

# Immigration – Système de mesure pour la reddition des comptes concernant les programmes de contrôles



**Exigences en matière de sécurité pour les fournisseurs de services**

Novembre 2002

## TABLE DES MATIÈRES

### Sommaire

### Introduction

## **PARTIE I : Sécurité de l'utilisateur**

### **1. Évaluation de la fiabilité des utilisateurs**

- 1.1 Historique
- 1.2 Vérification de l'information
- 1.3 Exemptions
- 1.4 Conflit d'intérêt
- 1.5 Validité, mise à jour et révocation
- 1.6 Sous-contrats

### **2. Traitement de l'information des évaluations de fiabilité**

- 2.1 Obtention du consentement
- 2.2 Vérification de l'information personnelle, sur les études et sur l'emploi et (ou) des références
- 2.3 Vérification du casier judiciaire
- 2.4 Comment remplir un « *Formulaire d'autorisation et d'évaluation de la fiabilité de l'utilisateur iSMRP* »

### **3. Décision liée à l'évaluation de fiabilité**

### **4. Évaluation de fiabilité positive**

- 4.1 Briefing en matière de sécurité
- 4.2 Comment remplir un « *Formulaire de demande/mise à jour du nom d'utilisateur et du mot de passe iSMRP* » (obligatoire)

### **5. Dossiers d'évaluation de fiabilité**

- 5.1 Conservation, élimination et accès

## **6. Annulation d'un nom d'utilisateur et d'un mot de passe iSMRP**

- 6.1 Comment remplir le « *Formulaire d'annulation du nom d'utilisateur et du mot de passe iSMRP* »

## **PARTIE II : Sécurité liée à la TI**

1. **Historique**
2. **Environnement iSMRP**
3. **Exigences : Ordinateurs autonomes (non réseautés) qui donnent accès à l'iSMRP**
4. **Recommandations : Réseaux et ordinateurs réseautés**

## **PARTIE III : Sécurité matérielle**

1. **Historique**
2. **Exigences**

## **PARTIE IV : Atteintes et violations liées à la sécurité**

### **Annexes**

**Annexe A** – Orientation

**Annexe B** – *Formulaire d'autorisation et d'évaluation de la fiabilité de l'utilisateur iSMRP*

**Annexe C** – Exigences liées à la sécurité de l'utilisateur iSMRP

**Annexe D** – *Formulaire de demande/mise à jour du nom de l'utilisateur et du mot de passe iSMRP*

**Annexe E** – *Formulaire d'annulation du nom de l'utilisateur et du mot de passe iSMRP*

**Annexe F** – *Formulaire de commentaires*

## Sommaire

En 1999, Citoyenneté et Immigration Canada (CIC) a mis au point le Cadre d'imputabilité pour les programmes de contributions (CIPC). Ces programmes comprenaient les suivants : Cours de langue pour les immigrants au Canada (CLIC), Programme d'établissement et d'adaptation des immigrants (PEAI), Programme d'accueil et Programme d'aide au rétablissement (PAR). L'Immigration – Système de mesure pour la reddition de comptes concernant les programmes de contributions (iSMRP) a été conçu pour soutenir la mesure du rendement du CIPC. L'iSMRP est un système fondé sur Internet qui recueille des données sur les clients et sur les services provenant des fournisseurs de services (FS) qui reçoivent du financement sous forme de contributions. L'information recueillie permet aux FS et à CIC d'offrir de meilleurs services aux clients, d'accroître l'efficacité des programmes et de montrer au public que les fonds sont dépensés de manière responsable.

L'information sur les clients recueillie dans l'iSMRP équivaut au renseignement protégé au gouvernement fédéral comme étant également « de nature particulièrement délicate », c'est-à-dire que l'on peut raisonnablement s'attendre à ce que sa divulgation nuise de façon considérable aux particuliers visés et qu'un minimum de mesures de protection doivent être en place pour la préserver.

CIC est tenu de protéger les renseignements personnels sur les clients en vertu de la législation fédérale relative à la protection de la vie privée. Cette exigence est élargie aux FS au moyen d'une entente de contribution. Au moment du développement de l'iSMRP, CIC a été informé par des experts en sécurité et en renseignements personnels de l'intérieur et de l'extérieur que, parce qu'il s'agit d'un système fondé sur Internet et en raison de la quantité de renseignements sur les clients qu'il renferme, des mesures de sécurité particulières doivent être introduites pour protéger l'information. Par conséquent, CIC a une obligation d'élaborer des mesures de sécurité précises pour l'environnement iSMRP. Ces mesures de sécurité sont décrites dans le présent document et comprennent des **exigences** en matière de sécurité de l'utilisateur, et de sécurité technologique et matérielle. CIC fait également une série de **recommandations** dont l'implantation sera laissée à la discrétion des FS. CIC encouragera les FS ainsi que leurs conseils d'administration (le cas échéant) à mettre en œuvre toute politique et toute procédure supplémentaire qu'ils jugent nécessaire à la protection des clients et de leurs renseignements personnels.

- **Exigences de sécurité liée à l'utilisateur :**
  - CIC requiert que tous les utilisateurs obtiennent un « nom d'utilisateur » et un « mot de passe » pour accéder à l'iSMRP. Avant de les obtenir, les utilisateurs FS (y compris les employés et les bénévoles) doivent subir une évaluation de fiabilité et se révéler fiables aux yeux du directeur général ou d'une personne autorisée. L'évaluation de fiabilité est

comparable à la « vérification de fiabilité approfondie » du gouvernement fédéral et sera fondée sur a) une vérification des documents/références **ou** la connaissance personnelle du particulier de la part du directeur général; et b) les résultats d'une vérification du casier judiciaire.

- Note : Les employés de longue date d'un FS, les personnes qui ont déjà fait l'objet d'une vérification de casier judiciaire chez un FS ou les employés d'un FS qui sont devenus des résidents permanents l'année précédant leur demande de nom d'utilisateur et de mot de passe sont exempts de l'obligation de l'évaluation de fiabilité.

#### **Exigences liées à la sécurité technologique :**

- Pour protéger l'information sur les clients dans l'iSMRP contre des menaces de l'extérieur comme celles qui proviennent d'Internet et de menaces de l'intérieur, comme un accès non autorisé, CIC demande aux FS d'installer un progiciel antivirus et un coupe-feu (McAfee VirusScan 7 ou l'équivalent) dans tous les ordinateurs autonomes qui ont accès à l'iSMRP. Les utilisateurs sont également tenus d'installer un mot de passe d'accès et un économiseur d'écran protégé par mot de passe.
- CIC **recommande** également que la protection par antivirus et coupe-feu soit installée dans les réseaux afin de protéger les ordinateurs réseautés.

#### **Exigences liées à la sécurité matérielle :**

- CIC demande aux utilisateurs de prendre des précautions minimales pour éviter l'accès à l'iSMRP par des personnes non autorisées. Cela comprend ce qui suit : veiller à ce que les écrans des ordinateurs soient orientés de manière à ce qu'on ne puisse les voir à partir des secteurs d'accès publics et des fenêtres lorsqu'iSMRP est utilisé. Cela signifie également de veiller à ce que les noms d'utilisateurs et les mots de passe ne soient pas affichés là où du personnel non autorisé pourrait les voir, à ce qu'ils ne soient partagés avec personne et à ce que les ordinateurs ne soient pas laissés sans surveillance lorsqu'ils sont connectés à l'iSMRP.

