Ministère
de l'Économie,
de l'Innovation
et de l'Énergie
Québec

Bureau du sous-ministre et Secrétariat général

PAR COURRIEL

[redacted],

La présente donne suite à votre demande d'accès à l'information reçue le 30 janvier 2026 pour laquelle vous souhaitez obtenir :

> *« copie de tout 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.*
>
> *À des fins de recherche, je souhaite également connaître les dépenses annuelles totales en papiers-mouchoirs pour cette même période.»*

Conformément à l'article 47 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) (« la Loi sur l'accès »), nous vous informons que le ministère de l'Économie, de l'Innovation et de l'Énergie détient un document quant au premier point de votre requête. Vous le trouverez ci-joint. Veuillez noter qu'un renseignement personnel de nature confidentielle a été caviardé en vertu des articles 14, 53 et 54 de la Loi sur l'accès.

Concernant le deuxième point de votre demande, aucun document n'a été retracé, le Ministère ne faisant pas l'acquisition de papiers-mouchoirs.

Si vous désirez contester cette décision, il vous est possible de le faire auprès de la Commission de l'accès à l'information. Vous trouverez ci-joint une note explicative concernant l'exercice de ce recours.

Je vous prie de recevoir, [redacted], l'expression de mes sentiments distingués.

Claudia Lacoste
Responsable de l'accès aux documents

710, place D'Youville, 6e étage
Québec (Québec) G1R 4Y4
Téléphone : 418 691-5656

AVIS DE RECOURS

Suite à une décision rendue en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

RÉVISION

a) Pouvoir

L'article 135 de la loi prévoit qu'une personne, dont la 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, peut 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
525, boulevard René-Lévesque Est, bureau 2.36
Québec (Québec)
G1R 5S9
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

Montréal
500, boulevard René-Lévesque Ouest, bur. 18.200
Montréal (Québec)
H2Z 1W7
Téléphone : 514 873-4016
Télécopieur : 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 de la Commission d'accès à l'information en appel devant trois juges de la Cour provinciale, sur toute question de droit ou de compétence. Cet appel ne peut toutefois être porté qu'avec la permission d'un juge de la Cour provinciale. Ce juge accorde la permission s'il est d'avis qu'il s'agit d'une question qui devrait être examinée en appel.

b) Délais et frais

L'article 149 prévoit que la requête pour permission d'appeler doit être déposée au greffe de la Cour provinciale, à Montréal ou à Québec, dans les 30 jours de la décision, après avis aux parties et à la Commission d'accès à l'information. Les frais de cette demande sont à la discrétion du juge.

c) Procédure

L'appel est formé, selon l'article 150 de la loi, par dépôt auprès de la Commission d'accès à l'information d'un avis à cet effet signifié aux parties dans les 10 jours qui suivent la date de la décision qui l'autorise. Le dépôt de cet avis tient lieu de signification à la Commission d'accès à l'information.

S'ENGAGER • INNOVER • *PROPULSER*

DIRECTIVE SUR L'UTILISATION DES ACTIFS INFORMATIONNELS

Version 1.0

Approuvée le 14 février 2024

Entrée en vigueur le 14 février 2024

Dans le présent document, le générique masculin est utilisé sans aucune discrimination et uniquement dans le but d'alléger le texte.

Québec

TABLE DES MATIÈRES

MISE EN CONTEXTE

Considérant le développement soutenu des technologies de l'information et l'accroissement des échanges et du partage d'information dans les différentes organisations, il est important pour le Ministère d'encadrer l'utilisation de ses actifs informationnels. Avec l'avènement du télétravail ainsi que l'utilisation accrue des appareils personnels à des fins professionnelles, cette directive vient encadrer l'utilisation des outils technologiques dans le cadre professionnel et limiter certaines pratiques.

La présente directive vient donc préciser les pratiques recommandées, le signalement de comportements non sécuritaires, les dérogations possibles, les sanctions en cas de non-respect et les responsabilités qui y sont rattachées.

