RÉGIME DE RETRAITE DES EMPLOYÉ(E)S DU SCFP

POLITIQUE DE GESTION DES RISQUES INFORMATIQUES

1. BUT

Le Conseil de fiducie mixte du Régime de retraite des employé(e)s du SCFP (le « CFM ») a adopté la présente Politique de gestion des risques informatiques (la « Politique ») dans le but de documenter certaines de ses pratiques de gestion des risques informatiques, notamment celles qui ont trait à l'examen des incidents relatifs à la gestion des risques liés aux technologies de l'information, et à leur réponse, qui peuvent avoir une incidence sur le CFM, le Régime de retraite des employé(e)s du SCFP (le « RRES ») ou tout prestataire du RRES.

2. DÉFINITIONS

Dans la présente Politique, les mots et expressions ci-dessous ont le sens suivant :

Par « **TI** », on entend les technologies de l'information.

Par « **RISQUES LIÉS AUX TI** », on entend les risques de perte financière, de perturbation ou de dommage opérationnel, ou de perte de réputation résultant de l'inadéquation, de la perturbation, de la destruction, de la défaillance ou de l'endommagement, par quelque moyen que ce soit, des systèmes, de l'infrastructure et des données. À des fins de clarté et malgré la généralité de ce qui précède, les risques liés aux TI du CFM :

(a) englobent, mais sans s'y limiter, les cyber risques;

(b) comprennent tout risque lié à l'utilisation de l'informatique;

(c) peuvent être externes ou internes au CFM.

Par « **incident important découlant de risques liés aux TI** », on entend tout incident découlant de risques liés aux TI dont le CFM détermine qu'il est important. Le CFM évaluera, et déterminera, si un incident découlant de risques liés aux TI constitue un incident important découlant de risques liés aux TI conformément à la présente Politique et en rapport avec toute exigence juridique et ligne directrice réglementaire.

Par « **renseignements personnels** », on entend tout renseignement sur un individu identifiable qui est de nature privée et qui n'est pas facilement accessible au public.

Par « **atteinte à la confidentialité de renseignements personnels** », on entend tout accès non autorisé, ou divulgation non autorisée, de renseignements personnels résultant de l'inadéquation, de la perturbation, de la destruction, de la défaillance ou de l'endommagement, par quelque moyen que ce soit, des systèmes, de l'infrastructure et des données.

3. LIGNE DIRECTRICE POUR LA GESTION DES RISQUES INFORMATIQUES

Les pratiques du CFM pour la gestion des risques liés aux TI sont conformes à la Ligne directrice pour la gestion des risques liés aux TI (la « Ligne directrice »), en vigueur depuis le 1er avril 2024 et publiée par l'Autorité ontarienne de réglementation des services financiers (« ASRF »). Les pratiques du CFM pour la gestion des risques liés aux TI comprennent la conformité continue aux exigences prévues par la loi et la protection des renseignements personnels, dont la *Loi sur la protection des renseignements personnels et les documents électroniques* (« *LPRPDE* »). Ces pratiques englobent aussi celles qui sont acceptées par l'industrie pour la gestion efficace des risques liés aux TI établies dans la Ligne directrice comme suit :

a) Gouvernance – Le CFM dispose d'une gouvernance et d'une surveillance de ses risques liés aux TI conformes aux pratiques acceptées par l'industrie des régimes de retraite.

b) Gestion des risques – Le CFM s'appuie sur des pratiques acceptées par l'industrie des régimes de retraite pour gérer efficacement ses risques liés aux TI.

c) Gestion des données – Le CFM utilise des stratégies acceptées par l'industrie des régimes de retraite pour gérer et sécuriser efficacement les données confidentielles.

d) Externalisation – Le CFM gère efficacement les risques liés aux TI associés à toute activité, fonction ou service externalisé ou co-sourcé.

e) Préparation aux incidents – Le CFM est prêt à détecter, enregistrer, gérer, résoudre, récupérer, surveiller et signaler les incidents informatiques efficacement et en temps opportun.

f) Continuité et résilience – Le CFM est prêt à assurer la continuité de ses actifs informatiques et sa capacité à fournir des services essentiels pendant et après un incident.

g) Avis en cas d'incidents importants découlant de risques liés aux technologies de l'information – Le CFM est prêt à aviser l'ARSF en cas d'indicent important découlant de risques liés aux TI.

Le CFM a recours à des tiers pour effectuer certaines activités, fonctions et services. Le CFM s'attend à ce que chaque tiers auquel il fait appel suive les pratiques acceptées par l'industrie des régimes de retraite pour la gestion efficace des risques liés aux TI. En outre, le CFM s'attend à ce que chaque tiers auquel il fait appel avise immédiatement le CFM en cas d'incident découlant de risques liés aux TI qui entraîne des répercussions sur ses opérations et qui peut entraîner des répercussions sur le CFM, le RRES ou tout prestataire du RRES. Le CFM visera à inclure la question des risques liés aux TI et la Ligne directrice dans les ententes contractuelles relatives aux activités, fonctions et services externalisés.

