture seule;
**5.4.3.2.** droit de consulter;
**5.4.3.3.** droit de supprimer;
**5.4.3.4.** droit de modifier;
**5.4.3.5.** droit de créer/d'ajouter des dossiers;
**5.4.3.6.** droit de produire des rapports;
**5.4.3.7.** droit d'exécuter les tâches d'administrateur de système.

5.4.4. La solution doit permettre aux administrateurs de compte d'IRCC de créer, de gérer et de tenir à jour l'information contenue dans les comptes d'utilisateur de tous les employés d'IRCC.

5.4.5. La solution doit permettre – ou être configurée de façon à permettre – aux administrateurs de compte d'IRCC de gérer (ce qui comprend créer, supprimer, archiver et renommer) les descripteurs ou mots-clés structurés que les utilisateurs peuvent associer aux dossiers pour en faciliter l'identification.

5.4.6. La solution doit fournir – ou pouvoir être configurée de façon à fournir – une liste des opérations et autorisations qu'un utilisateur individuel, un groupe d'utilisateurs ou une catégorie d'utilisateurs peut exécuter au niveau de l'application ou de la base de données.

5.4.7. La solution doit comprendre une fonction de vérification qui enregistre l'information concernant les modifications, ajouts, suppressions et sélections par les utilisateurs individuels pour tout objet individuel sélectionné.

5.4.8. La solution doit pouvoir être utilisée simultanément par au moins 50 utilisateurs.

5.4.9. La solution doit permettre aux administrateurs de séparer ou masquer certaines données (p. ex. des listes d'abonnés) pour que seuls certains groupes choisis puissent les voir et les modifier.

## 5.5. FONCTIONNALITÉ OPÉRATIONNELLE

5.5.1. La solution doit contenir – ou être configurée de façon à contenir – les champs habituels, notamment :

**5.5.1.1.** nom de famille et prénom du contact;
**5.5.1.2.** organisation;
**5.5.1.3.** titre du poste;
**5.5.1.4.** adresse;
**5.5.1.5.** adresse(s) courriel;
**5.5.1.6.** numéro(s) de téléphone (travail, cellulaire, télécopieur);
**5.5.1.7.** code postal;
**5.5.1.8.** pays;
**5.5.1.9.** langue de correspondance préférée.

5.5.2. La solution doit permettre d'établir des champs obligatoires.

5.5.3. La solution doit permettre aux utilisateurs de modifier, de créer et d'associer au moins 50 mots-clés ou descripteurs à chaque dossier.

5.5.4. La solution doit permettre aux utilisateurs d'associer des étiquettes ou des mots-clés aux inscriptions afin de regrouper ou de lier des inscriptions et faciliter la recherche.

5.5.5. La solution doit inclure une fonction qui permet aux utilisateurs de joindre des notes à un dossier.

5.5.6. La solution ne doit pas limiter le nombre de notes que les utilisateurs peuvent joindre à un dossier.

5.5.7. La solution doit inclure une fonction d'agenda/de planification d'événements qui permet de classer l'information par date et par groupe.

5.5.8. La solution ne doit pas limiter – ou doit pouvoir être configurée de façon à ne pas limiter – le nombre d'éléments d'agenda que les utilisateurs peuvent joindre à un dossier.

5.5.9. La solution doit avoir une fonction de gestion d'agenda et d'événements qui permet aux utilisateurs internes d'envoyer des invitations par courriel à des intervenants externes. Les intervenants doivent être en mesure d'accepter, de refuser ou de désigner un délégué à partir de l'invitation par courriel (au moyen de boutons ou d'une intégration avec Outlook).

5.5.10. La solution doit être munie d'une fonction de gestion d'agenda et d'événements qui permet aux utilisateurs internes d'ajouter des inscriptions d'événements (de courtes entrées marquant les événements à venir) et de gérer les confirmations des présences à partir de la solution ou d'une intégration à Outlook.

5.5.11. La solution ne doit pas limiter – ou doit pouvoir être configurée de façon à ne pas limiter – le nombre d'éléments d'agenda que les utilisateurs peuvent joindre à un dossier.

