CAHIER DE GESTION

POLITIQUE DE LA SÉCURITÉ DE L'INFORMATION ET DE LA GESTION ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Entrée en vigueur : 22 septembre 2022
Approbation par le conseil d'administration : 30 septembre 2022

Dans ce document, l'utilisation du masculin pour désigner des personnes a comme seul but d'alléger le texte et identifie sans discrimination les individus des deux sexes.

POLITIQUE DE SÉCURITÉ DE L'INFORMATION
ET DE LA GESTION ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

NOTE : Après consultation auprès de Me Julien Sirois du cabinet Montmorency, il appert que selon le libellé de ses articles 2 à 5, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ c. G-1.03) ne s'applique pas à la SOFAD et qu'il en est de même pour la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ c. A-2.1). La SOFAD n'est qualifiée d' « organisme public » que dans le cadre de l'application de la LCOP.

En ce sens, la SOFAD est assujettie à *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ c P-39). Cela étant, il est loisible à la SOFAD de s'imposer des règles de gouvernance qui s'inspirent du cadre légal applicable aux organismes publics, et ce, d'autant plus que la SOFAD est entièrement composée d'administrateurs qui proviennent du secteur public. C'est l'orientation retenue pour l'élaboration de la présente politique.

PRÉAMBULE

Cette politique répond aux exigences qui s'appliquent à la SOFAD telles qu'énoncées dans :

- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03, a. 20)
- La Loi modernisant des dispositions législatives en matière de protection des renseignements personnel.

La nature des activités de la SOFAD l'amène à utiliser des systèmes informatisés pour la totalité de ses opérations éditoriales, administratives et communicationnelles. Les données opérationnelles, les fichiers avec lesquels la SOFAD diffuse ses ressources et les renseignements personnels sont tous hébergés dans l'infonuagique. Plusieurs ressources externes associées à des projets éditoriaux peuvent accéder à des fichiers de travail hébergés dans l'infonuagique. La SOFAD a la responsabilité de protéger ses systèmes informatisés et d'assurer leur utilisation sécuritaire par les membres de son personnel et les ressources externes autorisées.

La réalisation de sa mission amène la SOFAD à collecter, utiliser, conserver, communiquer et détruire des renseignements personnels concernant, de manière non-exhaustive, ses utilisateurs, ses clients, ses fournisseurs ainsi que les membres de son personnel et de conseil d'administration. Ces renseignements personnels sont confidentiels, à l'exception de ceux qui ont un caractère public aux sens de la Loi. La SOFAD a la responsabilité d'en préserver la confidentialité et de se conformer aux obligations prévues par la Loi, dont notamment l'obtention du consentement des personnes qu'ils concernent avant de les communiquer à des tierces personnes.

Cette politique vise à mettre des mesures concrètes à ces fins. Elle doit être lue et interprétée en tenant compte des politiques internes suivantes :

- Politique de gouvernance numérique (sera actualisée – novembre 2022)
- Politique d'utilisation des actifs informatiques (sera actualisée – novembre 2022)
- Politique d'utilisation des médias sociaux (sera actualisée – novembre 2022)
- Politique d'utilisation des courriels (sera actualisée – novembre 2022)
- Politique de gestion des dossiers personnels (sera actualisée – novembre 2022)
- Plan des 15 mesures minimales de sécurité informatique
- Plan de gestion et de conservation des documents (sera actualisée – novembre 2022)

A. GÉNÉRALITÉS

1. OBJECTIFS

Cette politique met en place un cadre de gestion de la sécurité de l'information pour l'ensemble des actifs informatiques de la SOFAD.

De plus, elle encadre la collecte, l'utilisation, la conservation et la destruction des renseignements personnels concernant la communauté de la SOFAD composée, de manière non-exhaustive, de ses utilisateurs, de ses clients, des membres de son personnel, de ses stagiaires et des membres de son conseil d'administration.

2. DÉFINITIONS

- Centre opérationnel de cyberdéfense (COCD) : unité administrative du ministère de l'Éducation spécialisée en sécurité, auprès de qui la SOFAD peut demander appui et conseil
- Cycle de vie de l'information : ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation.
- Événement de sécurité : toute forme d'atteinte, présente ou appréhendée, telle une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle
- Document : une information détenue sur un support matériel, quelle que soit sa forme : écrite, graphique, sonore, visuelle, informatisée ou autre.
- Loi : Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03)
- Membres du personnel : personne salariée au service de la SOFAD, incluant les responsables, les chefs d'équipe, les coordonnateurs et les directeurs.
- Membre du conseil d'administration : personne ayant été élue ou désignée et assumant une fonction du conseil d'administration.
- Renseignement personnel : tout renseignement qui concerne une personne physique et qui permet de l'identifier. Le nom d'une personne n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement concernant cette personne. Le fait qu'une signature apparaisse au bas d'un document n'a pas pour effet de rendre personnels les renseignements qui y apparaissent.