Tout incident découlant de risques liés aux TI qui peut entraîner des répercussions sur le CFM ou le RRES, incluant tout prestataire du RRES, sera traité conformément à la procédure de préparation et de réponse aux incidents à la Section 4 ci-dessous.

4. PROCÉDURE DE PRÉPARATION ET DE RÉPONSE AUX INCIDENTS

(a) Identification et signalement interne

Le CFM s'attend à ce que tous les incidents découlant de risques liés aux TI qui pourraient entraîner des répercussions sur le CFM ou le RRES, incluant tout prestataire du RRES, soient immédiatement signalés au CFM. Cette attente s'applique à chaque membre du CFM et à chaque tiers dont les services ont été retenus par le CFM. Le CFM avisera chaque tiers auquel il aura fait appel de cette attente.

(b) Évaluation par le CFM d'un incident découlant de risques liés aux TI

Si le CFM est informé d'un incident découlant de risques liés aux TI qui pourrait entraîner des répercussions sur le CFM ou le RRES, incluant tout prestataire du RRES, il répondra aux questions suivantes :

(i) L'incident découlant de risques liés aux TI est-il un incident important découlant de risques liés aux TI?
(ii) L'incident découlant de risques liés aux TI constitue-t-il une atteinte à la confidentialité de renseignements personnels?

De plus, si le CFM détermine que l'incident découlant de risques liés aux TI constitue une atteinte à la confidentialité de renseignements personnels, il évaluera, et déterminera, s'il est raisonnable ou non de croire, dans les circonstances, que l'atteinte à la confidentialité des renseignements personnels crée un risque réel de préjudice important aux personnes dont les renseignements personnels ont fait l'objet d'une atteinte à la confidentialité de renseignements personnels.

(i) L'incident découlant de risques liés aux TI constitue-t-il un incident important découlant de risques liés aux TI?

Le CFM évaluera et déterminera si l'incident découlant de risques liés aux TI constitue un incident important découlant de risques liés aux TI en fonction des répercussions de l'incident découlant de risques liés aux TI sur les opérations du CFM ou du RRES, ainsi que sur les prestataires du RRES. Pour évaluer et déterminer si un incident découlant de risques liés aux TI constitue un incident important découlant de risques liés aux TI, le CFM tiendra compte de facteurs pertinents et pourra consulter un conseiller juridique, des experts en systèmes et en sécurité informatiques et d'autres conseillers.

Les indicateurs qu'un l'incident important découlant de risques liés aux TI s'est produit incluent notamment le fait qu'un incident découlant de risques liés aux TI :

- entraîne une perturbation des opérations du CFM ou du RRES au point où le RRES ne peut plus être efficacement administré;

- aura probablement des répercussions négatives sur d'autres entités ou individus réglementés par l'ARSF ou est susceptible de se reproduire avec d'autres entités ou individus réglementés par l'ARSF;

- compromet la confidentialité des données des participants du RRES, incluant les renseignements personnels;

- a des répercussions sur la capacité du CFM ou du RRES à verser des prestations.

(ii) L'incident découlant de risques liés aux TI constitue-t-il une atteinte à la confidentialité des renseignements personnels?

Le CFM évaluera et déterminera si l'incident découlant de risques liés aux TI constitue une atteinte à la confidentialité des renseignements personnels. Si le CFM détermine que l'incident découlant de risques liés aux TI constitue une atteinte à la confidentialité des renseignements personnels, il étudiera la question posée au point (iii) ci-dessous.

(iii) L'atteinte à la confidentialité des renseignements personnels crée-t-elle un risque réel de préjudice important?

Le CFM déterminera s'il est raisonnable de croire, dans les circonstances, que l'atteinte à la confidentialité des renseignements personnels crée un risque réel de préjudice important pour les individus dont les renseignements personnels ont fait l'objet d'une atteinte à la confidentialité. Pour faire cette détermination, le CFM peut consulter un conseiller juridique, des experts en systèmes et en sécurité informatique et d'autres conseillers.

Conformément à la *LPRPDE*, les facteurs qui sont pertinents pour déterminer si une atteinte à la confidentialité des renseignements crée un risque réel de préjudice important pour les individus dont les renseignements personnels ont fait l'objet d'une atteinte à la confidentialité comprennent la sensibilité des renseignements personnels en question et la probabilité que les renseignements personnels ont été, sont ou seront utilisés à mauvais escient.