Les exigences en matière de sécurité décrites dans le présent document feront partie de l'entente de contribution CIC avec les FS. CIC fournira une indemnité de démarrage **unique** afin de couvrir les frais comme les vérifications de casier judiciaire pour les utilisateurs iSMRP identifiés, le logiciel McAfee pour les ordinateurs qui accèdent à l'iSMRP et la période voulue pour former les utilisateurs. Des frais continus supplémentaires associés à ces exigences pourraient être négociés avec les bureaux de CIC locaux. Il y aura une **période de mise en place progressive de six mois** à partir du moment où les FS sont formés officiellement pour l'utilisation de l'iSMRP – CLIC, PEAI et du Programme d'accueil, jusqu'au

moment où l'on s'attend à ce qu'ils aient terminé la mise en oeuvre de ces exigences. La période de mise en place pour les FS qui offrent le PAR durera jusqu'à la signature de la prochaine entente de contribution, ou le premier avril 2003, si ils signent une nouvelle entente en janvier 2003.

Un formulaire de rétroaction à être complété par les FS est joint à la fin de ce document dans le but d'obtenir des commentaires sur les exigences en matière de sécurité. Des commentaires reçus serviront à déterminer si des modifications doivent être faites.

On peut obtenir de l'orientation ou de l'aide au sujet de ces exigences auprès des membres de l'Équipe de travail chargée de l'imputabilité CIC dont la liste figure à l'**Annexe A**.

## Introduction

En 1999, Citoyenneté et Immigration Canada (CIC) a lancé la mise en oeuvre du Cadre d'imputabilité pour les programmes de contributions (CIPC) pour ses programmes de contributions liés à l'établissement et au rétablissement. Ces programmes comprenaient le Cours de langue pour les immigrants au Canada (CLIC), le Programme d'établissement et d'adaptation des immigrants (PEAI), le Programme d'accueil et le Programme d'aide au rétablissement (PAR). Le CIPC a pour but d'assurer la responsabilité de dépenses ministérielles, le contrôle de la prestation de services et l'évaluation de l'efficacité des programmes de contributions dans la réponse aux besoins en établissement des nouveaux arrivants. Le CIPC comporte les cinq composantes suivantes :

- Évaluation
- Mesure du rendement
- Processus lié aux ententes de contribution
- Cadre de contrôle de gestion
- Responsabilisation à l'échelle provinciale et territoriale

Depuis l'an 2000, CIC a mis l'accent sur la composante de la mesure du rendement, ce qui supposait le recours au développement d'Immigration – Système de mesure pour la reddition de comptes concernant les programmes de contribution (iSMRP) en collaboration avec les fournisseurs de services (FS) qui reçoivent du financement sous forme de contributions. L'iSMRP est un système fondé sur Internet conçu pour recueillir des données de mesure du rendement. Il permet aux FS de fournir des données cohérentes et fiables sur les programmes à CIC. L'information aide les FS et CIC à offrir une meilleure prestation de services aux clients, à accroître l'efficacité des programmes et à montrer au public que les fonds sont dépensés de manière responsable. Avec l'implantation d'autres composantes

du CIPC, CIC devrait être bien en mesure de faire rapport sur les résultats obtenus.

L'iSMRP recueille de l'information sur des clients particuliers pour le CLIC et pour le PAR et des données globales ou individuelles (facultatives) sur les clients pour le PEAI et le Programme d'accueil. L'information recueillie comprend le nom, la date de naissance, le numéro d'immigration et les services reçus liés aux clients. En raison du type (p. ex. de l'information personnelle) et de la quantité d'information dans l'iSMRP, cette dernière équivaut à des renseignements « protégés » au gouvernement fédéral qui sont également « de nature particulièrement délicate », ce qui signifie que l'on pourrait s'attendre, raisonnablement, à ce que leur divulgation entraîne de graves problèmes pour les particuliers visés. Elle doit, par conséquent, faire l'objet de mesures de confidentialité conformément à certaines normes minimales.

CIC est tenu de protéger les renseignements personnels des clients en vertu de la législation fédérale sur la protection de la vie privée. Cette exigence est élargie aux FS par l'intermédiaire de l'entente de contribution.

Pour assurer la protection des renseignements sur les clients dans l'iSMRP et dans le cadre du processus de développement d'un système fondé sur Internet, CIC a effectué un certain nombre d'évaluations des renseignements personnels et de la sécurité. Cela comprend une évaluation de la menace et des risques ainsi qu'une évaluation des répercussions sur les renseignements personnels (un sommaire est accessible à l'adresse suivante : [www.integration-net.cic.gc.ca](http://www.integration-net.cic.gc.ca)). CIC a également tenu des consultations sur ces questions auprès du Commissariat à la protection de la vie privée du Canada, de partenaires de l'extérieur et de spécialistes ministériels internes. Pour l'aider à respecter ses obligations en vertu de la législation fédérale sur la protection de la vie privée, on a conseillé à CIC de mettre en œuvre des exigences particulières en matière de sécurité pour l'environnement iSMRP. Ces exigences sont décrites dans le présent document et comprennent des mesures liées à la sécurité du personnel, à la sécurité technologique et matérielle. Elles sont fondées sur la politique actuelle du gouvernement fédéral en matière de protection de la vie privée et de la sécurité et sont conçues pour protéger l'information sur les clients dans les bases de données de l'iSMRP et des FS. Il convient de remarquer que l'adoption de ces types de mesures constitue une bonne pratique pour tout environnement où des renseignements personnels sont recueillis et stockés.



La **Partie I** du document décrit les exigences en matière de sécurité du personnel ou des utilisateurs. Tous les utilisateurs sont tenus d'être soumis à une évaluation de fiabilité menée par le directeur général (DG) des FS ou par une personne autorisée avant la demande d'un « nom d'utilisateur » et d'un « mot de passe » d'accès à l'iSMRP. Cette évaluation est comparable à la « vérification de fiabilité approfondie » du gouvernement fédéral et comprend une vérification de la fiabilité passée de l'utilisateur pour déterminer sa fiabilité future en relation avec la

protection des renseignements sur les clients dans l'iSMRP. Le DG basera sa décision sur les vérifications des documents et des références ou sur ses connaissances personnelles du particulier et des résultats d'une vérification du casier judiciaire. Les utilisateurs qui reçoivent une évaluation de fiabilité positive peuvent demander l'accès à l'iSMRP. L'évaluation ne confère au particulier aucun statut du gouvernement fédéral en matière de sécurité. Elle consiste à être utilisée strictement à des fins d'accès à l'iSMRP et ne vise aucunement à avoir un effet quelconque sur les relations d'emploi entre le particulier et les FS.