1. OBJET

Cette directive vise à encadrer l'utilisation des actifs informationnels du Ministère par des règles auxquelles tout utilisateur doit se conformer dans le cadre de son travail. Les principaux objectifs sont de :

- s'assurer que l'utilisation des actifs informationnels est sécuritaire, légale et éthique;
- faire connaître aux utilisateurs les mesures de sécurité de l'information en vigueur ainsi que les sanctions qui pourraient être prises en cas d'usage inadéquat des actifs informationnels;
- préciser les comportements et les moyens de signalement attendus de la part des utilisateurs en cas d'incident de sécurité;
- définir les pratiques attendues de la part des utilisateurs pour préserver la sécurité de l'information.

2. CHAMP D'APPLICATION

La directive s'applique à tout le personnel[1] du Ministère utilisant sur place ainsi qu'à distance, ses infrastructures informatiques et ses actifs informationnels, ainsi qu'à toute autre personne dûment autorisée à y avoir accès.

L'information visée est celle que le Ministère détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

3. RÈGLES D'UTILISATION DES ACTIFS INFORMATIONNELS

Le Ministère met en œuvre des règles permettant l'utilisation de ses actifs informationnels en conformité avec les lois et règlements en vigueur au Québec et les bonnes pratiques reconnues en la matière.

[1] Le personnel inclut les employés du MEIE, les consultants et les stagiaires.

3.1 ÉTHIQUE

En lien avec les règles d'éthique énoncées dans le document L'éthique dans la fonction publique québécoise et la Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique (C.T. 198872 du 1er octobre 2002), l'utilisateur doit se comporter de manière telle que l'intégrité et l'efficacité de l'administration publique soient assurées en toutes circonstances. À cet effet, il doit :

- préserver l'image du Ministère en étant courtois et respectueux dans ses communications;
- éviter de se placer dans une situation où il y a conflit entre son intérêt personnel et les devoirs de ses fonctions ou d'avoir un intérêt direct ou indirect dans une activité qui crée un tel conflit;
- veiller à ne pas confondre les biens de l'État avec les siens;
- faire preuve de discrétion en préservant la confidentialité des renseignements personnels ou de nature confidentielle détenus par le Ministère;
- utiliser les actifs informationnels mis à sa disposition (ordinateur, espace de stockage réseau (U:, G:, O:, etc.), appareils mobiles, autres), dans le cadre de l'exécution de son travail et aux fins de cette exécution, de manière à ne pas nuire à l'exécution ou à l'efficacité de son travail.

3.2 DROITS DE PROPRIÉTÉ INTELLECTUELLE

En conformité avec la Loi sur le droit d'auteur (L.R.C. (1985), chapitre C-42), l'utilisateur doit respecter les droits de propriété intellectuelle, dont les droits d'auteur et les ententes contractuelles avec les fournisseurs. Il est donc strictement interdit à un utilisateur de copier, de reproduire ou de convertir dans un autre format tout programme, information ou logiciel si les lois ne le permettent pas.

3.3 SÉCURITÉ

Pour garantir la sécurité des actifs informationnels :

3.3.1 CONFIDENTIALITÉ

- L'utilisateur doit en tout temps préserver la confidentialité et l'intégrité du matériel informatique auquel il a accès. Il doit prendre toutes les précautions nécessaires afin d'assurer leur protection. Il doit également se conformer aux lois, aux règlements et aux politiques en matière d'accès aux documents et de protection des renseignements personnels, tout comme aux normes éthiques lui étant applicables dans le Règlement sur l'éthique et la discipline dans la fonction publique (F-3.1.1, r. 3). Il doit en outre faire preuve de jugement dans l'utilisation du matériel informatique mis à sa disposition. L'utilisateur ne doit pas chercher à obtenir et exploiter des informations ou avantages relatifs aux actifs informationnels auxquels il a accès dans le cadre de ses fonctions, quel qu'en soit le support;
- L'utilisateur doit respecter les mesures de sécurité mises en place afin de protéger de toute intrusion dans les locaux, les ordinateurs, les systèmes d'information et le réseau du Ministère;

3.3.2 PROTECTION DES ACTIFS

- L'utilisateur doit veiller à la sécurité des actifs informationnels mis à sa disposition ou placés sous sa responsabilité. Il est interdit d'utiliser, sur un actif informationnel, tout logiciel ou fichier susceptible de nuire au fonctionnement ou à la sécurité du réseau informatique. Il est également interdit de prendre connaissance, de modifier, de détruire, de divulguer en tout ou en partie, un actif informationnel sans une autorisation préalable.