5.5.12. La solution doit afficher – ou pouvoir être configurée de façon à afficher – le nom de l'utilisateur et la date de saisie des données dans les dossiers, notes ou fonctions d'agenda.

5.5.13. La solution doit permettre aux utilisateurs d'associer un nombre illimité de documents électroniques, y compris des courriels, aux dossiers et éléments d'agenda. Elle doit permettre l'utilisation de fichiers dans les formats suivants : jpg, jpg2000, tiff, bmp, xls, xlsx, xlsm, ppt, rtf, mso, txt, pdf, pptx, doc, docx et docm.

5.5.14. La solution doit permettre l'ouverture d'une pièce jointe dans son application native. Elle doit permettre l'utilisation de fichiers dans les formats suivants : jpg, jpg2000, tiff, bmp, xls, xlsx, xlsm, ppt, rtf, mso, txt, pdf, pptx, doc, docx et docm.

5.5.15. La solution doit comprendre une fonction « serveur de liste » (formulaires d'abonnement personnalisables, capacité de s'abonner/se désabonner aux courriels, automatisation de la distribution de courriels à une liste d'abonnés).

5.5.16. La solution doit être munie d'un formulaire de liste de diffusion qui peut se connecter au site Web d'IRCC par un programme HTML ou par d'autres moyens.

5.5.17. La solution doit permettre – ou pouvoir être configurée de façon à permettre – aux utilisateurs de créer des listes de distribution à partir des critères définis, ce qui comprend, entre autres :

**5.5.17.1.** intervenants par nom;
**5.5.17.2.** intervenants par organisation;
**5.5.17.3.** intervenants par activité;
**5.5.17.4.** intervenants par mot-clé ou descripteur;
**5.5.17.5.** intervenants par région (pays, province, ville);
**5.5.17.6.** intervenants par industrie ou secteur.
**5.5.17.7.** La solution doit permettre aux utilisateurs d'envoyer des courriels individuels et en lot.

5.5.18. La solution doit permettre aux utilisateurs d'envoyer des tâches de courriels individuellement et en lots. Les tâches en lots peuvent contenir jusqu'à 500 000 adresses courriel, voire davantage.

5.5.19. La solution doit permettre d'envoyer des courriels en lot à un taux minimal de 50 000 courriels par heure.

5.5.20. La solution ne doit pas limiter le nombre de tâches de courriels individuels ou en lot que les utilisateurs peuvent envoyer.

5.5.21. La solution doit permettre à l'administrateur de fusionner les dossiers en double (p. ex. intervenants ou descripteurs).

5.5.22. La solution doit pouvoir gérer au moins 5 millions d'inscriptions et être évolutive (augmentation du volume).

## 5.6. RECHERCHE

5.6.1. La solution doit permettre aux utilisateurs d'effectuer des recherches en utilisant différents termes ou moyens, notamment :

**5.6.1.1.** date ou période;
**5.6.1.2.** mot-clé ou descripteur;

**5.6.1.3.** nom de l'organisation;
**5.6.1.4.** nom de la personne-ressource;
**5.6.1.5.** courriel;
**5.6.1.6.** adresse postale;
**5.6.1.7.** site Web;
**5.6.1.8.** numéro de téléphone;
**5.6.1.9.** pays, province ou ville.

5.6.2. La fonction de recherche doit permettre aux utilisateurs d'utiliser des termes ou des mots-clés complets ou partiels.

5.6.3. La solution doit permettre d'effectuer – ou pouvoir être configurée de façon à permettre d'effectuer – des recherches sur les entrées trouvées dans les dossiers ou les notes.

5.6.4. La solution doit conserver – ou être configurée de façon à conserver – l'historique de certains champs (p. ex. le nom et les données d'anciennes personnes-ressources).

## 5.7. INTERFACE UTILISATEUR

5.7.1. La solution doit contenir une interface utilisateur exploitable sur le Web.

5.7.2. La solution doit supporter, au minimum, les jeux de caractères complets en anglais canadien et en français canadien (Unicode UTF-8 v4.1).

