Québec
Santé Québec

PAR COURRIEL

Québec, le 27 février 2026

[redacted]

Objet : Réponse - Demande d'accès à des documents

Madame,

Nous donnons suite à votre demande d'accès reçue le 30 janvier 2026 visant l'obtention des documents suivants :

- *Document ou fiche de breffage concernant l'utilisation des sites pornographiques par les employés de votre organisation, en particulier les hauts fonctionnaires, pour la période du 1er janvier 2023 à aujourd'hui;*
- *[…] les dépenses annuelles totales en papiers-mouchoirs pour cette même période.*

Le 5 février 2026, vous nous avez transmis les précisions suivantes au sujet du premier point de votre demande:

[…] Voici le type de documents recherchés :

- *Politique-cadre concernant l'accès à du matériel pornographique pour les employés de Santé Québec;*
- *Politique ministérielle d'utilisation des services Internet;*
- *Procédures d'enquête pour les employés ayant visionné de la pornographie;*
- *Résultats d'enquête interne et dossiers dénominalisés d'employés ayant reçu des sanctions disciplinaires ou des avertissements pour avoir accédé à de la pornographie sur le réseau de Santé Québec, ce qui inclut de la pédopornographie.*

En ce qui concerne le premier point de votre demande, vous trouverez ci-joint un document pouvant y répondre.

En ce qui concerne le deuxième point de votre demande, vous trouverez ci-joint un tableau qui contient les renseignements recherchés. Veuillez noter que ce tableau présente l'ensemble des dépenses effectuées pour l'achat de papiers-mouchoirs par le siège social de Santé Québec depuis la fusion des établissements de santé survenue le 1er décembre 2024. Par ailleurs, nous tenons à préciser que le tableau est présenté en fonction de l'année financière plutôt que l'année civile.

Conformément à l'article 51 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1), nous vous informons que vous pouvez demander la révision de cette décision auprès de la Commission d'accès à l'information. Vous trouverez ci-joint une note explicative à ce sujet.

Nous vous prions d'agréer nos cordiales salutations.

[redacted]

Me Anne de Ravinel, responsable de l'accès aux documents et de la protection des renseignements personnels

N/Réf. : 26-SQ-0001-047-01

p.j Avis de recours
Document (2)

AVIS DE RECOURS EN RÉVISION

Révision

a) **Pouvoir**

L'article 135 de la Loi prévoit qu'une personne peut, lorsque sa demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels ou dans le cas où le délai prévu pour répondre est expiré, demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

QUÉBEC

Commission d'accès à l'information
525, boul. René-Lévesque Est, bur. 2.36
Québec (Québec) G1R 5S9

Tél : (418) 528-7741
Téléc : (418) 529-3102

MONTRÉAL

Commission d'accès à l'information
2045, rue Stanley, bur. 900
Montréal (Québec) H3A 2V4

Tél : (514) 873-4196
Téléc : (514) 844-6170

b) **Motifs**

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) **Délais**

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135). La loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

APPEL DEVANT LA COUR DU QUÉBEC

a) **Pouvoir**

L'article 147 de la loi stipule qu'une personne directement intéressée peut porter la décision finale de la Commission d'accès à l'information en appel devant un juge de la Cour du Québec sur toute question de droit ou de compétence. L'appel d'une décision interlocutoire ne peut être interjeté qu'avec la permission d'un juge de la Cour du Québec s'il s'agit d'une décision interlocutoire à laquelle la décision finale ne pourra remédier.

b) **Délais**

L'article 149 prévoit que l'avis de l'appel d'une décision finale doit être déposé au greffe de la Cour du Québec, dans les 30 jours qui suivent la date de réception de la décision de la Commission par les parties.

c) **Procédure**

Selon l'article 151 de la loi, l'avis d'appel doit être signifié aux parties et à la Commission dans les dix jours de son dépôt au greffe de la Cour du Québec.

Titre :	**Règles sur le filtrage Web**		
État :	Approuvé	Effective à partir de :	2025-11-30
		Dernière mise à jour :	2025-11-30

Type :	Règles		
Code du document :	SanteQc-REG-0005	Portée :	Santé Québec
Mots clés :	Filtrage Web; Catégorie à risque; Blocage de contenu; Sites malveillants; Contrôle d'accès Internet; Sécurité réseau; Surveillance Web; Filtrage DNS; Contournement de Proxy		
Justification :	Cette règle vise à définir les paramètres de filtrage Web afin de protéger les actifs informationnels de Santé Québec, incluant ses unités administratives, contre les menaces en ligne. Elle impose le blocage de catégories de contenu Web à haut risque. Elle s'inscrit dans une approche de gouvernance de la sécurité de l'information et constitue une obligation minimale à mettre en œuvre dans tous les établissements relevant de Santé Québec ainsi qu'au ministère de la Santé et des Services sociaux (MSSS) et à ses organismes publics (OP).		