3.3.3 DROIT D'ACCÈS

- L'utilisateur doit respecter les règles de sécurité liées à l'infrastructure technologique ministérielle, en évitant toute modification ou contournement. L'authentification est un moyen de protéger les informations, et chaque utilisateur doit se conformer aux mesures de sécurité en vigueur. Toute demande d'accès doit être approuvée par un responsable habilité, sans quoi elle sera automatiquement refusée.
- L'utilisateur est responsable de la confidentialité de son identifiant et de son mot de passe, et il ne doit jamais les divulguer. Les mots de passe doivent être stockés de manière sécurisée, sans être accessible physiquement ou mémoriser dans un navigateur Internet. En cas d'usurpation d'identité, l'utilisateur doit changer son mot de passe rapidement et contacter le Centre de services informatiques (CSI) du Ministère. Il est strictement interdit de falsifier ou d'usurper une autre identité, et l'utilisateur doit se conformer aux règles établies par le Ministère, y compris les vérifications d'identité nécessaires.
- Le gestionnaire doit informer les ressources humaines du départ d'un membre du personnel interne en respectant les délais prescrits, afin de retirer rapidement les accès non nécessaires et réduire les risques de sécurité. La Direction des ressources informationnelles (DRI) peut révoquer ou modifier les accès d'un utilisateur à tout moment, en informant l'utilisateur concerné des modifications apportées.

PRÉCISION ACCÈS À PRIVILÈGES ÉLEVÉS

Les utilisateurs ayant un ou des compte(s) à privilèges élevés dans le cadre de leurs fonctions bénéficient de droits d'accès exceptionnels à des éléments d'actif informationnel du Ministère. Ces privilèges élevés impliquent également l'accès à des informations de nature confidentielle ou sensible et dont l'utilisation est protégée et réservée à certains utilisateurs.

Ces utilisateurs à privilèges élevés occupent, entre autres, les postes d'administrateur de systèmes, de pilote de systèmes ou ils sont responsables en tout ou en partie d'un ou plusieurs systèmes, logiciels, programmes, applications ou banques de données.

Chaque utilisateur détenant un compte à privilèges élevés, qu'il soit employé du Ministère ou non, s'engage à ce que ses accès ou ses droits exceptionnels se limitent exclusivement aux interventions requises dans le cadre de ses fonctions ainsi qu'au respect des règles de sécurité en vigueur. Tout accès se doit d'être justifié. Les utilisations jugées conformes sont : la gestion d'un système, le maintien des opérations ainsi que la gestion de la sécurité. La confidentialité de toute information accessible doit être préservée.

Tout employé disposant d'accès à privilèges élevés est assujetti à une vérification proportionnelle aux droits qui lui sont attribués par le Ministère. Tout acte susceptible de compromettre la sécurité des actifs informationnels ou d'altérer l'image du Ministère sera jugé répréhensible et pourra conduire à la révocation des accès octroyés ainsi que donner lieu à des mesures administratives ou légales selon la gravité de l'action posée.

3.3.4 INCIDENTS

- L'utilisateur doit rapporter à son gestionnaire et au Responsable opérationnel de cyberdéfense (ROCD) tout incident ou problème de sécurité dans l'utilisation d'un actif informationnel.