Les **Parties II et III** de ce document traitent des exigences liées à la sécurité technologique et matérielle, respectivement. La sécurité technologique se rapporte aux mesures de sécurité qui ont été conçues pour protéger l'information contre des menaces de l'extérieur, comme celles provenant d'Internet ou contre des menaces intérieures, comme celles provenant de particuliers qui cherchent à obtenir un accès non autorisé. On trouve également dans cette partie des recommandations visant à améliorer la sécurité technologique. La sécurité matérielle suppose la présentation et la conception adéquates des installations et l'utilisation de mesures visant à empêcher l'accès non autorisé.



La **partie IV** traite des mesures à prendre par le DG et (ou) les utilisateurs dans l'éventualité d'une atteinte à la sécurité ou d'une violation connexe chez un FS qui pourrait toucher la sécurité de l'information sur les clients dans l'iSMRP.

Les FS sont tenus de mettre en œuvre ces exigences en matière de sécurité en vertu de l'entente de contribution CIC dans le cadre du processus de collecte de l'information sur les clients pour l'iSMRP. Ils peuvent demander de l'orientation ou de l'aide sur leur mise en œuvre aux membres de l'Équipe de travail chargée de l'imputabilité CIC, dont la liste figure à l'Annexe A.

## PARTIE I : Sécurité des utilisateurs

### 1. Évaluation de la fiabilité des utilisateurs

#### 1.1 Historique

CIC offre aux utilisateurs FS (employés et bénévoles) un nom d'utilisateur et un mot de passe, sur une base du « besoin de savoir » et avec l'autorisation du directeur général (DG) ou d'une personne autorisée par le DG, les références au « DG » dans le présent document comprennent la personne autorisée. Le terme « utilisateur » dans le présent document se rapporte aux personnes qui font une demande et à celles qui ont un nom d'utilisateur et un mot de passe. Le DG ne peut donner son autorisation que lorsqu'il a effectué une évaluation de fiabilité de l'utilisateur (les exceptions sont énumérées à la section 1.3) et lorsqu'il a déterminé que cette personne est fiable pour accéder à de l'information sur les clients dans l'iSMRP.

#### 1.2 Vérification de l'information

Une évaluation de fiabilité par le DG suppose la vérification de certains documents et une vérification du casier judiciaire afin d'évaluer la sincérité, l'honnêteté, la droiture et la fiabilité de l'utilisateur. La Partie A du tableau ci-après sert de guide pour décider quelle information (autre que les résultats de la vérification du casier judiciaire) doit être vérifiée au moment d'une évaluation. Plutôt que de vérifier un ou plusieurs de ces documents, le DG peut choisir de se fier à sa **connaissance personnelle** du particulier. Il est obligatoire, toutefois, de prendre en considération les résultats d'une vérification de casier judiciaire (Partie B du tableau) lorsqu'il prend sa décision liée à l'évaluation de fiabilité.

**Tableau d'évaluation de la fiabilité de l'utilisateur iSMRP :**

Information de l'utilisateur à vérifier	But de la vérification	Exemples de ce qu'il faut vérifier
<b>Partie A</b>		
Date de naissance (c.-à-d. données personnelles)	Vérifier si l'identité de la personne faisant l'objet de la vérification est authentique.	<ul style="list-style-type: none"> <li>• Certificat de naissance</li> <li>• Autre document officiel vérifiable</li> </ul>
Adresse (c.-à-d. données personnelles)	Même que précédemment	<ul style="list-style-type: none"> <li>• Permis de conduire</li> <li>• Bail ou autre document officiel vérifiable</li> </ul>
Études et qualités	Vérifier l'honnêteté du	<ul style="list-style-type: none"> <li>• Études/certificats</li> </ul>

professionnelles	particulier au sujet de ses antécédents personnels et professionnels.	professionnels <ul style="list-style-type: none"> <li>Autre document officiel provenant d'un établissement d'enseignement, par exemple une lettre</li> </ul>
Antécédents professionnels	Déterminer si le particulier a été fiable et vérifier s'il est sincère au sujet de ses antécédents personnels et professionnels. <b>Cela ne comprend pas une vérification de crédit.</b>	<ul style="list-style-type: none"> <li>Contact avec des employeurs précédents</li> </ul>
Références/réputation personnelle	Déterminer si la personne a été honnête, sincère et fiable.	<ul style="list-style-type: none"> <li>Doivent être limitées aux références fournies par le particulier.</li> </ul>
Partie B Vérification du casier judiciaire	Déterminer si l'utilisateur a, par le passé, commis des crimes qui pourraient indiquer un risque inacceptable en relation avec l'accès aux renseignements sur les clients dans l'iSMRP.	<ul style="list-style-type: none"> <li>À obtenir, par le particulier, du bureau de police local ou de la GRC.</li> </ul>

### 1.3 Exceptions

Vous trouverez ci-après des situations au cours desquelles des personnes, qui ont autrement été autorisées par le DG à faire une demande de nom d'utilisateur et de mot de passe, sont exemptées de la nécessité de subir une vérification de fiabilité : (toutefois le DG a la possibilité d'en effectuer une)

1. Les personnes qui ont été employées par un FS pendant une période d'au moins **trois ans**.
2. Des particuliers employés par des FS qui ont subi des vérifications d'antécédents criminels et de sécurité dans le cadre d'une demande de résidence permanente et qui sont devenues des résidents permanents dans l'année précédant leur demande d'un nom d'utilisateur et d'un mot de passe.
3. Des personnes qui, aux fins d'un emploi ou lorsqu'employées par un FS, ont subi une vérification de casier judiciaire en vertu d'un des éléments suivants :

- ✓ Politique interne en matière de sécurité (FS)
  - ✓ Politique en matière de sécurité d'autres fournisseurs de fonds/partenaires
  - ✓ Législation en matière de sécurité fédérale/provinciale/municipale
4. Des utilisateurs existants qui deviennent employés d'un FS différent, sont tenus de faire une demande de nouveaux noms d'utilisateur et de nouveaux mots de passe, mais qui ne sont pas tenus de subir une vérification de fiabilité.

#### **1.4 Conflit d'intérêt**

Les DG ne doivent pas exécuter leur propre vérification de fiabilité.

#### **1.5 Validité, mise à jour et révocation**

Une évaluation de fiabilité positive aux fins d'obtenir un nom d'utilisateur et un mot de passe reste valide pendant **dix ans** au cours desquels un utilisateur est employé par le FS courant ou un autre; toutefois, le DG peut les mettre à jour ou les révoquer à n'importe quel moment. Une mise à jour suppose seulement l'évaluation des résultats d'une nouvelle vérification de casier judiciaire.

#### **1.6 Sous-contrats**

Il incombe aux DG de remplir les évaluations de fiabilité des utilisateurs qui travaillent pour des organismes avec lesquels le FS a des sous-contrats. Par ailleurs, ils peuvent déléguer la tâche au responsable de cette organisation.

## **2. Traitement de l'information des évaluations de fiabilité**

### **2.1 Obtention du consentement**

Les DG doivent :

- ✓ Veiller à ce qu'aucune collecte d'information liée à une évaluation de fiabilité ne soit entreprise sans le consentement de la personne visée.
- ✓ Informer les particuliers qui ne consentent pas à ces vérifications qu'on ne tiendra plus compte de leur demande d'accès à l'iSMRP.