5.7.3. La solution doit permettre – ou être configurée de façon à permettre – aux utilisateurs de travailler dans la langue officielle de leur choix : anglais canadien ou français canadien.

5.7.4. La solution doit permettre aux utilisateurs de consulter tous les écrans, les messages-guide et l'aide en ligne en anglais canadien ou en français canadien.

5.7.5. La solution doit permettre l'inscription de la classification de sécurité [protégé A] sur tous les écrans et rapports de la base de données.

## 5.8. RAPPORTS

5.8.1. La solution doit produire – ou pouvoir être configurée de façon à produire – un ensemble de rapports courants que l'utilisateur peut exécuter dans le système, ce qui comprend :

**5.8.1.1.** dossiers des intervenants par mot-clé ou descripteur;
**5.8.1.2.** dossiers des intervenants par région (ville, province, pays);
**5.8.1.3.** notes/interactions des intervenants par mot-clé ou descripteur;
**5.8.1.4.** événements des intervenants par date ou période;
**5.8.1.5.** événements des intervenants par mot-clé ou descripteur;
**5.8.1.6.** nombre de campagnes par courriel par période;
**5.8.1.7.** nombre de comptes d'utilisateur actifs.

5.8.2. La solution doit fournir – ou être configurée de façon à fournir – des rapports d'analyse des courriels envoyés, ce qui comprend

**5.8.2.1.** taux de lecture ou d'ouverture;

**5.8.2.2.** taux de clics (nombre de fois où on a cliqué sur une adresse URL intégrée à un courriel);
**5.8.2.3.** refus ou désabonnements;
**5.8.2.4.** courriels non livrables ou renvoyés à l'expéditeur.

5.8.3. La solution doit permettre de sauvegarder et d'imprimer des rapports normalisés et ponctuels.

5.8.4. La solution doit permettre – ou pouvoir être configurée de façon à permettre – aux utilisateurs d'exporter des rapports en format xlsx ou csv et pdf.

**Documentation, formation, services professionnels**

## 6. DOCUMENTS

**6.1.** L'entrepreneur doit fournir la documentation suivante sous la forme de manuels de l'utilisateur :

6.1.1. le manuel d'installation;
6.1.2. manuel de l'administrateur;
6.1.3. manuel de l'utilisateur;
6.1.4. manuel de formation;
6.1.5. La documentation doit correspondre à la version du logiciel proposée.

**6.2.** L'entrepreneur doit donner à IRCC le droit de copier ou d'imprimer la documentation relative à la solution. La documentation doit être offerte en format électronique (Microsoft Word).

**6.3.** L'entrepreneur doit fournir toute la documentation en anglais canadien et en français canadien.

## 7. FORMATION

**7.1.** L'entrepreneur doit fournir vingt (20) heures de formation aux administrateurs du système, aux utilisateurs finaux et aux responsables du soutien technique. Cette formation devrait inclure des tutoriels sur le système et ses caractéristiques, ainsi que des périodes de questions et réponses. Cette formation peut être donnée sur place au 70, rue Crémazie, à Gatineau (Québec), ou à distance dans le cadre de réunions en ligne.

**7.2.** L'entrepreneur doit fournir tous les documents de formation applicables en anglais canadien et en français canadien. La documentation doit être offerte en format électronique (Microsoft Word).

## 8. SERVICES PROFESSIONNELS ET ÉLÉMENTS LIVRABLES

**8.1.** L'entrepreneur doit fournir les services nécessaires à la réalisation des tâches suivantes dans les délais prévus. Le responsable de projet d'IRCC doit confirmer l'achèvement satisfaisant de chaque étape au moyen de sa signature électronique. Si un délai additionnel est nécessaire pour corriger ces problèmes, les phases/jalons subséquents seront ajustés en conséquence.