3.3.5 PROTECTION DES RENSEIGNEMENTS PERSONNELS

- Le Ministère et ses utilisateurs ont des obligations en matière de protection des renseignements personnels. Ces obligations, prévues par la Loi sur l'accès aux documents des organismes publics et sur

la protection des renseignements personnels, concernent les façons de collecter, conserver les données, la façon de protéger ces données une fois collectées et les obligations envers les citoyens à l'origine de ces données. Les employés du ministère de l'Économie, de l'Innovation et de l'Énergie (MEIE) doivent prendre connaissance de ces obligations à partir du document normatif approuvé en septembre 2023 : Politique sur la protection des renseignements personnels.

4. MESURES DE SÉCURITÉ DE L'INFORMATION

Le Ministère effectue la surveillance de ses actifs informationnels par différentes mesures de sécurité, afin de veiller à leur disponibilité, à leur intégrité et à leur confidentialité. Pour ce faire, le Ministère effectue, entre autres et sur demande préalable dans certains cas, la surveillance et la journalisation des accès à ses édifices, la journalisation des accès informatiques, l'identification de chaque site Internet visité ainsi que la prise de copie des courriels entrants et sortants. Cela comprend des spécifications adaptées au contexte du télétravail, considérant que les risques pour la sécurité de l'information sont plus élevés, notamment en matière de cyberattaques. Dans ces conditions, l'utilisateur doit être vigilant et appliquer rigoureusement les mesures de sécurité de l'information énoncées dans la présente directive.

Journalisation des accès

Si un gestionnaire a un doute sur l'utilisation qu'un de ses employés fait des actifs informationnels du Ministère, il peut demander à la Direction des ressources humaines ou au sous-ministre de soumettre un utilisateur à une analyse particulière. Cette analyse permettra de déterminer si son utilisation est conforme ou non au cadre normatif en cette matière (lois, règlements, directives, politiques et règles internes).

À noter que toute information enregistrée ou consignée est réputée constituer une information à laquelle le Ministère a accès. Au besoin, l'utilisateur doit être en mesure d'expliquer son temps d'utilisation et de justifier ses accès.

Équipement informatique fourni par le Ministère

L'équipement mis à la disposition d'un utilisateur doit être conservé de façon sécuritaire. En cas de vol ou de perte d'un équipement informatique appartenant au Ministère, il doit le déclarer à son gestionnaire et au CSI qui réaliseront les mesures appropriées dans les meilleurs délais. L'utilisateur doit respecter les configurations de sécurité mises en place sur l'équipement informatique du Ministère. Il ne doit pas les modifier, les désactiver, les atténuer, les contourner ou éviter des mécanismes de protection ou des contrôles qui permettent la gestion ou la vérification de l'utilisation appropriée.

Il est interdit d'utiliser à son profit ou de tirer quelconques avantages personnels des moyens électroniques mis à la disposition des employés du Ministère. Il n'est pas permis d'utiliser l'équipement informatique fourni à des fins autres que celles explicitement autorisées. Les utilisations non permises incluent, entre autres, une utilisation illégale, abusive ou malveillante de celui-ci. Le Wi-Fi et les réseaux du MEIE sont considérés comme des équipements du Ministère et doivent être utilisés à des fins de travail seulement.

Applications sur les postes

L'utilisateur doit avoir recours uniquement aux applications homologuées et installées par la DRI sur l'équipement informatique (cellulaire, tablette, ordinateur, portable, etc.) appartenant au Ministère. Avant l'utilisation d'une application, ce dernier doit s'assurer de respecter les règles en vigueur et de suivre les indications de la DRI à cet effet. L'installation ou l'utilisation d'applications non autorisées constituent un risque de sécurité et pourront être retirées en tout temps.

Données et stockages infonuagiques

L'infonuagique ministérielle, telle qu'Office 365, OneDrive, Microsoft Teams et Sharepoint, peut être utilisée pour la plupart des activités courantes et la collaboration gouvernementale. Les outils de partage et d'entreposage disponibles gratuitement, tels que la version personnelle de OneDrive, Dropbox et Google Drive, ne doivent pas être utilisés à des fins professionnelles. Seuls les outils autorisés par la DRI et pour lesquels le Ministère dispose d'ententes sont permis.