## 2.2 Vérification de l'information personnelle, sur les études et sur l'emploi et (ou) des références

Les DG doivent limiter leur vérification des renseignements personnels, sur les études et sur l'emploi et (ou) des références (par exemple les éléments dans la Partie A du tableau d'évaluation de la fiabilité de l'utilisateur iSMRP) aux **cinq dernières années**. La vérification de l'un ou de tous ces éléments contribue à l'évaluation par le DG visant à établir si un utilisateur est fiable, honnête et sincère.

## 2.3 Vérification du casier judiciaire

Une vérification du casier judiciaire est effectuée par le poste de police local ou par la section civile de la Gendarmerie royale du Canada (GRC) selon le bureau qui a l'autorité voulue dans la région du FS. Un certificat indiquant les résultats est émis. L'existence d'un casier judiciaire peut être, mais n'est pas nécessairement, suffisante pour refuser la fiabilité. Un casier judiciaire peut être envisagé à la lumière des fonctions et des tâches à exécuter, de la nature et de la fréquence du délit et du temps qui s'est écoulé depuis.

Le DG doit déterminer ce qui suit :

- L'attitude de la personne face à un délit pour lequel elle n'a pas été graciée et la mesure selon laquelle elle a modifié son comportement à cet égard.
- La récurrence probable de délits semblables et leur effet possible sur la fiabilité du particulier.

Le DG ne doit pas demander de renseignements au sujet d'une infraction criminelle pour laquelle une **grâce** a été accordée.

Les résultats d'une vérification de casier judiciaire pour le processus d'évaluation de fiabilité iSMRP restent valides pour une période de **douze** mois après la date d'émission.

## 2.4 Comment remplir un « *Formulaire d'autorisation et d'évaluation de la fiabilité de l'utilisateur iSMRP* »

Lorsqu'ils remplissent une évaluation, les DG doivent utiliser le :

« **Formulaire d'autorisation et d'évaluation de la fiabilité de l'utilisateur iSMRP** »  
(Annexe B)

Ce formulaire a été conçu comme outil pour faciliter le travail des DG et il n'est pas nécessaire de le remplir.

### 3. Décision liée à l'évaluation de fiabilité

Lorsqu'il prend une décision en matière d'évaluation de fiabilité, on s'attend à ce que le DG donne une évaluation juste et objective qui respecte les droits du particulier. La question à laquelle il faut répondre consiste à savoir si on peut se fier au particulier qui respectera la confiance qui peut lui être accordée en lui donnant accès aux renseignements sur les clients dans l'iSMRP.

En d'autres termes, y a-t-il un motif raisonnable de croire que le particulier peut exploiter les biens et l'information à son profit personnel, négliger de protéger l'information et les biens qui lui sont confiés ou faire preuve d'un comportement qui aurait des répercussions négatives sur sa fiabilité? De telles décisions supposent une évaluation de tous les risques liés au fait d'accorder l'accès et de juger si de tels risques sont acceptables ou non.

La décision du DG selon laquelle le risque est acceptable signifie que l'utilisateur a reçu une détermination positive au sujet de l'état de fiabilité et qu'il peut demander un nom d'utilisateur et un mot de passe tels que décrits dans la section suivante.

Si le risque n'est pas acceptable, le particulier n'est pas autorisé à demander un nom d'utilisateur et un mot de passe. De plus, on doit communiquer au particulier les raisons de ce refus.

### 4. Évaluation de fiabilité positive

#### 4.1 Briefing en matière de sécurité

Lorsque les utilisateurs ont reçu une évaluation de fiabilité positive, ils doivent être informés, oralement ou par écrit, de leurs responsabilités en ce qui concerne la protection de l'information sur les clients iSMRP confiée.

**« Exigences liées à la sécurité de l'utilisateur iSMRP » (Annexe C)**

Ces exigences comprennent notamment d'informer le DG lorsqu'il y a une tentative d'accès non autorisé à l'iSMRP ou lorsque l'information sur les clients iSMRP est modifiée, endommagée ou volée. Le DG doit immédiatement transmettre tous les renseignements au sujet de ces types d'incidents à un membre de l'Équipe de travail chargée de l'imputabilité CIC (Voir l'Annexe A).

#### 4.2 Comment remplir un « *Formulaire de demande/mise à jour du nom d'utilisateur et du mot de passe iSMRP* »

Lorsque les utilisateurs ont reçu une évaluation de fiabilité et un briefing en matière de sécurité indiqué ci-dessus, le DG et l'utilisateur doivent remplir le « *Formulaire de demande/mise à jour du nom d'utilisateur et du mot de passe iSMRP* » (Annexe D).

« *Formulaire de demande/mise à jour du nom d'utilisateur et du mot de passe iSMRP* » (Annexe D)

La signature du DG et l'acceptation de l'utilisateur et un mot de passe alors que la signature du DG et l'acceptation de l'utilisateur accepte de se conformer aux exigences liées à la sécurité des renseignements sur iSMRP.

### 5. Dossiers d'évaluation de fiabilité

#### 5.1 Conservation, élimination et accès

##### Conservation :

Les DG sont tenus de conserver un relevé du nombre, de la date d'émission et du responsable de l'émission du certificat de vérification du casier judiciaire de l'utilisateur à des fins de contrôle CIC.

##### Élimination :

Tous les dossiers liés à l'évaluation de fiabilité doivent être détruits deux ans après la date à laquelle l'emploi de l'utilisateur se termine.

##### Accès :

Tout dossier se rapportant à l'évaluation de fiabilité doit être utilisé uniquement aux fins pour lesquelles il a été colligé et ne doit être divulgué à personne (à l'exception du numéro de certificat de vérification du casier judiciaire, de la date d'émission et du responsable, lesquelles pourraient être fournies à CIC) sans le consentement de l'utilisateur.

## 6. Annulation d'un nom d'utilisateur et d'un mot de passe iSMRP

### 6.1 Comment remplir le « *Formulaire d'annulation du nom d'utilisateur et du mot de passe iSMRP* »

Lorsqu'une évaluation de fiabilité d'un utilisateur a été révoquée et qu'il y a une demande d'annulation d'un « nom d'utilisateur » et d'un mot de passe iSMRP, le DG et l'utilisateur doivent signer le formulaire suivant.



« *Formulaire d'annulation du nom d'utilisateur et du mot de passe iSMRP* »  
(Annexe E)

La signature du DG indique la demande d'annulation du nom d'utilisateur et du mot de passe alors que la signature de l'utilisateur indique qu'il comprend son engagement permanent à protéger les renseignements sur les clients iSMRP auxquels il a accès.