| Activité / élément livrable | Calendrier connexe | | Formule |
|---|---|---|---|
| | **Entrepreneur** | **Approbation par IRCC** | |
| **8.2.** Rencontre de lancement | Dans les cinq (5) jours ouvrables suivant l'attribution du marché. | s.o. | En personne au 365, avenue Laurier Ouest, à Ottawa (Ontario), ou par téléconférence/ cyberconférence |
| **8.3.** Document relatif à la gestion du projet<br>8.3.1. Plan de gestion du projet<br>8.3.2. Calendrier du projet<br>8.3.3. Plan de migration des données<br>8.3.4. Spécifications et guides de configuration<br>8.3.5. Plan de mise à l'essai<br>8.3.6. Plan et stratégie de mise en œuvre | Dans les quinze (15) jours ouvrables suivant l'attribution du marché et lorsque des changements importants sont apportés (demandes de changement). | Dans les cinq (5) jours ouvrables suivant la réception de tous les éléments livrables. | Microsoft Word |
| **8.4.** Conception de la solution | Dans les vingt (20) jours ouvrables suivant l'attribution du marché. | Dans les trois (3) jours ouvrables suivant l'achèvement de la conception. | |
| **8.5.** Installation de la solution dans l'environnement de développement d'IRCC | Dans les cinq (5) jours ouvrables suivant l'approbation de la conception par IRCC. | Dans les trois (3) jours ouvrables suivant l'achèvement de l'installation. | |
| **8.6.** Configuration de la solution et des rapports dans un environnement de développement d'IRCC | Dans les vingt (20) jours ouvrables suivant l'approbation de l'installation par IRCC. | Dans les cinq (5) jours ouvrables suivant la configuration et la mise en œuvre des rapports. | |

| | | | |
|---|---|---|---|
| **8.7.** Accès aux services Web gérés pour au moins 5 utilisateurs aux fins d'essai d'acceptation des utilisateurs et aux versions préliminaires des manuels de l'utilisateur suivants (en anglais canadien) :<br>8.7.1. le manuel d'installation;<br>8.7.2. manuel de l'administrateur;<br>8.7.3. manuel de l'utilisateur;<br>8.7.4. manuel de formation; | Dans les cinq (5) jours ouvrables suivant la configuration de la solution et des rapports dans un environnement de développement d'IRCC | L'essai d'acceptation des utilisateurs doit être achevé dans les dix (10) jours suivant la réception de l'accès et des versions préliminaires des manuels. | Microsoft Word |
| **8.8.** Configuration finale et vérification de la solution dans l'environnement d'IRCC. | Dans les cinq (5) jours ouvrables suivant l'approbation de l'essai d'acceptation des utilisateurs. | Dans les trois (3) jours ouvrables suivant la configuration et la vérification finales. | |
| **8.9.** Migration des données en format .xls vers la solution dans l'environnement de développement d'IRCC | Dans les cinq (5) jours ouvrables suivant la configuration et la vérification finales. | Dans les trois (3) jours suivant l'achèvement de la migration des données. | |
| **8.10.** Accès à un service Web géré pour au moins 500 utilisateurs et aux versions finales des manuels de l'utilisateur en anglais canadien et en français canadien.<br>8.10.1. le manuel d'installation;<br>8.10.2. manuel de l'administrateur;<br>8.10.3. manuel de l'utilisateur;<br>8.10.4. manuel de formation; | Dans les cinq (5) jours ouvrables suivant l'achèvement de la migration des données. | Dans les trois (3) jours suivant la réception de l'accès et des versions finales des manuels. | Microsoft Word |
| **8.11.** Rapports d'étape | Toutes les semaines jusqu'à ce que la solution soit pleinement mise en œuvre à IRCC. | | Microsoft Word |

| | | | |
|---|---|---|---|
| **8.12.** Rapport final | Dans un délai de 120 jours ouvrables après l'attribution du marché. | | Microsoft Word |

**8.13.** L'entrepreneur doit fournir les services techniques requis pour assurer un soutien à la clientèle pendant toute la période visée, y compris :

8.13.1. un soutien à la clientèle sur le Web;
8.13.2. un dispositif de suivi en ligne des demandes de soutien des clients, qui précise le problème, la date de création et la réponse
8.13.3. la capacité de voir l'état des demandes de soutien des clients.