PRÉCISION POUR LE RÉPERTOIRE PERSONNEL

Le répertoire personnel des usagers est un espace à accès restreint qui est réservé à un utilisateur afin d'y déposer des documents reliés à l'emploi. Par exemple : des processus, des guides, des comptes rendus de réunion, des documents syndicaux, des bulletins de paie, les attentes, le bilan, la description d'emploi, etc. L'utilisateur doit en faire un usage raisonnable, en limitant la quantité de fichiers à caractère professionnel qui y sont emmagasinés.

Le téléchargement et le stockage de fichiers vidéo ou audio illégaux comme des films, des séries et des œuvres musicales sont considérés comme une violation du droit d'auteur qui est susceptible d'entraîner des poursuites judiciaires. Cette pratique déroge également aux règles d'éthique et de discipline applicables dans la fonction publique et est susceptible d'entraîner des sanctions administratives le cas échéant. Il n'est pas permis de télécharger ou distribuer d'œuvres protégées par le droit d'auteur en utilisant l'équipement informatique du Ministère.

Appareils personnels

Seuls les appareils homologués par la DRI tels qu'un téléphone intelligent, une tablette et un ordinateur peuvent être branchés sur le réseau du Ministère.

Un accès aux courriels et teams peut être permis sur des téléphones personnels s'ils se conforment à nos règles et conditions d'accès.

Courriel

Conformément à la Directive gouvernementale sur l'utilisation éthique du courriel (C.T. 198872 du 1er octobre 2002), d'un collecticiel et des services d'Internet par le personnel de la fonction publique, chaque utilisateur doit faire usage des actifs informationnels du ministère de façon judicieuse. Il s'agit ici d'actions effectuées par l'utilisateur vers l'extérieur de l'infrastructure technologique du Ministère.

L'utilisateur doit avoir recours à son adresse courriel ministérielle avec jugement et réserve pour limiter les risques visant les actifs informationnels. Son utilisation est permise sur des sites en lien avec le travail, sur les infrastructures et lors de communications au nom du Ministère. Il n'est pas permis d'utiliser l'adresse courriel ministérielle pour un usage personnel.

Pour que l'envoi d'un courriel soit sécuritaire, il ne faut pas inclure de renseignements personnels tels qu'une date de naissance, un numéro d'assurance sociale, un identifiant et un mot de passe. De plus, il ne faut pas transférer de document de nature confidentielle par courriel, mais plutôt utiliser un moyen de transfert sécuritaire selon le besoin qui se présentera. Il est interdit de créer, d'expédier ou de réexpédier par courriel tout message électronique ou fichier qui contient un élément susceptible d'affecter le fonctionnement de l'équipement mis à sa disposition ou d'un réseau gouvernemental auquel il est relié. L'utilisateur ne peut, pour quelque motif que ce soit, poser un geste contraire aux règles d'utilisation des services de courriels ou d'Internet en vigueur au Ministère (voir la liste non exhaustive des gestes proscrits à l'annexe 1).

Lorsqu'un courriel douteux (hameçonnage ou ingénierie sociale) se retrouve dans la boîte de réception, et qu'il n'est pas classé automatiquement dans le dossier courrier indésirable, l'utilisateur doit utiliser le bouton « signaler comme hameçonnage » dans Outlook, sans l'ouvrir lorsque possible. Si le courriel a été ouvert, il doit en aviser le CSI dans les plus brefs délais.

PRÉCISION SUR L'IDENTIFICATION D'UN COURRIEL DOUTEUX

Voici des signes qu'un courriel pourrait être douteux :

- Une demande de mise à jour ou de confirmation de renseignements personnels telle que : identifiant, mots de passe, coordonnées bancaires par un prétendu organisme d'accès public ou commercial de confiance.
- Une demande de règlement pour éviter la révocation d'un permis, d'une facture ou autre urgence.
- Une demande urgente, tel un paiement immédiat, qui impose une courte échéance.
- Une offre qui semble trop belle pour être vraie.
- Un courriel d'apparence légitime, mais qui contient des fautes d'orthographe ou de grammaire, etc.
- Un nom, une adresse courriel ou un numéro de téléphone d'expéditeur que vous ne reconnaissez pas (extension douteuse telle que « .net, .info, .ru ») ou de provenance externe.