Déclaration	**Définitions**

Précisions :

- **Filtrage Web** : technique essentielle pour restreindre l'accès à des contenus Internet inappropriés ou dangereux;
- **Transfert de flux Nord/Sud** : mouvement de données entre l'intérieur du réseau (interne) et l'extérieur (Internet ou réseaux publics). Il s'agit du trafic qui entre ou sort du périmètre de sécurité de l'organisation, lequel inclut le réseau et peut s'étendre à tout appareil géré par l'organisation (exemple : poste de travail, tablette, etc.);
- **Lien réseau mission** : lien nécessitant une disponibilité élevée réservée aux équipements gérés de confiance et aux services critiques (exemple : postes de travail, systèmes cliniques, services essentiels, etc.);
- **Lien réseau hors mission** : lien distinct du lien de mission nécessitant une séparation physique/logique rigoureuse, destiné aux équipements non gérés ou à un usage non critique (exemple : Wi-Fi publics, milieu de vie);
- **Milieu de vie** : désigne un environnement physique, humain et social dans lequel une personne vit de façon permanente ou prolongée (exemple : Centre hospitalier de soins de longue durée, résidences pour aînés, etc.);
- **Catégories sensibles** : ensemble de contenus dont l'accès est justifié par un besoin professionnel spécifique et qui peut être délicat (exemple : adulte, nudité);

• **Catégories à risque discutable** : ensemble de contenus dont la pertinence professionnelle peut être mise en doute et qui peut présenter un risque modéré pour la sécurité (exemple : jeux, réseaux sociaux); • **Catégories à haut risque** : ensemble de contenus susceptibles ou reconnus pour présenter un risque élevé pour la sécurité (confidentialité, intégrité et disponibilité).
Lien avec :

Déclaration	**Mesures obligatoires du filtrage web**
Précisions :	
Tout établissement ou entité sous la responsabilité de Santé Québec doit minimalement activer un filtrage Web présentant les caractéristiques suivantes : 1. Blocage des catégories de contenu à haut risque (défini dans les déclarations subséquentes); 2. Activation sur tous liens réseau (mission, hors mission) permettant un transfert de flux Nord/Sud géré ou appartenant à l'organisation; 3. Être appliqué à tous les utilisateurs, postes de travail, serveurs et équipements réseau. Les établissements ou entités sans expertise suffisante pour mettre en œuvre le filtrage Web de manière sécuritaire doivent formellement solliciter l'assistance du Centre opérationnel de cyberdéfense (COCD).	
Justification :	L'activation du filtrage Web contribue à la protection des utilisateurs, à la sécurité des ressources informationnelles et à l'amélioration de la productivité.

Déclaration	**Catégories de contenu à haut risque à bloquer sur tout lien réseau mission**

Précisions :

Les catégories suivantes doivent systématiquement être bloquées sur **tout lien réseau mission** permettant un transfert de flux Nord/Sud géré ou appartenant à l'organisation.

Catégories de filtrage pré-définies	Description courte
Minage de cryptomonnaie (*Crypto mining*)	Sites exploitant les ressources informatiques pour miner des cryptomonnaies.
Stationnement de domaine (*Domain parking*)	Pages génériques associées à des domaines inactifs ou en attente.
Groupes extrémistes (*Extremist groups*)	Sites promouvant des idéologies radicales ou violentes.
Piratage informatique (*Hacking*)	Contenus liés à l'intrusion ou à la compromission de systèmes.
Illégal ou non éthique (*Illegal or unethical*)	Sites promouvant des activités interdites ou contraires à l'éthique.
Sites malveillants (*Malicious websites*)	Pages contenant des logiciels ou scripts nuisibles.
Domaine nouvellement observé (*Newly observed domain*)	Domaines récemment détectés sans historique connu.
Domaine nouvellement enregistré (*Newly registered domain*)	Domaines fraîchement enregistrés, souvent utilisés pour des attaques.
Partage de fichiers pair-à-pair (*Peer-to-peer file sharing*)	Sites facilitant le partage direct de fichiers entre utilisateurs.
Hameçonnage (*Phishing*)	Sites imitant des services légitimes pour voler des informations.
Programme potentiellement indésirable (*Potentially Unwanted Program*)	Applications pouvant affecter la performance ou la sécurité.
Contournement de proxy (*Proxy avoidance*)	Services permettant de contourner les contrôles de sécurité réseau.
Liens de pourriel (*Spam URLs*)	Adresses associées à des campagnes de pourriel ou redirections malveillantes.
Terrorisme (*Terrorisim*)	Contenus liés à des activités ou groupes terroristes.
Non classé (*Unrated*)	Sites sans catégorisation connue ou en attente d'analyse.

