CIHR IRSC

ITAMS

Canadian Institutes of Health Research | Instituts de recherche en santé du Canada

Politique d'enquête de sécurité sur le personnel

Table des matières

1. Date d'entrée en vigueur

1.1. La présente politique entre en vigueur le 9 février 2011.
1.2. Elle remplace la *Politique d'enquête de sécurité des IRSC* 2005.

2. Application

2.1. La présente politique s'applique à :

- toutes les personnes qui auront accès aux renseignements et aux biens des IRSC;
- tous les employés, le personnel des instituts, les consultants, les entrepreneurs, les étudiants, les bénévoles ou leurs agents au service des IRSC. Dans le contexte de la présente politique, le terme « personnel » désigne l'ensemble de ces individus.

3. Contexte

La Politique sur la sécurité du gouvernement du Canada exige que les IRSC veillent à ce que toutes les personnes qui auront accès aux renseignements et aux biens du gouvernement fassent l'objet d'une enquête de sécurité appropriée avant de commencer leur travail et soient traitées de manière juste et impartiale.[1] La présente politique décrit la manière dont les IRSC gèrent la sécurité du personnel selon la Politique sur la sécurité du gouvernement.

La sécurité commence en établissant une confiance dans les interactions impliquant le gouvernement et les Canadiens ainsi que dans celles prenant place au sein du gouvernement lui-même. Au sein du gouvernement, il est nécessaire de veiller à ce que les personnes qui ont accès aux renseignements, aux biens et aux services gouvernementaux soient dignes de confiance, fiables et loyales. Le programme de la sécurité du personnel des IRSC a été établi pour appuyer ces exigences.

Le programme de sécurité du personnel limite l'accès aux renseignements et aux biens aux personnes qui ont un besoin de connaître. Ceci permet de s'assurer qu'une personne a fait l'objet d'une enquête de sécurité appropriée fondée sur les renseignements et les biens auxquels elle doit avoir accès pour accomplir ses fonctions. Une gestion efficace de la sécurité du personnel permet aux IRSC :

- De s'assurer que les personnes qui ont accès à des renseignements/biens gouvernementaux et/ou ayant un accès privilégié aux systèmes essentiels sont fiables et dignes de confiance;
- De s'assurer de la loyauté de ces personnes envers le Canada afin de se protéger contre la collecte de renseignements par des puissances étrangères et le terrorisme;
- De prévenir l'activité malveillante et la communication non autorisée de renseignements protégés et/ou classifiés ou dommage effectué aux systèmes essentiels par une personne mal intentionnée qui occupe un poste de confiance.

[1] Politique sur la sécurité du gouvernement, Section 6.1.5

4. Définitions

Les définitions relatives aux termes utilisés dans la présente politique se trouvent à l'annexe A – Glossaire

5. Énoncé de la politique

5.1. OBJECTIF

La présente politique vise à s'assurer que les IRSC :

- fournissent au personnel qui a été jugé digne de confiance et loyal conformément à la Politique sur la sécurité du gouvernement du Canada l'accès approprié aux renseignements et aux biens du gouvernement du Canada.

5.2. RÉSULTATS ESCOMPTÉS

- Respecter la Politique sur la sécurité du gouvernement (PSG);
- Le personnel comprend ses responsabilités en ce qui a trait à la sécurité des biens et/ou renseignements du gouvernement;
- Les renseignements, les biens et les services ne sont pas compromis et les employés sont protégés contre la violence en milieu de travail;
- L'interopérabilité et l'échange de renseignements avec les sections de sécurité des autres ministères et agences du gouvernement du Canada;
- Les structures et les mécanismes sont en place pour assurer la gestion efficace et efficiente de la sécurité du personnel aux IRSC.

6. Exigences

Pour exécuter le programme et offrir un service efficacement, le Programme de la sécurité du personnel des IRSC doit :