3. CHAMP D'APPLICATION

En matière de gestion et de protection des renseignements personnels, la SOFAD entend respecter la Loi, le Code civil du Québec et la Charte des droits et libertés de la personne du Québec ainsi que toute autre loi applicable.

4. RESPONSABLE DE L'APPLICATION

Du fait qu'elle assume aussi la fonction de secrétaire de la SOFAD, la direction générale est responsable de l'application de cette politique.

La direction générale met en place et dirige un comité de sécurité de l'information composé du chef d'équipe - technologies éducatives, de la cheffe d'équipe – intégration et d'un analyste-programmeur responsable de la cybersécurité à l'application de cette politique et à la mise en place de pratiques et de solutions permettant la prise en charge globale de la sécurité de l'information au sein de la SOFAD. Ce comité peut s'assurer des services d'une ressource externe experte pour jouer le rôle de chef de la sécurité de l'information organisationnelle (CSIO).

La direction générale assure la liaison avec les agences publiques ou les ministères responsables de la sécurité de l'information. Il peut déléguer ou associer le chef d'équipe – technologies éducatives, la cheffe d'équipe – intégration ou l'analyste-programmeur responsable de la cybersécurité à ces communications.

B. SÉCURITÉ DE L'INFORMATION

5. PRINCIPES DIRECTEURS DE LA SÉCURITÉ DE L'INFORMATION

La SOFAD doit assurer la sécurité des ressources informationnelles et de l'information qu'elle détient ou utilise conformément aux cinq (5) principes directeurs suivants :

a) Éthique : La SOFAD met en place un processus de gestion de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle
b) Évolution : La SOFAD réévalue et actualise périodiquement ses pratiques et ses solutions en matière de sécurité de l'information afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des risques de sécurité de l'information afférents.
c) Responsabilité et imputabilité : La SOFAD attribue clairement des responsabilités à tous les niveaux de l'organisation et met en place des processus de gestion de la sécurité de l'information permettant une reddition de compte adéquate.
d) Transparence : La SOFAD communique de manière fluide auprès des agences gouvernementales concernées à propos d'événements de sécurité, de ses pratiques et de ses solutions de sécurité de l'information.
e) Universalité : La SOFAD retient des pratiques et des solutions en matière de sécurité de l'information qui correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale ou internationale.

6. OBLIGATIONS EN SÉCURITÉ DE L'INFORMATION

La SOFAD :

a) Adopte et met en œuvre une politique et un cadre de gestion de la sécurité de l'information, les maintenir à jour et en assurer leur application
b) Met en place les comités et les groupes de travail appropriés de coordination et de concertation en matière de sécurité de l'information
c) Assure la gestion de la sécurité de l'information, déployer les mesures y afférentes et assurer le suivi de leur mise en œuvre
d) Applique les indications d'application formulées par le chef gouvernemental ou par le chef délégué de la sécurité de l'information
e) Élabore et met en œuvre pour les membres du personnel et les cadres un programme formel et continu de formation et de sensibilisation en matière de sécurité de l'information
f) Respecte, lorsqu'elle utilise un service commun, les exigences de sécurité de l'information qui la concernent
g) Rend compte au chef délégué de la sécurité de l'information du respect de ses obligations en matière de sécurité de l'information et répond aux demandes qui lui sont formulées

7. GESTION DES RISQUES ET DES VULNÉRABILITÉS EN SÉCURITÉ DE L'INFORMATION

La SOFAD met en place un processus de gestion des risques basé sur l'amélioration continue permettant l'identification, l'analyse et le traitement des risques de sécurité de l'information. Sur une base récurrente, une analyse de risques est effectuée pour chaque domaine d'activité visé par la présente Politique afin d'identifier les risques pouvant affecter leur fonctionnement efficace. Ce processus est réalisé par les membres de l'équipe concernés par ces questions avec la collaboration du CSIO externe.

8. GESTION DE LA REPRISE ET DE LA CONTINUITÉ DES AFFAIRES

La SOFAD met en place un plan de reprise et de continuité des affaires en cas d'événement informatique. Elle choisit ses applications, ses infrastructures et ses ressources externes en considérant l'adéquation des solutions proposées pour assurer une reprise et une continuité des affaires dans des délais raisonnables. Elle valide et teste régulièrement le fonctionnement des processus de reprise et de continuité des affaires.

9. GESTION DES RESSOURCES EXTERNES

La SOFAD met en place des mesures de gestion des ressources externes qui rend obligatoire le respect de mesures de sécurité de l'information. Ces mesures sont incluses dans les ententes de services convenues avec les ressources externes.