Justification :	Les catégories ciblées sont reconnues comme présentant un risque élevé pour la sécurité. Les bloquer contribue à la protection des utilisateurs, à la sécurité des ressources informationnelles et à l'amélioration de la productivité.

Déclaration	**Catégories de contenu à haut risque à bloquer sur tout lien réseau hors mission**
Précisions :	

Les catégories bloquées sur **tout lien réseau mission** doivent également être systématiquement bloquées sur tout **lien réseau hors mission** permettant un transfert de flux Nord/Sud géré ou appartenant à l'organisation.

- Consultez le tableau de la déclaration « **Catégories de contenu à bloquer sur tout lien réseau mission** ».

-Le blocage des catégories suivantes est **fortement recommandé,** sans être obligatoire, pour les réseaux hors mission:

Catégories de filtrage pré-définies (en recommandation)	Description courte
Domaine nouvellement observé (*Newly observed domain*)	Domaines récemment détectés sans historique connu.
Domaine nouvellement enregistré (*Newly registered domain*)	Domaines fraîchement enregistrés, souvent utilisés pour des attaques.
Non classé (*Unrated*)	Sites sans catégorisation connue ou en attente d'analyse.

Justification :	Bien que les catégories en recommandation présentent également un risque accru, leur blocage est recommandé et non obligatoire, sur les liens hors mission, en raison de contraintes liées à l'expérience utilisateur. Les catégories ciblées sont reconnues comme présentant un risque élevé pour la sécurité. Les bloquer contribue à la protection des utilisateurs, à la sécurité des ressources informationnelles et à l'amélioration de la productivité.

Déclaration	**Dérogation à l'activation du filtrage Web**
Précisions :	

Toute demande de dérogation doit être:

- Justifiée et documentée;
- Limitée dans le temps;
- Appliquée uniquement après approbation des niveaux d'autorité requis.
    - L'approbation doit être:
        1. Donnée par le Chef de la sécurité de l'information organisationnelle (CSIO) local;
        2. Approuvée définitivement par l'instance de gouvernance de Santé Québec afin d'assurer la conformité aux orientations provinciales et aux exigences de sécurité.

Lien avec :	Formulaire de dérogation

Déclaration	**Rappels liés au filtrage Web**
Précisions :	
1. Activer le filtrage Web à plusieurs niveaux (ex. : réseau, DNS, EDR tel que *Microsoft Defender for Endpoint*, etc.) afin de maximiser la couverture et la résilience contre les menaces Web; 2. Mettre en place un processus de vérification périodique pour s'assurer que les paramètres de filtrage Web sont correctement appliqués et fonctionnels; 3. Former les utilisateurs aux bonnes pratiques de navigation sécuritaire et à l'importance du filtrage Web dans la protection des actifs informationnels; 4. Exiger des utilisateurs le respect des paramètres de filtrage Web; 5. Mettre en place des mécanismes permettant aux utilisateurs de signaler les faux positifs; 6. Mettre en place un accès aux catégories sensibles ou à risques discutables basé sur des profils d'accès clairement définis (au niveau opérationnel ou local). Par exemple : un travailleur social ayant besoin d'accéder à une catégorie sensible (adulte) pourra y avoir accès en étant membre d'un profil d'accès défini selon ses besoins professionnels. L'accès à ces profils doit être audité, documenté, soumis à un cycle de vie formel et faire l'objet d'une révision régulière.	
Justification :	Une approche de défense en profondeur (*defense-in-depth*) est essentielle pour réduire les angles morts. De plus, une vérification régulière est requise pour garantir l'efficacité continue des contrôles de sécurité. Également, renforcer la responsabilité des utilisateurs permet une gestion proactive des exceptions.

Année	Période	Produit	Segment (classif. int.)	Type compte	Fournisseur	Origine réquisition	Montant
2026	06	70354 - MOUCHOIR KLEENEX2PLI BTE125BLC	70 - ACQUISITION AUTRES	10 - Dépense	100059 - HAMSTER / NOVEXCO INC.	3 - Bon de commande	25,94
2026	08	70354 - MOUCHOIR KLEENEX2PLI BTE125BLC	70 - ACQUISITION AUTRES	10 - Dépense	100059 - HAMSTER / NOVEXCO INC.	3 - Bon de commande	25,94
2026	10	70354 - MOUCHOIR KLEENEX2PLI BTE125BLC	70 - ACQUISITION AUTRES	10 - Dépense	100059 - HAMSTER / NOVEXCO INC.	3 - Bon de commande	51,89
2026	10	70501 - MOUCHOIR 2PLIS BLANC	70 - ACQUISITION AUTRES	10 - Dépense	100059 - HAMSTER / NOVEXCO INC.	3 - Bon de commande	10,9