## PARTIE II : Exigences et recommandations liées à la sécurité

### 1. Historique

La sécurité en matière de technologie de l'information (TI) vise à assurer la confidentialité et l'intégrité de l'information stockée, traitée ou transmise par voie électronique. Le gouvernement fédéral adopte diverses mesures de sécurité, telles que demandées par la GRC, le Conseil du Trésor et les politiques en matière de sécurité ministérielle TI afin de protéger ses systèmes électroniques. À CIC, par exemple, des mesures de sécurité sont utilisées à divers niveaux du système comme le périmètre du réseau (où le reste du monde se connecte à CIC) et dans le réseau même, comme au niveau du poste de travail individuel. Les mesures de sécurité comprennent, au minimum, un coupe-feu et un logiciel antivirus. De brèves descriptions de ces éléments se trouvent ci-après.

**Coupe-feu :** Ces éléments pourraient être utilisés tant au niveau du réseau et qu'à celui du poste de travail individuel. Ils servent à limiter et à filtrer la circulation d'arrivée et de sortie d'un réseau ou d'un ordinateur en recevant et en transmettant de l'information uniquement à des ports particuliers, ce qui rend plus difficile la prise de contrôle du système provenant de menaces de l'extérieur par un accès aux ports ouverts.

**Détection de virus :** Cet élément peut être utilisé à divers niveaux du système (par exemple au niveau du réseau et de l'ordinateur individuel) pour veiller à ce que tout le trafic qui arrive à ces secteurs soit traité par un détecteur de virus qui examine les messages ou les transmissions afin d'y détecter des codes de virus. Si le message ou la transmission est sûr, il est transmis au destinataire. Dans le cas contraire, il est refusé ou mis en quarantaine. Il convient de remarquer que dans le cas des ordinateurs réseautés, où seuls les ordinateurs sont dotés d'un logiciel antivirus, des transmissions sûres provenant de ces appareils peuvent être altérées lorsqu'elles passent par d'autres dispositifs dans le réseau comme, par exemple, les serveurs. Cela signifie que le message pourrait être infecté et utilisé pour propager le virus dans d'autres appareils ou dans d'autres réseaux. De plus, un ordinateur protégé connecté à un réseau qui a été altéré devient inutile étant

## 2. Environnement iSMRP

CIC met en oeuvre des exigences en matière de sécurité TI et fait des recommandations pour l'environnement iSMRP aux FS afin de veiller à ce toutes les transmissions à la base de données iSMRP soient sûres (c'est-à-dire exemptes de codes malveillants comme des virus qui peuvent avoir été acquis par le FS et transmis par inadvertance). Ils visent également à protéger les bases de données des FS, leurs fichiers et la circulation par courriel contre des menaces provenant de l'Internet.

### 2.1 Exigences : Ordinateurs autonomes (non réseautés) qui donnent accès à l'iSMRP

Ces exigences s'appliquent **uniquement** aux ordinateurs autonomes (non réseautés) qui donnent accès à l'iSMRP. Les FS sont tenus de faire ce qui suit :

#### 1. Installer McAfee VirusScan 7.0, qui est un coupe-feu et un progiciel de protection contre les virus pour les ordinateurs autonomes iSMRP.

La Division de la sécurité TI de CIC a indiqué que, bien qu'aucun logiciel ne soit en mesure de garantir qu'il n'y aura pas d'atteinte à la sécurité du système, le progiciel recommandé devrait fournir une protection raisonnable.

Les FS pourraient utiliser un produit de rechange pourvu que les fonctions de sécurité soient comparables à McAfee VirusScan 7.0.

Note : le logiciel de protection antivirus nécessite une mise à jour régulière (laquelle peut être hebdomadaire) pour être efficace à détecter les nouveaux virus. Les instructions incluses dans l'installation du logiciel vous expliqueront comment faire.

Pour des renseignements supplémentaires sur ce progiciel, consultez le site Web suivant : <http://www.mcafee.com/myapps/vs7/>

Pour obtenir davantage de sécurité, nous exigeons que chaque utilisateur installe ce qui suit dans son ordinateur autonome qui donne accès à l'iSMRP :

#### 2. un mot de passe d'accès (qui doit être modifié périodiquement)


#### 3. un économiseur d'écran protégé par mot de passe (une période d'activation d'un maximum de 15 minutes de non-utilisation est suggérée).

## 2.2 Recommandations : Réseaux et ordinateurs réseautés

Dans le cas des ordinateurs réseautés, il est inefficace d'installer un logiciel de protection dans des ordinateurs individuels si le réseau lui-même n'est pas doté d'un logiciel de protection particulièrement conçu à cet effet. Pour cette raison, CIC **recommande** ce qui suit pour les réseaux et les ordinateurs réseautés :

- Les FS qui utilisent un réseau (ou le réseau de quelqu'un d'autre, comme une commission scolaire, etc.) veillent à sa protection au moyen, au minimum, d'un coupe-feu et d'une technologie antivirus spécifique au réseau.
- Les FS installent un logiciel antivirus dans des postes de travail individuels connectés au réseau.

Le fait de mettre en oeuvre ces mesures de sécurité réduira considérablement le risque de menaces technologiques pour les systèmes et les bases de données des FS ainsi que pour l'iSMRP.

 **Note : Les FS qui exploitent des réseaux sans coupe-feu et sans logiciel de protection antivirus spécifique au réseau sont tenus d'entrer les données iSMRP dans des ordinateurs autonomes dotés du progiciel de protection requis tel que décrit dans la section 2.1.**

Les FS pourraient envisager de se procurer une technologie de protection supplémentaire pour les réseaux comme la détection d'intrusion et l'inspection du contenu selon les descriptions ci-après.

**Détection d'intrusion :** Cette protection peut être combinée à un dispositif de coupe-feu ou à un logiciel qui surveille les modèles de circulation et repère les tentatives d'accès non autorisé à un réseau. Il recueille l'information à l'origine de la transmission et prend diverses mesures comme mettre fin à la connexion jusqu'à informer l'administrateur du système qu'une intrusion dans le système ou qu'une atteinte à sa sécurité est en cours. Il est très souvent bien utile dans la prévention de tentatives d'accès ou d'essais futurs.

**Inspection du contenu :** Il s'agit d'une détection du genre détection de virus mais à l'inverse. Ce logiciel examine les messages et ne transmet que ceux qui sont d'une source légitime et dans un format correct acceptable. Il convient de remarquer que des transmissions sûres provenant d'appareils protégés peuvent être altérées quant elles passent par des dispositifs dans un réseau, comme des serveurs. Cela signifie que ces messages peuvent être infectés et utilisés pour propager des virus dans d'autres appareils ou dans d'autres réseaux.

L'inspection du contenu détectera des codes malveillants cachés à l'intérieur de

En plus, du matériel/logiciel de protection de réseau, nous **recommandons** que les FS disposent de ce qui suit :

- Un système de gestion des mots de passe : il s'agit d'un système géré par un administrateur de réseau par lequel les utilisateurs sont tenus d'installer des mots de passe d'accès exclusifs et au moyen desquels on leur rappelle et on exige qu'ils doivent les modifier régulièrement. L'administrateur de réseau veille également à ce que des mots de passe répétés et anciens soient éliminés.

Tel que requis pour les ordinateurs autonomes qui accèdent à l'iSMRP, les ordinateurs réseautés devraient également être dotés d'économiseurs d'écran protégés par mot de passe (Il est suggéré qu'ils s'activent après un maximum de 15 minutes de non-utilisation.)