## 9. RÉUNIONS

L'entrepreneur devra participer, au besoin, à des réunions avec l'équipe de projet; ces réunions pourront avoir lieu en personne au 365, avenue Laurier Ouest, à Ottawa (Ontario), ou par téléconférence/cyberconférence.

## 10.VOYAGES

Le Canada ne remboursera pas les frais de déplacement ou de subsistance liés à l'exécution des travaux. Les frais de déplacement, le cas échéant, devront entièrement être assumés par l'entrepreneur.

## 11.CONTRAINTES

L'entrepreneur ne pourra pas commencer la mise en œuvre technique de la solution tant que l'évaluation des facteurs relatifs à la vie privée et l'évaluation et autorisation de sécurité n'auront pas été réalisées par le Canada.

## 12. SOUTIEN À LA CLIENTÈLE

IRCC fournira les services suivants au besoin afin d'assurer la réalisation des travaux visés par le présent contrat :

**12.1.** communication de la documentation et des documents de référence pertinents par courriel en format Word, Excel ou PDF;

**12.2.** examen des rapports/soumissions, selon les besoins, et formulation de commentaires/suggestions de mises à jour en temps utile;

**12.3.** coordination des activités et des réponses des secteurs d'IRCC qui se rapportent aux questions ciblées par l'entrepreneur, de façon à permettre à ce dernier de fournir les services demandés;

**12.4.** communication de toutes les données nécessaires pour appuyer la transition vers le Système de gestion de l'information sur les intervenants;

**12.5.** communication de directives à l'entrepreneur, dans la mesure du possible et sur demande, au sujet de ses obligations concernant les lois, les politiques et les règlements du Canada qui portent sur la protection des renseignements personnels;

**12.6.** tout autre soutien et aide jugés pertinents.

**Appendice A** – Exigences en matière de protection des renseignements personnels et de sécurité

Le présent appendice décrit les exigences en matière de sécurité et de protection des renseignements personnels que l'entrepreneur doit respecter pour assurer l'application et le maintien des mesures de sécurité et de protection des renseignements personnels prévues dans le présent document lors de la fourniture du Système de gestion de l'information sur les intervenants.

## 1) Sécurité des opérations

a) Il faut stocker les données, y accéder et les transmettre conformément au profil de contrôle de sécurité « Protégé A » du gouvernement du Canada ainsi qu'il est décrit dans l'ITSG-33 (publication du Centre de la sécurité des télécommunications Canada, https://www.cse-cst.gc.ca/fr/node/265/html/22839).

b) L'entrepreneur doit s'assurer que toutes les activités réalisées relativement à la section des exigences relatives à la protection des renseignements personnels et à la sécurité fournissent des niveaux de protection comparables aux niveaux de protection définis dans les politiques du gouvernement du Canada et qu'elles respectent ou surpassent les pratiques exemplaires ou les normes de l'industrie, les exigences les plus rigoureuses étant retenues.

c) L'entrepreneur doit empêcher les membres de son personnel d'accéder à des comptes de courriel personnels ou à des applications de messagerie instantanée à partir du matériel informatique servant à la réalisation des travaux.

## 2) Sécurité matérielle

a) L'entrepreneur doit mettre en place des mesures de sécurité matérielle afin de protéger les documents et les renseignements du Canada contre les risques de perte, de dommage ou de vol. L'entrepreneur doit au moins prendre les mesures de sécurité suivantes

i) contrôler l'accès du personnel aux installations;
ii) la prévention des incendies et le matériel d'extinction;
iii) installer un dispositif de détection d'intrusion contre les entrées par effraction;
iv) la surveillance des installations;
v) avoir la capacité de faire sortir des installations les personnes qui ont un comportement anormal, perturbateur ou menaçant;
vi) limiter l'accès du public à un seul secteur – la zone d'accueil;
vii) aménager un espace pour héberger les principaux systèmes de TI, c'est-à-dire les serveurs de fichiers et de bases de données contenant les renseignements liés aux travaux, qui répondent aux normes spécifiées dans la ligne directrice de la GRC intitulée G1-031 Protection matérielle des serveurs informatiques;
viii) utiliser des contenants de sécurité approuvés qui fournissent un niveau de protection comparable à celui des normes canadiennes (voir le Guide

d'équipement de sécurité de la GRC fourni par le chargé de projet sur demande) pour la conservation des données liées aux travaux, y compris les ordinateurs portatifs ou les tablettes.