- Déterminer le niveau de sécurité pour chaque poste. Pour ce faire, chaque profil de rôle doit décrire quel accès aux renseignements/biens protégés ou classifiés et/ou aux systèmes essentiels est requis pour effectuer les tâches de l'emploi. Pour les profils de rôle génériques, tout accès additionnel à des renseignements protégés ou classifiés requis pour effectuer les tâches de l'emploi doit être déterminé selon le niveau du poste. Voici des exemples de renseignements classifiés :
  - Documents du Cabinet, y compris les mémoires au Cabinet (Secret)
  - Soumissions du Secrétariat du Conseil du trésor (SCT) (Secret).
- S'assurer que tous les individus qui ont besoin d'un accès à des biens/renseignements protégés/classifiés et/ou d'un accès privilégié à des systèmes essentiels ont obtenu la cote de sécurité exigée avant le début d'une affectation, d'une nomination ou d'un détachement.
  - La cote de fiabilité est requise si l'accès à des renseignements protégés (A, B ou C) est une exigence pour accomplir les tâches du travail. La cote de fiabilité ou de sécurité est une condition d'emploi aux IRSC;
  - La cote de sécurité de niveau « secret » est requise si l'accès à des renseignements classifiés est une exigence pour accomplir les tâches du travail.

Ce niveau est aussi requis quand l'accès privilégié à des systèmes essentiels est nécessaire pour effectuer les tâches du travail.

7. Rôles et Responsabilités

7.1. PRÉSIDENT

Le président des IRSC est chargé de gérer efficacement les activités de sécurité au sein des IRSC et de contribuer à la gestion efficace de la sécurité à l'échelle du gouvernement. Le président est responsable de ce qui suit :

- S'assurer que les IRSC respectent la PSG et les autres instruments en matière de politiques et la législation connexes;
- Approuver le programme de sécurité des IRSC et mettre sur pied un programme de sécurité afin d'assurer la coordination et la gestion des activités globales, y compris la sécurité du personnel;
- Nommer un agent de sécurité ministériel pour gérer le programme de sécurité des IRSC;
- S'assurer que les gestionnaires de tous les niveaux intègrent les exigences en matière de sécurité du personnel aux plans, aux programmes, aux activités et aux services;
- Refuser ou révoquer une cote de sécurité pour un motif valable;
- S'assurer que les enjeux importants concernant la conformité à politique, les allégations d'inconduite, les activités criminelles soupçonnées, les incidents liés à la sécurité ou la violence en milieu de travail font l'objet d'une enquête, d'une intervention ou d'un signalement auprès des autorités compétentes.

7.2. AGENT DE SÉCURITÉ MINISTÉRIEL (ASM)

L'agent de sécurité ministériel (ASM) est responsable de la gestion du programme de sécurité des IRSC et a les responsabilités suivantes concernant la sécurité du personnel :

- Élaborer, mettre en œuvre, surveiller et actualiser un plan de sécurité de l'organisme qui intègre la sécurité du personnel;
- Assurer une approche coordonnée de tous les aspects de la sécurité des IRSC : sécurité du personnel, sécurité des contrats, sécurité des technologies et sécurité matérielle;
- Veiller à ce que les responsabilités, les délégations de pouvoir, les rapports hiérarchiques ainsi que les rôles et responsabilités des employés des IRSC à l'égard des responsabilités de sécurité soient définis, documentés et communiqués aux personnes concernées;
- Autoriser les exceptions aux nominations et aux postes sans la cote de sécurité appropriée;
- Conseiller le président ou lui présenter des recommandations dans les cas de refus ou d'annulation d'une cote de sécurité;
- Dans le cas d'un motif valable :
    - Refuser, révoquer ou suspendre une cote de fiabilité et en informer le gestionnaire ou le directeur scientifique;
    - Suspendre une cote de sécurité et en informer le gestionnaire ou le directeur scientifique.

7.3. AGENT DE SÉCURITÉ

L'agent de sécurité est chargé de coordonner toutes les fonctions qui sont liées aux aspects techniques et opérationnelles de la sécurité du personnel, à savoir :

- Maintenir un lien hiérarchique fonctionnel ou direct avec l'ASM afin d'assurer la coordination et l'intégration des activités de sécurité ministérielle.
- Sélectionner, mettre en œuvre et maintenir des contrôles de sécurité liés à la sécurité du personnel.
- Déterminer les exigences de sécurité de chaque poste en fonction du caractère délicat des renseignements, des biens auxquels le titulaire a accès ainsi que l'accès privilégié aux systèmes essentiels.
- Informer les gestionnaires et/ou les ressources humaines (RH) de l'état de l'évaluation de la sécurité.
- Traiter les demandes d'enquête de sécurité, notamment la vérification des noms, des dossiers criminels (empreintes digitales si requises), du crédit et des cotes de sécurité.
- Informer les RH par écrit des résultats de l'enquête de sécurité du candidat.
- S'assurer que les employés reçoivent une séance d'information et signent le formulaire « Certificat d'enquête de sécurité et profil de sécurité ».
- Maintenir à jour les dossiers de sécurité des employés.
- S'assurer que les cotes de fiabilité et de sécurité sont mises à jour avant leur expiration, conformément aux exigences de sécurité du poste. L'agent de sécurité mettra à jour :
  - la cote de fiabilité : tous les 10 ans
  - la cote de niveau secret : tous les 10 ans
  - la cote de niveau très secret : tous les 5 ans.
- Il mettra à jour la cote de sécurité ou de fiabilité dans les cas suivants :
  - notification d'infraction criminelle :
  - changement de situation (ex : mariage, conjoint de fait, etc.)
  - non-conformité aux exigences
  - réévaluation
  - octroi d'un pardon.