## **PARTIE III : Sécurité matérielle**

### **1. Historique**

L'évaluation de la menace et des risques pour l'iSMRP a permis d'examiner les risques d'accès non autorisé à l'information en relation avec l'emplacement matériel des installations, y compris les ordinateurs, chez les FS. L'évaluation a permis de remarquer que des mesures de sécurité matérielle inappropriées pourraient entraîner l'accès non autorisé à un poste de travail iSMRP et (ou) à de l'information de nature délicate. De plus, les moniteurs situés dans des endroits d'accès public, des bureaux avec fenêtre, etc., peuvent ne pas être placés de manière à éviter d'être vus par des personnes non autorisées (de l'intérieur ou de l'extérieur). Ces situations pourraient avoir des répercussions sur la confidentialité de l'information de nature délicate.

### **2. Exigences**

Par conséquent, CIC exige que les mesures de sécurité matérielle suivantes soient mises en place :

- Les moniteurs des ordinateurs au moyen desquels on a accès à l'iSMRP doivent être placés loin des fenêtres ou des zones d'accès public pour empêcher que des personnes non autorisées puissent les voir ou y avoir accès.
- Les utilisateurs ne doivent pas afficher leur nom d'utilisateur et leur mot de passe là où ils peuvent être vus par du personnel non autorisé, ne doivent pas les partager et ne doivent pas laisser leurs ordinateurs sans surveillance quand ils sont connectés à l'iSMRP.

## PARTIE IV : Atteintes et violations liées à la sécurité

Les DG doivent donner des instructions à tout leur personnel, en plus des utilisateurs de l'iSMRP, les informer immédiatement lorsqu'ils prennent connaissance d'une violation ou d'une atteinte à la sécurité qui pourrait influencer sur la sécurité de l'information sur les clients.

### Atteinte à la sécurité :

Se rapporte à la **divulgation** non autorisée de l'information sur les clients.

### Violations en matière de sécurité :

Événements qui auraient pu conduire à une atteinte à la sécurité, mais qui ne l'ont pas été.

Ces événements peuvent se rapporter à une menace provenant d'Internet comme un virus ou un intrus ou à des personnes non autorisées qui essaient d'obtenir l'accès à de l'information sur les clients dans l'iSMRP.

En plus de suivre leurs procédures de sécurité normales, les DG doivent immédiatement informer un membre de l'Équipe de travail chargée de l'imputabilité CIC (Voir l'Annexe A) de manière à pouvoir évaluer leurs répercussions sur la base de données iSMRP. Le DG devrait également avertir le bureau local de CIC responsable de l'entente de contribution. Les deux bureaux devraient également être tenus informés, à intervalles réguliers, du résultat final toutes les fois qu'une enquête est menée.

## **Annexe A**

Pour obtenir des conseils et de l'orientation sur l'application de ces exigences, communiquez avec les personnes suivantes :

**ADMINISTRATION CENTRALE  
NATIONALE**

Teresa Pires  
Gestionnaire du programme  
Direction générale de l'intégration, Division de  
l'établissement  
Citoyenneté et Immigration Canada  
300, rue Slater, 5<sup>e</sup> étage  
Ottawa (Ontario) K1A 1L1  
Tél. : (613) 952 – 6321  
Télé. : (613) 952 – 7416  
Courriel : [teresa.pires@cic.gc.ca](mailto:teresa.pires@cic.gc.ca)

Lanielle Caron  
Conseillère principale, politique et programmes  
Direction générale de l'intégration, Division de  
l'établissement  
Citoyenneté et Immigration Canada  
300, rue Slater, 5<sup>e</sup> étage  
Ottawa (Ontario) K1A 1L1  
Tél. : (613) 952-2561  
Télé. : (613) 952-7416  
Courriel : [lanielle.caron@cic.gc.ca](mailto:lanielle.caron@cic.gc.ca)

Catherine Smith  
Conseillère principale, politique et programmes  
Direction générale de l'intégration, Division de  
l'établissement  
300, rue Slater, 5<sup>e</sup> étage  
Ottawa (Ontario) K1A 1L1  
Tél. : (613) 957-8014  
Télé. : (613) 952-7416  
Courriel : [catherine.smith@cic.gc.ca](mailto:catherine.smith@cic.gc.ca)

**ATLANTIQUE**

Bruna Caracristi  
Spécialiste des programmes  
Direction générale de l'intégration, Division de  
l'établissement  
Citoyenneté et Immigration Canada  
300, rue Slater, 5<sup>e</sup> étage  
Ottawa (Ontario) K1A 1L1  
Tél. : (613) 957-8526  
Télé. : (613) 952-7416  
Courriel : [bruna.caracristi@cic.gc.ca](mailto:bruna.caracristi@cic.gc.ca)

**PRAIRIES**

Iris Bemister  
Spécialiste des programmes  
Direction générale de l'intégration, Division de  
l'établissement  
a/s CIC de Regina  
Citoyenneté et Immigration Canada  
1871, rue Hamilton  
Regina (Saskatchewan) S4P 2B9  
Tél. : (306) 780-5257  
Télé. : (306) 780-8745  
Courriel : [iris.bemister@cic.gc.ca](mailto:iris.bemister@cic.gc.ca)

**ONTARIO**

John Lu  
Spécialiste des programmes  
Direction générale de l'intégration, Division de  
l'établissement  
a/s OASIS  
Citoyenneté et Immigration Canada  
74, rue Victoria, Pièce 1001  
Toronto (Ontario) M5C 2S1  
Tél. : (416) 952-8967  
Télé. : (416) 973-9027  
Courriel : [john.lu@cic.gc.ca](mailto:john.lu@cic.gc.ca)

**Annexe B**

<b>Formulaire de demande d'autorisation et de vérification de la fiabilité pour l'utilisateur de l'iSMRP (facultatif)</b>	
<input type="checkbox"/> Nouveau <input type="checkbox"/> Mise à jour	
<b>PARTIE A À REMPLIR PAR L'UTILISATEUR</b>	
Nom de famille:	Prénoms au complet (pas initiales) <u>soulignez le prénom usuel</u> :
Nom de famille à la naissance :	Tous les autres noms utilisés :
Date de naissance : Y-A    M-M    D-J	Sexe : <input type="checkbox"/> Homme <input type="checkbox"/> Femme
Numéro de téléphone : Domicile : (    )    Travail : (    )	
Adresse du domicile :	Ville/Municipalité :    Province :    Code postal :
<b>PARTIE B RENSEIGNEMENTS SUR LE POSTE</b>	
Titre du poste :	
<b>PARTIE C VÉRIFICATION DE LA FIABILITÉ ET CONSENTEMENT</b>	
REMARQUE : À moins d'être annulé par l'intéressé, le présent formulaire de consentement autorisera les vérifications précisées ci-après, y compris celles requises pour les mises à jour ultérieures.	
_____	_____
Signature de l'intéressé	Date
<input type="checkbox"/> Date de naissance	<input type="checkbox"/> Antécédents de travail
<input type="checkbox"/> Adresse	<input type="checkbox"/> Références
<input type="checkbox"/> Études/Qualifications professionnelles	Vérification de casier judiciaire - Veuillez mentionner : <input type="checkbox"/> Numéro de certificat : Date de délivrance : Fondé de pouvoir :
Je, soussigné, en ma qualité de directeur général (DG) du fournisseur de services (FS) ou de son représentant, atteste, par la présente, que les renseignements donnés plus haut ont été vérifiés. Conformément aux lignes directrices sur la sécurité de l'iSMRP pour les fournisseurs de services, j'estime que cette personne est fiable pour ce qui concerne l'accès à l'iSMRP.	
_____	_____
Signature	Date