b) Le maintien de l'accès autorisé aux biens de grande valeur et aux biens protégés et classifiés est primordial pendant leur transport.

c) Pendant le transport de biens protégés et classifiés d'une personne à une autre ou d'un lieu à un autre, les mesures de protection à adopter doivent permettre de contrôler l'accès aux renseignements selon le principe du besoin de connaître. Cela s'applique également à l'entretien des contenants.

d) Pendant la transmission de biens protégés et classifiés d'une personne à une autre ou d'un lieu à un autre, il faut mettre l'accent, pour les mesures de protection à adopter, sur l'utilisation d'un l'emballage approprié, sur des services postaux et de messagerie fiables et sur l'anonymat de ces renseignements pendant le transport.

3) Sécurité de la technologie de l'information

a) L'entrepreneur doit appliquer des mesures de protection pour protéger toute base de données ou tout système informatique où sont conservées les données liées aux travaux visés par le présent contrat contre l'accès non autorisé. Ces mesures de protection doivent comprendre :

i) les contrôles d'authentification et d'autorisation;
ii) la défense périphérique – pare-feu;
iii) détection des intrusions;
iv) l'isolation du réseau;
v) la désactivation de tous les ports d'accès par support d'information amovible sur les postes informatiques : ports USB, réseau Wi-Fi, lecteurs de disques, lecteur de DVD/CD, système Bluetooth.

**4) Journal des incidents et vérifications**

a) L'entrepreneur doit tenir un journal de vérification où sont consignées de façon électronique toutes les tentatives d'accès à des dossiers d'information sur les intervenants enregistrés sur support électronique. Le journal de vérification doit être dans un format pouvant être examiné en tout temps par l'entrepreneur et le chargé de projet. Les journaux des vérifications doivent au moins contenir les éléments de données suivants :

i) l'entité d'origine (par ex., ID utilisateur);
ii) date et heure de l'événement;
iii) type d'événement;
iv) l'objet : identificateur unique des fichiers/ensembles de données qui ont été manipulés;
v) l'état des résultats (le cas échéant);
vi) la machine : identificateur unique de la machine;
vii) l'emplacement : identificateur unique de l'emplacement.

b) L'entrepreneur doit conserver les journaux des incidents de sécurité pendant au moins six (6) mois et les mettre à la disposition du chargé de projet sur demande.

**5) Authentification et autorisation**

a) L'entrepreneur doit conserver les renseignements personnels sous format électronique de manière à ce qu'un mot de passe (ou un autre mécanisme de contrôle de l'accès) soit exigé pour accéder au système ou à la base de données où sont conservés les renseignements personnels.

b) L'entrepreneur doit voir à ce que les mots de passe ou les autres contrôles d'accès ne soient fournis qu'aux membres du personnel qui ont besoin d'accéder à l'information sur les intervenants pour exécuter les travaux.

c) L'entrepreneur doit mettre en application des mots de passe solides qui sont conformes aux caractéristiques suivantes :

   i) Verrouillage après un nombre configurable de tentatives d'accès infructueuses.
   ii) Comporter au moins huit (8) caractères et au minimum toutes les exigences suivantes :
      i. au moins une (1) lettre majuscule (A – Z);
      ii. au moins une (1) lettre minuscule (a – z);
      iii. au moins un (1) caractère non alphanumérique (%, +, @, !);
      iv. au moins deux (2) caractères numériques (de 0 à 9).

   iii) L'entrepreneur doit demander aux utilisateurs de changer leur mot de passe tous les 84 jours.

d) L'entrepreneur doit veiller à ce que le compte d'un membre du personnel soit fermé rapidement lors de la cessation de ses fonctions.