7.4. RESSOURCES HUMAINES

Les RH sont responsables de ce qui suit :

- Vérifier les renseignements suivants pour les nouveaux employés
  - renseignements personnels (c'est-à-dire date de naissance, adresse, etc.)
  - formation et titres professionnels
  - antécédents professionnels
  - références personnelles
- Lancer le processus de l'enquête de sécurité.
- S'assurer qu'aucun employé n'est embauché sans faire l'objet d'une enquête de sécurité ou obtenir le niveau de sécurité requis de la section de la sécurité.

7.5. DIRECTEURS SCIENTIFIQUES

Les directeurs scientifiques sont responsables de ce qui suit :

- Déterminer le caractère délicat des renseignements, des biens et des accès privilégiés pour chaque poste à l'externe doté d'un accès aux renseignements et/ou aux biens des IRSC.
- Vérifier les renseignements suivants pour les employés des instituts :
  - renseignements personnels (c'est-à-dire date de naissance, adresse, etc.)
  - formations et titres professionnels
  - antécédents professionnels
  - références personnelles
- S'assurer que le personnel externe des instituts détient le niveau de sécurité requis avant de commencer son emploi.

7.6. GESTIONNAIRES DES IRSC

Les gestionnaires sont chargés d'assurer un niveau approprié de sécurité pour leurs programmes et services. Dans la conception de programmes et de services, les gestionnaires travailleront avec les spécialistes de la sécurité du ministère afin de gérer efficacement les risques. Les gestionnaires seront soutenus et aidés par l'agent de sécurité pour remplir les responsabilités suivantes :

- Veiller à ce que les exigences en matière de sécurité soient intégrées à la planification des opérations, aux programmes, aux services et aux autres activités de gestion;
- S'assurer que les employés appliquent des pratiques de sécurité efficaces;
- Déterminer le caractère délicat des renseignements, des biens et l'accès privilégié aux systèmes essentiels pour chaque poste de leur unité et en informer la section de la sécurité des IRSC afin d'obtenir les exigences en matière de sécurité convenable au poste;
- S'assurer qu'aucun employé n'est embauché sans faire l'objet d'une enquête de sécurité ou obtenir le niveau de sécurité requis de la section de la sécurité;
- Préciser les exigences en matière de sécurité lorsque des contrats sont requis et s'assurer qu'aucun conseiller, entrepreneur ou aide temporaire n'est embauché sans faire l'objet d'une enquête de sécurité et sans avoir obtenu le niveau approprié, comme requis dans le contrat ou l'entente.

7.7. EMPLOYÉS

Les employés sont responsables de ce qui suit :

- Protéger les renseignements et les biens dont ils ont la responsabilité, qu'ils travaillent sur place ou non aux IRSC;
- Appliquer des mesures de contrôle de sécurité liées à leur domaine de responsabilité pour veiller à ce que les exigences en matière de sécurité fassent partie de l'exécution quotidienne des programmes, processus et pratiques;
- Signaler les incidents de sécurité en passant par les voies de communication appropriées;
- Informer l'ASM de toutes les situations pouvant influer sur leur cote de fiabilité ou de sécurité, telles que :
    - Arrestation ou condamnation
    - Faillite
    - Célibat/cohabitation/mariage/divorce
    - Si abordé par un criminel, un représentant d'un gouvernement étranger, un groupe d'intérêt marginal ou un ressortissant étranger qui désire obtenir des renseignements au sujet des IRSC ou des activités des IRSC, ce qui risquerait de mettre en péril l'intérêt national ou l'intégrité de l'organisme.