Exigences en matière de sécurité pour les fournisseurs de services - iSMRP

---

Nom et titre du représentant officiel :	Adresse au bureau :	Téléphone : (    )	Télocopieur : (    )
---	---------------------	-----------------------	-------------------------

**A**

### Exigences liées à la sécurité de l'utilisateur iSMRP

Tous les utilisateurs iSMRP doivent connaître les exigences suivantes en matière de sécurité et s'y conformer :

1. Seuls les particuliers qui possèdent un nom d'utilisateur et un mot de passe iSMRP ont droit d'accéder à l'iSMRP.
2. Les utilisateurs doivent préserver la confidentialité de leur nom d'utilisateur et de leur mot de passe en tout temps, par exemple ils ne doivent jamais les divulguer, les afficher là où ils peuvent être vus ou les partager avec qui que ce soit.
3. L'information sur les clients dans l'iSMRP est une information de nature délicate et les utilisateurs doivent en préserver la confidentialité en tout temps conformément aux dispositions sur les renseignements personnels de l'entente de contribution CIC.
4. Les utilisateurs ne doivent pas laisser leurs ordinateurs sans surveillance pendant qu'ils sont connectés au iSMRP.
5. Les utilisateurs doivent veiller à ce que leurs ordinateurs soient dotés d'un économiseur d'écran protégé par mot de passe. On suggère une période d'activation qui n'est pas supérieure à 15 minutes de non-utilisation.
6. Les utilisateurs doivent faire face aux écrans de leur ordinateur loin des fenêtres ou des secteurs d'accès public pour éviter la visualisation ou l'accès non autorisé à l'information sur les clients iSMRP.
7. Les utilisateurs doivent signaler immédiatement au directeur général toute tentative ou occurrence liée à un accès non autorisé à l'iSMRP ou à l'information sur les clients iSMRP en vue de la modifier, de l'endommager ou de la voler. Le directeur général des FS doit immédiatement signaler le cas à un membre de l'Équipe d'imputabilité CIC (Voir l'Annexe A).
8. Les utilisateurs qui ne requièrent plus l'accès à l'iSMRP doivent remplir le formulaire intitulé *Annulation du nom d'utilisateur et du mot de passe iSMRP* et indiquer qu'ils sont conscients de leur obligation continue de préserver la confidentialité de l'information iSMRP à laquelle ils ont eu accès.
9. Les utilisateurs doivent savoir que CIC surveille et examine les activités iSMRP et que les noms d'utilisateurs et les mots de passe peuvent être retirés à n'importe quel moment.

## Annexe D

### Formulaire de demande/mise à jour du nom d'utilisateur et du mot de passe iSMRP

Tous les renseignements demandés dans le présent formulaire doivent être fournis pour qu'un « nom d'utilisateur » et un « mot de passe » soient attribués à un nouvel utilisateur du Immigration-Système de mesure pour la reddition de comptes concernant les programmes de contributions (iSMRP), pour remplacer un mot de passe oublié ou mettre à jour les coordonnées d'un utilisateur. Les directives pour l'envoi du formulaire se trouvent à la fin du formulaire.

#### Coordonnées du Fournisseur de services (FS)

Nom du FS :			
Adresse :			
Ville :	Province :	Code postal :	
Numéro d'identification dans le iSMRP :			

#### Coordonnées du directeur général (ou personne autorisée)

Salutation (M., M <sup>me</sup> , etc.) :	Prénom :	Nom de famille :	
Titre :			
Numéro de téléphone et poste :	( )	Numéro de télécopieur :	( )
Adresse de courriel :			

#### Coordonnées de l'utilisateur

Salutation (M., M <sup>me</sup> , etc.) :	Prénom :	Nom de famille :	
Titre :			
Numéro de téléphone et poste :	( )	Numéro de télécopieur :	( )
Adresse de courriel :			

**Demande d'accès pour l'utilisateur :** Le directeur général doit préciser le(s) programme(s) et le(s) niveau(x) d'accès (Accès ordinaire = Entrer des données, sauvegarder, modifier, voir des rapports statistiques; Accès avancé = Ordinaire plus supprimer, corriger les erreurs et gérer les périodes visées par l'entrée des données. Il ne faudrait qu'un seul utilisateur à l'accès avancé par FS.)

Programmes iSMRP auxquels l'utilisateur a besoin d'accéder (faire un X dans toutes les cases appropriées) :		Privilèges demandés pour l'utilisateur dans chaque programme (faire un seul X par ligne) :			
i. iSMRP-PAR		Accès ordinaire		Accès avancé	
ii. iSMRP-CLIC Évaluation		Accès ordinaire		Accès avancé	

iii. iSMRP-CLIC Formation		Accès ordinaire		Accès avancé	
iv. iSMRP-PEAI Sommaire		Accès ordinaire		Accès avancé	
v. iSMRP-PEAI Individuel		Accès ordinaire		Accès avancé	
vi. iSMRP-Programme d'accueil sommaire		Accès ordinaire		Accès avancé	
vii. iSMRP-Programme d'accueil individuel		Accès ordinaire		Accès avancé	

Date où l'utilisateur aura besoin d'y avoir accès (aaaa-mm-jj) :	
--	--

L'utilisateur doit fournir une **Question confidentielle** et une **Réponse confidentielle** ci-dessous (par exemple : Question confidentielle = Mon film préféré est? Réponse confidentielle = Les Parapluies de Cherbourg). Cette information permettra au Soutien iSMRP de vérifier l'identité de l'utilisateur.

Question confidentielle :	
Réponse confidentielle :	

#### DÉCLARATION DE L'UTILISATEUR :

Je reconnais avoir reçu des instructions orales ou écrites sur les exigences en matière de sécurité d'iSMRP à l'annexe C des « iSMRP Exigences en matière de sécurité pour les fournisseurs de services » et je consens à les respecter ou mon accès à l'iSMRP pourra m'être révoqué.

Signature de l'utilisateur :	
Date (aaaa-mm-jj) :	

#### DÉCLARATION DU DIRECTEUR GÉNÉRAL (OU DE LA PERSONNE AUTORISÉE) :

En ma qualité de directeur général, je confirme que l'utilisateur nommé ci-dessus est fiable, d'après les « iSMRP Exigences en matière de sécurité pour les fournisseurs de services » et j'autorise ce formulaire de demande/mise à jour du nom d'utilisateur et du mot de passe avec les accès et les privilèges spécifiés.