**7) Prévention contre les logiciels malveillants**

a) L'entrepreneur doit installer un logiciel de lutte contre les logiciels malveillants au moyen de mesures de protection dans tous les systèmes de TI utilisés dans la réalisation des travaux visés par le présent contrat.

b) L'entrepreneur doit s'assurer que le contrôle antivirus et la mise à jour de la liste des virus sont effectués quotidiennement.

**8) Sécurité des réseaux**

a) L'entrepreneur doit chiffrer toute l'information recueillie, sauvegardée, transférée et transmise dans le système et doit utiliser les algorithmes de chiffrement approuvés par le CSTC définis dans la publication ITSP.40.111 Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (https://www.cse-cst.gc.ca/fr/node/1831/html/26515).

**9) Autres applications de sécurité des TI**

a) L'entrepreneur doit installer sur-le-champ, dans tous les systèmes informatiques servant à l'exécution des travaux prévus au contrat, les correctifs de sécurité recommandés par les fabricants du système d'exploitation et les fournisseurs des applications.
b) L'entrepreneur doit tenir des registres détaillés des changements apportés aux systèmes d'information servant au traitement et au stockage des renseignements

personnels. L'entrepreneur doit fournir, sur demande, les registres de modification et de gestion de la configuration au chargé de projet.

**10) Gestion de l'information**

a) L'entrepreneur doit élaborer un plan de sécurité et le présenter à l'examen et à l'approbation du chargé de projet. Ce plan de sécurité doit au moins décrire les éléments suivants :
   i. les rôles et les responsabilités de l'entrepreneur;
   ii. le processus d'enquête de sécurité de l'entrepreneur et les mesures de protection connexes relatives à la sécurité du personnel;
   iii. les mesures de protection de la sécurité matérielle;
   iv. le programme de sensibilisation à la sécurité de l'entrepreneur;
   v. le programme de gestion de la configuration de l'entrepreneur;
   vi. les mesures de protection de la sécurité des TI de l'entrepreneur (p. ex. pare-feu, systèmes d'authentification et d'autorisation, vérification et consignation);
   vii. la planification d'urgence de l'entrepreneur (continuité des activités, reprise après sinistre);
   viii. les processus d'intervention de l'entrepreneur en cas d'incident relatif à la protection des renseignements personnels et à la sécurité;
   ix. le programme de vérification et de responsabilisation de l'entrepreneur;
   x. les processus de vérification interne et d'atténuation des risques de l'entrepreneur;
   xi. le processus de renforcement de la sécurité de l'entrepreneur;
   xii. le processus d'installation des correctifs dans le système d'exploitation et les applications de l'entrepreneur;
   xiii. les normes et les pratiques de l'entrepreneur en ce qui concerne le renforcement de la sécurité;
   xiv. les mesures de protection de l'entrepreneur en ce qui concerne les contenants sécurisés et la gestion des clés et des combinaisons.

b) L'entrepreneur doit fournir au chargé de projet, sur demande, toute l'information raisonnable et pertinente pour permettre au Canada d'effectuer une évaluation des menaces et des risques, si le Canada décide de mener sa propre évaluation des menaces et des risques sur les activités menées au centre. Cette information peut comprendre, sans s'y limiter, ce qui suit :
   i. Politiques et procédures
   ii. Plan de sûreté
   iii. Plan d'intervention d'urgence
   iv. Registres de système liés au traitement et au stockage par le système de TI des renseignements des intervenants
   v. Rapports d'évaluation de la vulnérabilité
   vi. Rapports sur les essais de pénétration
   vii. Rapports sur la définition de l'autorisation et des utilisateurs.

c) L'entrepreneur doit surveiller périodiquement sa situation sur le plan de la sécurité et transmettre les résultats au chargé de projet. À cette fin, il doit au moins prendre les mesures suivantes :
   i. réévaluer les menaces locales à la sécurité au moins une fois par année, ou lorsque l'exige un changement important;
   ii. réaliser un examen de la sécurité si un important incident de sécurité s'est produit;

iii. soumettre les systèmes hôtes à une évaluation de la vulnérabilité au moins une fois par année;
iv. effectuer des essais de pénétration des mesures de protection du périmètre au moins une fois par année;
v. faire une vérification, à l'interne ou par un tiers externe autorisé, des processus et des procédures de sécurité au moins une fois par année;
vi. passer en revue les systèmes d'information et les journaux manuels au moins une fois par semaine.

d) L'entrepreneur doit veiller à maintenir les renseignements et les systèmes concernant ce service complètement séparés de la totalité de ses autres renseignements, données, documents ou dossiers et qu'ils ne sont ni partagés avec les autres secteurs d'activité de l'entrepreneur ni accessibles à ceux-ci.

