Institut canadien d'information sur la santé

Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité

Objectif

La présente *Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité* établit les exigences qui permettent à l'ICIS de détecter, d'évaluer, de prendre en charge et de surveiller les risques liés au respect de la vie privée et à la sécurité, ainsi que les rôles et responsabilités connexes.

Portée

Tous les membres du personnel de l'ICIS jouent un rôle dans la détection et la gestion des risques liés au respect de la vie privée et à la sécurité.

Définitions

Gestion des risques liés au respect de la vie privée et à la sécurité : processus officiel et reproductible visant la détection, l'évaluation, la prise en charge et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leur incidence possible.

Incidence : mesure de la gravité d'un risque.

Mesure d'atténuation : mesure à prendre pour réduire la probabilité d'un risque ou son incidence possible.

Plan de prise en charge du risque : processus défini et mise en œuvre d'options d'atténuation, de transfert, d'évitement ou d'acceptation du risque.

Prise en charge du risque : modification du risque par atténuation, transfert, évitement ou acceptation du risque.

Probabilité : mesure de la possibilité qu'un risque se matérialise.

Registre des risques liés au respect de la vie privée et à la sécurité : liste des risques liés au respect de la vie privée et à la sécurité qui ont été détectés.

Risque lié au respect de la vie privée et à la sécurité : possibilité qu'une situation se produise et

- entraîne le non-respect des lois et règlements en matière de vie privée ou des politiques et procédures de l'ICIS à l'égard du respect de la vie privée et de la sécurité de l'information;
- entraîne le défaut de protéger les renseignements personnels ou d'en prévenir la collecte, l'utilisation ou la divulgation non autorisée ou, de façon plus générale, la confidentialité, l'intégrité et la disponibilité des banques de données de l'ICIS;
- mette autrement en péril le statut de l'ICIS en vertu de la *Loi sur la protection des renseignements personnels sur la santé*, 2004 (LPRPS).

Toutes ces situations auraient une incidence négative sur l'atteinte des objectifs stratégiques de l'ICIS.

Politique

L'ICIS doit mettre sur pied un programme de gestion des risques liés au respect de la vie privée et à la sécurité et des processus connexes qui

- permettent la détection, l'évaluation, la prise en charge et la surveillance des risques liés au respect de la vie privée et à la sécurité;
- s'harmonisent au programme de gestion des risques de l'ICIS;
- permettent à l'ICIS de remplir ses obligations juridiques et les exigences réglementaires en ce qui a trait au respect de la vie privée et à la sécurité de l'information;
- contribuent à la culture de sensibilisation aux risques liés au respect de la vie privée et à la sécurité en place à l'ICIS.

Rôles et responsabilités

1. Le **Comité de la haute direction de l'ICIS** est responsable de la gestion des risques liés au respect de la vie privée et à la sécurité à l'ICIS et de ce qui suit :
    - surveiller et examiner les rapports d'étape trimestriels sur l'atténuation des risques;
    - recommander aux fins d'inclusion possible au registre des risques de l'ICIS tout risque lié au respect de la vie privée et à la sécurité qui répond à la définition du terme *risque* dans le programme de gestion des risques de l'ICIS;

- accepter les risques non pris en charge ou résiduels au nom de l'ICIS;
- examiner et régler les problèmes renvoyés à un échelon supérieur par le chef de la protection des renseignements personnels et le chef de la sécurité de l'information en ce qui a trait à la prise en charge des risques liés au respect de la vie privée et à la sécurité.

2. Le **comité chargé du respect de la vie privée, de la confidentialité et de la sécurité** est responsable de ce qui suit :
   - examiner et approuver régulièrement le registre des risques liés au respect de la vie privée et à la sécurité de l'ICIS tel que soumis par le chef de la protection des renseignements personnels et le chef de la sécurité de l'information.

3. Les **cadres supérieurs et les autres responsables désignés** sont responsables de la gestion des risques liés au respect de la vie privée et à la sécurité dans leur secteur et de ce qui suit :
   - collaborer avec le chef de la protection des renseignements personnels et le chef de la sécurité de l'information afin de déceler les risques liés au respect de la vie privée et à la sécurité qui sont déjà présents ou pourraient survenir dans leur secteur;
   - aider le chef de la protection des renseignements personnels et le chef de la sécurité de l'information à élaborer un plan de prise en charge des risques liés au respect de la vie privée et à la sécurité;
   - surveiller tous les risques liés au respect de la vie privée et à la sécurité applicables à leur secteur;
   - remettre chaque trimestre au chef de la protection des renseignements personnels et au chef de la sécurité de l'information un rapport sur l'état de l'ensemble des plans de prise en charge des risques dans leur secteur.

4. Le **chef de la protection des renseignements personnels et le chef de la sécurité de l'information** sont responsables des processus de gestion des risques liés au respect de la vie privée et à la sécurité de l'ICIS et de ce qui suit :
   - élaborer et mettre en œuvre une stratégie de gestion des risques liés au respect de la vie privée et à la sécurité, ce qui comprend, sans toutefois s'y limiter, la présente politique et un Cadre de gestion des risques liés au respect de la vie privée et à la sécurité qui s'harmonisent au programme de gestion des risques de l'ICIS et appuient le programme de gestion des risques du système de gestion de la sécurité de l'information (SGSI);

- collaborer avec la haute direction de l'ICIS afin de définir les risques liés au respect de la vie privée et à la sécurité à l'échelle de l'ICIS et recommander la prise en charge des risques conformément au programme de gestion des risques liés au respect de la vie privée et à la sécurité;
- évaluer les risques liés au respect de la vie privée et à la sécurité, conformément à la méthodologie de gestion des risques liés au respect de la vie privée et à la sécurité;
- tenir à jour le registre des risques liés au respect de la vie privée et à la sécurité, conformément au Cadre de gestion des risques liés au respect de la vie privée et à la sécurité;
- signaler aux cadres supérieurs ou aux autres responsables désignés tout risque lié au respect de la vie privée et à la sécurité applicable dans leur secteur;
- aider les cadres supérieurs ou les autres responsables désignés à élaborer un plan de prise en charge de leurs risques;
- surveiller tous les risques liés au respect de la vie privée et à la sécurité qui figurent dans le registre, ce qui inclut de procéder à un examen annuel des évaluations et des plans de prise en charge des risques;
- recommander aux fins d'inclusion possible au registre des risques de l'ICIS tout risque lié au respect de la vie privée et à la sécurité qui répond à la définition du terme *risque* dans le programme de gestion des risques de l'ICIS;
- fournir des rapports d'étape trimestriels sur l'atténuation des risques au Comité de la haute direction;
- examiner chaque année la présente politique et le Cadre de gestion des risques liés au respect de la vie privée et à la sécurité.

Politiques, procédures et documents connexes

Cadre de gestion des risques liés au respect de la vie privée et à la sécurité

Pour de plus amples renseignements

securite@icis.ca

vieprivee@icis.ca

Historique des révisions :

Date A/M/J	Version	Description des révisions	Responsable de l'approbation
2015-07-16	1.0	Document original	Comité de la haute direction
2017-03-09	1.1	Mise à jour administrative	s.o.

s.o. : sans objet