Signature du directeur général :	
Date (aaaa-mm-jj) :	

**LES DIRECTIVES POUR L'ENVOI DU FORMULAIRE :**

Ce formulaire doit être posté avec la signature originale de l'utilisateur et du directeur général. Puisque le formulaire contient des renseignements confidentiels, il doit être posté dans une enveloppe double. Veuillez suivre les étapes suivantes :

1. Placez le formulaire dans une enveloppe scellée et inscrite avec les mots PROTÉGÉ B, portant l'adresse suivante :

Lanielle Caron  
Équipe de travail chargée de l'imputabilité  
Direction générale de l'intégration, Division de l'établissement  
Citoyenneté et Immigration Canada  
Tour Jean-Edmonds Nord  
300, rue Slater, 5<sup>e</sup> étage  
Ottawa (Ontario) K1A 1L1

2. Placez cette enveloppe dans une **deuxième** enveloppe sans inscription spéciale portant la même adresse.

**Recevoir le nom d'utilisateur et le mot de passe** : CIC transmettra directement le nom d'utilisateur et le mot de passe à l'intéressé en utilisant les coordonnées fournies sur le présent formulaire.

**Annexe E**

**Formulaire d'annulation  
du nom d'utilisateur et du mot de passe iSMRP**

Tous les renseignements demandés dans le présent formulaire doivent être fournis pour annuler un « nom d'utilisateur » et un « mot de passe » dans le Immigration-Système de mesure pour la reddition de comptes concernant les programmes de contributions (iSMRP). Une annulation doit être demandée lorsqu'un utilisateur n'utilise plus iSMRP. Si la cote de fiabilité de l'utilisateur est expirée ou s'est fait révoquée ou si l'utilisateur a utilisé le système iSMRP d'une façon malveillante, une annulation doit être demandée immédiatement. Les directives pour l'envoi du formulaire se trouvent à la fin de ce formulaire.

**Coordonnées du Fournisseur de services (FS)**

<b>Nom du FS :</b>			
<b>Adresse :</b>			
<b>Ville :</b>	<b>Province :</b>	<b>Code postal :</b>	
<b>Numéro d'identification dans le iSMRP :</b>			

**Coordonnées du directeur général (ou de la personne autorisée)**

<b>Salutation (M., M<sup>me</sup>, etc.) :</b>	<b>Prénom :</b>	<b>Nom de famille :</b>
<b>Titre :</b>		
<b>Numéro de téléphone et poste :</b>	( )	<b>Numéro de télécopieur :</b> ( )
<b>Adresse de courriel :</b>		

**Coordonnées de l'utilisateur**

<b>Salutation (M., M<sup>me</sup>, etc.) :</b>	<b>Prénom :</b>	<b>Nom de famille :</b>
<b>Titre :</b>		
<b>Numéro de téléphone et poste :</b>	( )	<b>Numéro de télécopieur :</b> ( )
<b>Adresse de courriel :</b>		

**Demande d'annulation pour l'utilisateur :** Le directeur général doit préciser le(s) programme(s) qui doivent être annulé(s) pour l'utilisateur.

Accès de l'utilisateur devrait être annulé pour ces programmes iSMRP (faire un X dans toutes les cases appropriées)			
iSMRP-PAR		iSMRP-PEAI Sommaire	
iSMRP-CLIC Évaluation		iSMRP-PEAI Individuel	
iSMRP-CLIC Formation		iSMRP-Programme d'accueil Sommaire	
		iSMRP-Programme d'accueil Individuel	

<b>Raison(s) pour l'annulation -</b> Préciser le nom du programme pour lequel l'accès est annulé :	
---	--

<b>La date à laquelle l'annulation doit être en vigueur (aaaa-mm-jj) :</b>	
--	--

**DÉCLARATION DE L'UTILISATEUR :**

Je reconnais qu'une fois mon accès au iSMRP annulé, j'ai encore l'obligation à garder confidentielles toutes les informations sur les clients dans iSMRP auxquelles j'ai eu accès.

<b>Signature de l'utilisateur :</b>	
<b>Date (aaaa-mm-jj) :</b>	

**DÉCLARATION DU DIRECTEUR GÉNÉRAL (OU DE LA PERSONNE AUTORISÉE) :**

En ma qualité de directeur général j'autorise l'annulation de l'accès au iSMRP, comme précisé sur ce formulaire, pour l'utilisateur nommé ci-dessus.

<b>Signature du directeur général :</b>	
<b>Date (aaaa-mm-jj) :</b>	

**DIRECTIVES POUR L'ENVOI DU FORMULAIRE :**

Ce formulaire doit être posté avec la signature originale de l'utilisateur et du directeur général à :

Lanielle Caron  
Équipe de travail chargée de l'imputabilité  
Direction générale de l'intégration, Division de l'établissement  
Citoyenneté et Immigration Canada  
Tour Jean-Edmonds Nord  
300, rue Slater, 5<sup>e</sup> étage  
Ottawa (Ontario) K1A 1L1

Aucune confirmation de l'annulation ne sera accordée sans une demande particulière.

## Annexe F

### FORMULAIRE DE COMMENTAIRES

#### *Exigences en matière de sécurité iSMRP pour les fournisseurs de services*

Les exigences de sécurité exposées dans les *Exigences en matière de sécurité iSMRP pour les fournisseurs de services* entreront en vigueur dans le cadre de l'Entente de contribution (PEAI, ACCUEIL, CLIC) de CIC six mois après que la formation régulière sur l'iSMRP aura été donnée pour chacun des programmes. Les fournisseurs de services (FS) offrant le PAR devront se soumettre à ces exigences dès le 1<sup>er</sup> avril 2003.

Comme il s'agit de nouvelles exigences, CIC aimerait recueillir les commentaires des FS sur toute question ou préoccupation que vous pourriez avoir concernant leur mise en œuvre et connaître vos suggestions de modifications.

Nous aimerions que tous les commentaires présentés par des employés des FS soient vus par leur directeur général avant d'être transmis à CIC. CIC acceptera vos commentaires jusqu'au **31 mars 2003**. Les commentaires seront étudiés minutieusement et CIC se basera sur ceux-ci pour déterminer si des changements devraient être apportés aux exigences de sécurité de l'iSMRP.

Vos suggestions permettront de faire en sorte que CIC et les FS travaillent en collaboration afin de protéger les renseignements de nature délicate concernant les clients.

#### Commentaires

FORMULAIRE DE COMMENTAIRES

(Page 2)

*Exigences en matière de sécurité iSMRP pour les fournisseurs de services*

Commentaires de : \_\_\_\_\_

Date : \_\_\_\_\_

N° de téléphone : \_\_\_\_\_

Fournisseur de services : \_\_\_\_\_

Ville et province :

Vus par le directeur exécutif :  **Oui**  **Non** (en cocher un)

\*Veuillez faire parvenir vos commentaires à l'Équipe chargée de l'imputabilité par télécopieur, au (613) 952-7416, ou par courriel, à [Catherine.smith@cic.qc.ca](mailto:Catherine.smith@cic.qc.ca). Merci.