10. ÉVÉNEMENTS DE SÉCURITÉ

10.1 Comité de gestion d'événements de sécurité

La direction générale met sur pied un comité de gestion d'événements de sécurité, qui se compose des personnes suivantes :

- Direction générale
- Chef d'équipe – technologies éducatives
- Chef d'équipe – intégration
- Analyste programmeur responsable de la cybersécurité
- Responsable du développement des affaires
- Chef d'équipe – marketing et promotion

Ce comité a pour responsabilité d'identifier et d'analyser les causes d'un événement de sécurité, d'autoriser la mise en place des solutions appropriées, de faire le suivi auprès des clients potentiellement affectés et d'assurer la liaison avec les instances suivantes :

- Responsable de la gouvernance numérique désigné par le conseil d'administration de la SOFAD
- Centre opérationnel de cyberdéfense du ministère de l'Éducation (COCD)
- Commission d'accès à l'information (CAI)
- Médias si l'événement devenait d'intérêt public

Ce comité peut demander un appui à des ressources expertes, dont :

- Le CSIO
- Le fournisseur de solutions infonuagiques
- Le fournisseur de services gérés
- Un spécialiste des relations avec les médias

Un rapport est déposé à la séance suivante du conseil d'administration.

10.2 Tenue d'un registre des événements de sécurité

La SOFAD tient à jour un registre des événements de sécurité. Ce registre doit notamment comprendre :

a) Coordonnées des personnes associées à la gestion des événements de sécurité : direction générale, chef d'équipe – technologies éducatives, chef d'équipe – intégration, analyste-programmeur responsable de la cybersécurité
b) Date et heure de l'événement
c) Localisation de l'événement (adresse)
d) Nature de l'événement
e) Description de l'événement
f) Les préjudices engendrés et les personnes morales ou physiques concernées

g) Les actions prises
h) L'acceptation ou non du risque résiduel et les justificatifs afférents
i) Les actions prévues
j) La date de clôture de l'événement

Sur demande et dans le délai prescrit, la SOFAD transmet au chef gouvernemental de la sécurité de l'information une copie de ce registre.

10.3 Survenance d'un événement de sécurité à risque de préjudice sérieux

Si un événement de sécurité présente un risque qu'un préjudice sérieux soit causé, la SOFAD doit aviser sans délai le COCD.

C. GESTION ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

11. GESTION ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

11.1 Caractère confidentiel des renseignements personnels

À l'exception des cas prévus à l'article 5.2, les renseignements personnels détenus par la SOFAD sont confidentiels et soumis aux règles de protection prévus par la Loi. Ils ne sont accessible s qu'aux personnes qu'ils concernent et, au sein de la SOFAD, qu'aux seules personnes qui ont la qualité pour les recevoir lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

Lorsque la personne concernée par un renseignement personnel a donné son consentement à sa divulgation, un renseignement personnel cesse d'être confidentiel. Le cas échéant, ce consentement doit être donné expressément, de façon libre et éclairée et être spécifique et limité.

12. COLLECTE, CONSERVATION, UTILISATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

La SOFAD prend les mesures de sécurité propres à assurer la protection des renseignements personnelles qu'elle collecte, utilise, communique, conserve ou détruit et ce, en fonction, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

12.1 Collecte des renseignements personnels

La SOFAD ne recueille que les renseignements personnels qui sont nécessaires à la réalisation de ses mandats.

12.2 Conservation des renseignements personnels

La SOFAD s'assure que les renseignements personnels qu'elle détient sont complets, à jour et exacts pour servir aux fins pour lesquelles elle les recueille ou les utilise.

L'accès aux renseignements personnels détenus par la SOFAD n'est autorisé, en tout ou en partie, qu'aux membres du personnel pour qui cela est nécessaire aux fins de l'exercice de leurs fonctions.

12.3 Utilisation des renseignements personnels

La SOFAD n'utilise les renseignements personnels qu'elle détient qu'aux fins pour lesquelles elle les a recueillis, sauf dans l'une ou l'autre des situations suivantes :

a) Elle a préalablement obtenu le consentement de la personne concernée
b) L'utilisation est faite à des fins compatibles avec celles pour lesquelles le renseignement personnel a été recueilli
c) L'utilisation est faite manifestement au bénéfice de la personne concernée
d) L'utilisation est nécessaire à l'application d'une loi au Québec

Les membres du personnel et les cadres de la SOFAD qui utilisent des renseignements personnels dans le cadre de l'exercice de leurs fonctions doivent :

a) Limiter leur utilisation aux fins de l'exercice de leurs fonctions
b) S'assurer d'en préserver la confidentialité en toutes circonstances
c) Informer sans délai leur supérieur immédiat ou la direction générale de toute situation où la confidentialité de renseignements personnels pourrait avoir été compromise
d) Ne conserver, au terme de leur lien d'emploi avec la SOFAD, aucun renseignement personnel porté à leur connaissance dans le cadre de l'exercice de leurs fonctions et continuer d'en préserver la confidentialité.