## 11) Détection, intervention et rétablissement

a) L'entrepreneur doit aviser immédiatement le chargé de projet de toute atteinte à la sécurité et des incidents de sécurité touchant l'exécution des travaux prévus au contrat. Il peut s'agir notamment des incidents suivants :
i. consultation, utilisation et communication non autorisées de renseignements sur les intervenants;
ii. incidents pouvant compromettre la sécurité ou l'intégrité des renseignements des intervenants;
iii. actes de malfaisance (vol de renseignements sur les intervenants, allégations de corruption ou chantage);
iv. alertes à la bombe;
v. incendies;
vi. agressions physiques
vii. menaces (verbales, écrites, téléphoniques)
viii. Introduction par effraction
ix. manifestations et occupations illégales;
x. vandalisme;
xi. vol (biens/articles en stock);
xii. dommages et pertes (biens matériels);
xiii. logiciels malveillants (ex. : virus);
xiv. atteintes à la sécurité des systèmes de TI;
xv. altération des contenants de sécurité.

b) L'entrepreneur doit élaborer et consigner des procédures d'intervention en cas de manquement à la protection des renseignements personnels et d'incident de sécurité, y compris des procédures de renvoi aux paliers supérieurs selon la gravité du manquement ou de l'incident. Ces procédures doivent comprendre les mesures suivantes :

i. prendre des mesures immédiates en vue d'arrêter l'infraction et de protéger les documents, systèmes ou sites Web touchés;
ii. prendre toutes les mesures raisonnables pour résoudre le problème et empêcher qu'il se reproduise;
iii. consigner les infractions et les incidents liés à la sécurité ou à la protection des renseignements personnels;
iv. aviser immédiatement le chargé de projet des situations dans lesquelles des renseignements sur les intervenants risquent d'être compromis;
v. aviser les personnes dont les renseignements ont été divulgués;

vi. appliquer les mesures demandées par le chargé de projet;
vii. consigner les mesures correctives prises.

## 12) Production de rapports de sécurité

a) Dans les trente (30) jours civils suivant la fin de l'année civile, l'entrepreneur doit remettre au chargé de projet le rapport de sécurité annuel comprenant au moins les éléments suivants :
   i. la liste de tous les emplacements où les renseignements sur les intervenants sous forme électronique sont conservés (p. ex. l'emplacement du serveur sur lequel la base de données, y compris les renseignements sur les intervenants, est installée), ainsi que les copies de sauvegarde;
   ii. la liste de toutes les personnes auxquelles l'entrepreneur a donné l'accès aux renseignements sur les intervenants
   iii. la liste de toutes les mesures de protection prises par l'entrepreneur pour protéger les renseignements sur les intervenants;
   iv. la liste de toutes les menaces potentielles ou réelles pour les renseignements sur les intervenants et une explication détaillée de ces menaces, ainsi qu'une évaluation des risques créés par ces menaces et du caractère adéquat des mesures de sauvegarde existantes pour prévenir ces risques.
   v. la liste de toutes les nouvelles mesures de protection des renseignements sur les intervenants que l'entrepreneur prévoit mettre en œuvre au cours de la prochaine année, et une explication détaillée de ces mesures.

## 13) Élimination de documents

a) L'entrepreneur doit éliminer les documents et les données électroniques conformément aux directives énoncées dans la publication suivante du Centre de la sécurité des télécommunications : ITSP.40.006 v2 – Nettoyage des supports de TI (https://www.cse-cst.gc.ca/fr/node/2206/html/27963).