(c) Confinement

Le CFM prendra des mesures raisonnables et adéquates pour déterminer l'ampleur de tout incident découlant de risques liés aux TI, y compris les atteintes à la confidentialité des renseignements personnels et les incidents importants découlant de risques liés aux TI, et prendra des mesures raisonnables et adéquates pour les confiner. Ces mesures peuvent notamment inclure les suivantes :

- mesures pour mettre fin à tout accès non autorisé;
- collaboration avec des experts en systèmes et en sécurité informatiques, des conseillers juridiques et d'autres conseillers;
- documentation de la nature de l'incident découlant de risques liés aux TI;
- documentation des activités nécessaires pour confiner l'incident découlant de risques liés aux TI;

- mesures visant à ne compromettre aucune capacité à enquêter et à ne détruire aucune preuve pouvant aider à déterminer la cause de l'incident découlant de risques liés aux TI.

(d) Avis externe – Incident important découlant de risques liés aux TI

Si le CFM conclut qu'un incident découlant de risques liés aux TI est un incident important découlant de risques liés aux TI, il en avisera l'ARSF dès que possible après avoir déterminé que l'incident découlant de risques liés aux TI est un incident important découlant de risques liés aux TI. Conformément à la Ligne directrice, cet avis sera normalement fourni à l'ARSF dans les 72 heures, ou avant, de la conclusion par le CFM qu'un incident important découlant de risques liés aux TI s'est produit. Cet avis sera fourni en faisant parvenir à l'ARSF par courriel le Formulaire d'avis d'incident découlant de risques liés aux TI à l'adresse courriel applicable fournie par l'ARSF, ou par toute autre méthode de notification acceptable pour l'ARSF. Le CFM répondra aux demandes de suivi, s'il y a lieu, de l'ARSF au sujet de l'incident découlant de risques liés aux TI.

Le CFM songera à aviser tout assureur concerné de l'incident découlant de risques liés aux TI. Pour l'aider à décider s'il faut ou non aviser un assureur concerné de l'incident découlant de risques liés aux TI, le CFM peut consulter un conseiller juridique, des experts en systèmes et en sécurité informatiques et d'autres conseillers.

(e) Avis externe – Atteinte à la confidentialité des renseignements personnels

S'il conclut qu'il est raisonnable de croire qu'une atteinte à la confidentialité des renseignements personnels crée un risque réel de préjudice important pour les individus dont les renseignements personnels ont fait l'objet d'une atteinte, le CFM rendra compte de l'atteinte à la confidentialité des renseignements personnels au Commissariat à la protection de la vie privée et, à moins que la loi l'interdise, aux individus concernés. Chacun de ces rapports sera fourni conformément à la *LPRPDE*. Le CFM évaluera aussi si l'un ou l'autre des tiers devrait être informé de l'atteinte à la confidentialité des renseignements personnels. Si le CFM détermine que ces tiers devraient être informés de l'atteinte à la confidentialité des renseignements personnels, il les en avisera. Pour l'aider à évaluer si un tiers devrait être informé de l'atteinte à la confidentialité des renseignements personnels, le CFM peut consulter un conseiller juridique, des experts en systèmes et en sécurité informatiques et d'autres conseillers.

Le CFM répondra aux demandes de suivi, s'il y a lieu, au sujet de l'atteinte à la confidentialité des renseignements personnels.

(f) Enquête

Pour déterminer si d'autres mesures sont nécessaires pour répondre à l'incident découlant de risques liés aux TI, y compris une atteinte à la confidentialité des renseignements personnels et à un incident important découlant de risques liés aux TI, le CFM fera enquête sur l'incident découlant de risques liés aux TI. Le CFM fera enquête sur les circonstances et les répercussions de l'incident découlant de risques liés aux TI. Pour l'aider dans son enquête, le CFM peut retenir les services d'un conseiller juridique, d'experts en systèmes et sécurité informatiques et d'autres conseillers.

(g) Prévention

Après avoir fait enquête sur un incident découlant de risques liés aux TI, le CFM examinera et évaluera les moyens à prendre pour prévenir de futurs incidents potentiels découlant de risques liés aux TI. Pour l'aider dans son examen et son évaluation, le CFM peut consulter un conseiller juridique, des experts en systèmes et en sécurité informatiques et d'autres conseillers. Le CFM mettra en œuvre les mesures qu'il jugera adéquates pour prévenir un futur incident découlant de risques liés aux TI.

(h) Tenue de dossiers

Des dossiers doivent être tenus sur tous les incidents découlant de risques liés aux TI signalés au CFM, incluant ceux qui constituent des incidents importants découlant de risques liés aux TI et des atteintes à la confidentialité des renseignements personnels. Ces dossiers doivent comprendre la date de l'incident, une description de l'incident (y compris, s'il y a lieu, la nature de l'information touchée par l'incident) et si l'indicent a été signalé à l'ARSF, au Commissariat à la protection de la vie privée ou à tout individu concerné. Ces dossiers seront conservés pendant au moins cinq ans, selon la détermination du CFM.

:cp/sepb 491
5 décembre 2024