12.4 Destruction des renseignements personnels

La SOFAD détruit de façon sécuritaire les renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis sont accomplis, sous réserve des lois applicables quant à leur conservation.

13. COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

La SOFAD ne peut communiquer un renseignement personnel confidentiel à une tierce personne sans le consentement de la personne concernée sauf dans les circonstances suivantes :

13.1 À une personne

a) Qui est autorisée par la Commission d'accès à l'information, à des fins d'étude, de recherche ou de statistiques.
b) À qui il est nécessaire de le faire afin de recueillir des renseignements personnels déjà colligés par celle-ci, en informant préalablement la Commission d'accès à l'information.

13.2 À toute personne ou organisme si la communication des renseignements personnels est nécessaire pour :

a) L'application d'une loi au Québec, que cette communication soit ou non prévue par la loi.
b) Prévenir, détecter ou réprimer le crime ou les infractions aux lois.
c) L'application d'une convention collective, d'un décret, d'un arrêté, d'une directive ou d'un règlement qui établissent des conditions de travail.
d) L'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise confié par la SOFAD. Le cas échéant, le contrat concerné doit être conclu par écrit et contenu doit être conforme à la Loi.

13.3 À un organisme public ou à un organisme d'un autre gouvernement, en concluant et soumettant préalablement à la Commission d'accès à l'information une entente écrite conforme à la Loi, lorsque cette communication est nécessaire :

a) Pour l'exercice de ses attributions par l'organisme receveur.
b) Est manifestement au bénéfice de la personne concerné.
c) Dans le cadre de la prestation d'un service à la personne concernée par un organisme public.
d) Lorsque des circonstances exceptionnelles le justifient.

La SOFAD doit communiquer certains renseignements personnels en temps opportun dans les circonstances suivantes :

a) À toute personne susceptible de porter secours à une personne exposée à une situation d'urgence ou à un danger imminent de mort ou de blessures graves pouvant être

provoquée(s) par un acte de violence, dont un suicide, s'il existe un motif raisonnable de croire qu'un tel danger la menace et que cela est nécessaire pour le prévenir. Le cas échéant, seuls les renseignements personnels nécessaires aux fins poursuivies par leur communication doivent être communiqués.

b) Aux autorisé policières lorsqu'il existe un motif raisonnable de croire qu'une personne est en possession d'une arme à feu sur les terrains ou dans les locaux de la SOFAD, qu'une personne a un comportement susceptible de compromettre sa sécurité ou celle d'autrui avec une arme à feu. Le cas échéant, la SOFAD communique aux autorités policières que les renseignements personnels nécessaires pour faciliter la tâche des policiers.

13.4 Registre de communications de renseignements personnels

La SOFAD tient un registre de tous les renseignements personnels qu'elle communique dans les cas par la Loi sans le consentement des personnes concernés.

Tout membre de la communauté de la SOFAD qui communique un renseignement personnel dans de telles circonstances doit en informer la direction générale et lui spécifier :

a) La nature ou le type de renseignement personnel communiqué.
b) La personne ou l'organisme qui reçoit cette communication.
c) La fin pour laquelle ce renseignement est communiqué.
d) La raison justifiant cette communication.

Toute personne qui en fait la demande peut accéder au registre tenu par la SOFAD, dans les limites et aux conditions prévues par la Loi.

14. DROITS DE LA PERSONNE CONCERNÉE PAR UN RENSEIGNEMENT PERSONNEL

14.1 Accès

Les personnes concernées par les renseignements personnels détenus par la SOFAD ont le droit d'être informées de l'existence de renseignements personnels les concernant et d'en recevoir communication, dans les limites et aux conditions prévues par la Loi.

14.2 Rectification

La personne concernée par un renseignement personnel inexact, incomplet ou équivoque ou dont la collecte, la communication ou la conservation ne sont pas autorisées par la Loi, peut exiger la rectification du fichier, dans les limites et aux conditions prévues par la Loi.

14.3 Transmission d'une demande d'accès ou de rectification

Toute demande en ce sens doit être transmise par courriel à la direction générale.

14.4 Réponse écrite en cas d'un refus

Dans le cas où la SOFAD ne sera pas en mesure d'autoriser l'accès d'un particulier à ses renseignements personnels, la direction générale fournira par écrit les raisons qui motivent ce refus.