8. Conséquences

Le président est chargé d'enquêter et de répondre aux questions de non-respect de cette politique et de prendre des mesures correctives. Les conséquences du non-respect de cette politique peuvent inclure :

- De mauvaises évaluations de rendement pour les IRSC concernant l'article 19 du CRG (gestion efficace de la sécurité et la continuité des activités);
- Une vérification externe par le vérificateur général du Canada;
- Une enquête par le Commissariat à la protection de la vie privée du Canada.

9. Références

Les documents suivants sont pertinents par rapport à la présente politique :

- **Politique sur la sécurité du gouvernement**
- Politique sur la dotation
- Directive sur la gestion de l'identité
- Directive sur la gestion de la sécurité ministérielle
- Norme sur la sécurité du personnel
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)

10. Demandes de renseignements

Veuillez adresser toute demande de renseignements au sujet de la présente politique, à l'ASM, au conseiller principal de la sécurité ou à l'agent de sécurité du personnel des IRSC.

Programme de sécurité
Services de gestion de l'information, de la technologie et de l'administration (SGITA)
Instituts de recherche en santé du Canada
Ottawa (Ontario) K1A 0W9

Courriel : Security@cihr-irsc.gc.ca.
Téléphone : 613-954-7216/613-948-4636/613-954-1942
Télécopieur : 613-954-1800

Annexe A : Glossaire

Besoin de connaître : Besoin éprouvé par une personne d'accéder à des renseignements et de les connaître pour accomplir les tâches qui lui incombent**.**

Cote de fiabilité : Indique que l'évaluation de fiabilité a été achevée avec succès et donne à la personne visée un accès régulier aux biens gouvernementaux et un accès à des renseignements protégés en fonction du besoin de connaître.

Cote de sécurité : Indique que l'évaluation de sécurité a été achevée avec succès; avec un besoin de connaître, permet d'avoir accès à des renseignements classifiés. Il y a trois niveaux : confidentiel, secret et très secret.

Intérêt national : La sécurité du Canada ainsi que sa stabilité sociale, politique et économique.

Interopérabilité : Capacité des ministères du gouvernement fédéral de fonctionner en synergie au moyen de pratiques uniformes en matière de gestion de la sécurité et de l'identité.

Pour un motif raisonnable : Terme indiquant qu'il y a un motif raisonnable de revoir, suspendre, abaisser ou révoquer une cote de fiabilité ou de sécurité, ou un accès à des sites.

Programme de sécurité : Groupe d'intrants constitués de ressources et d'activités connexes qui est géré pour répondre à un ou des besoins précis et pour obtenir les résultats visés.

Renseignements classifiés : Renseignements d'intérêt national susceptibles d'être visés par une exclusion ou une exception en vertu de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels, et dont la divulgation sans autorisation risquerait vraisemblablement de porter préjudice à l'intérêt national.

Les niveaux de classification sont :

- **Confidentiel :** s'applique lorsqu'une atteinte à l'intégrité des renseignements risquerait vraisemblablement de porter préjudice à l'intérêt national;
- **Secret :** s'applique aux renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice sérieux à l'intérêt national;
- **Très secret** : s'applique à un nombre très restreint de renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice exceptionnellement grave à l'intérêt national.

Renseignements protégés : Des renseignements sont « protégés » si leur divulgation pourrait être préjudiciable à des intérêts autres que « l'intérêt national ».

Les trois niveaux sont les suivants :

- **Protégé A (renseignements de nature peu délicate) :** s'applique aux renseignements pour lesquels toute atteinte à l'intégrité des renseignements risquerait vraisemblablement de porter préjudice à des intérêts autres que l'intérêt national, p. ex. la divulgation du salaire exact.
- **Protégé B (renseignements de nature particulièrement délicate) :** s'applique aux renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de

causer un préjudice sérieux à des intérêts autres que l'intérêt national, p. ex. la perte de réputation ou d'avantage concurrentiel.

- **Protégé C (renseignements de nature extrêmement délicate) :** s'applique à un nombre très restreint de renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice extrêmement grave à des intérêts autres que l'intérêt national, p. ex. la perte de vie.

Ressortissant étranger : Personne autre qu'un citoyen canadien ou un résident permanent.

Service essentiel : Service dont la compromission, du point de vue de la disponibilité ou de l'intégrité, causerait un préjudice élevé à la santé, à la sûreté, à la sécurité ou au bien-être économique des Canadiens, ou encore au fonctionnement efficace du gouvernement du Canada.

Systèmes essentiels : Systèmes requis pour accomplir les services essentiels.