Signalement

Il est du devoir de l'utilisateur de signaler tout acte ou problème susceptible de constituer une atteinte présumée ou réelle aux mesures de sécurité de l'information applicables ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du Ministère à leur supérieur immédiat ou hiérarchique. De la même façon, toute contravention à la présente directive doit être signalée. Si l'utilisateur constate une activité inhabituelle ou suspecte sur l'équipement informatique (ordinateur, appareil mobile, réseau domestique ou public), reçoit un courriel malicieux, détecte un virus ou toute autre menace, il doit le signaler immédiatement.

Pour signaler un incident informatique ou un incident de sécurité de l'information, contactez l'équipe du CSI en composant le 1111 (ou 1-866-680-1879) ou en écrivant un courriel à l'adresse csi-demandes@economie.gouv.qc.ca. Le CSI fournira également les instructions requises pour effectuer les correctifs nécessaires qui doivent être pris avant de débrancher le poste du réseau.

5. DISPOSITIONS FINALES

La présente directive découle de la Politique ministérielle sur la sécurité de l'information et du Cadre de gestion de la sécurité de l'information du Ministère.

Le responsable organisationnel de la sécurité de l'information s'assure de la mise en œuvre des dispositions de la présente directive et de ses règles d'utilisation.

La présente directive doit être révisée lors de changements significatifs qui pourraient l'affecter.

6. ENTRÉE EN VIGUEUR

Cette directive entre en vigueur à la date de son approbation par le sous-ministre.

[redacted]

SOUS-MINISTRE

2024-02-14

DATE

ANNEXE 1 – GESTES PROSCRITS (LISTE NON EXHAUSTIVE)

Activité pyramidale

Participation, conduite ou administration d'un plan, d'un arrangement ou d'une opération de type pyramidal qui procure un bénéfice personnel ou des retombées positives personnelles.

Diffamation

Diffusion, sans justification ni excuse légitime, d'information qui est de nature à nuire à la réputation de quelqu'un en l'exposant à la haine, au mépris ou au ridicule ou qui est destinée à outrager la personne concernée.

Harcèlement

Agissement vexatoire, méprisant, menaçant ou nuisible à l'égard d'une personne ou d'un groupe de personnes en raison notamment des éléments suivants : la race, un handicap, une grossesse, l'apparence physique, l'orientation sexuelle, l'état civil, l'âge, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale ou la condition sociale.

Harcèlement sexuel

Acte à connotation sexuelle pouvant porter atteinte à la dignité ou à l'intégrité physique ou psychologique d'une personne, pouvant compromettre un de ses droits ou pouvant entraîner pour elle des conditions de travail défavorables, une mise à pied ou un congédiement.

Interception d'une communication privée

Fait d'intercepter illégalement un message ou un document numérique destiné à quelqu'un d'autre.

Message publicitaire

Transmission d'un message publicitaire qui sollicite de manière inconsidérée les ressources du réseau.

Obscénité

Fait d'accéder volontairement à tout document obscène, de l'avoir en sa possession, de le produire, de l'imprimer, de le télécharger ou de le distribuer. Un document est réputé obscène s'il a comme caractéristique dominante l'exploitation indue de la sexualité ou de la sexualité combinée au crime, à l'horreur, à la cruauté ou à la violence.

Pornographie

Fait d'accéder volontairement à de la pornographie, d'en avoir en sa possession, d'en produire, d'en imprimer, d'en télécharger ou d'en distribuer.

Propagande haineuse

Fait d'accéder volontairement à un site Internet incitant à la haine ou à la violence contre des groupes identifiables ou fait de distribuer des messages de cette nature.

Téléchargement de musique

Fait d'accéder volontairement à des sites de musique afin d'en télécharger à des fins non liées au travail.

Vol, fraude, abus de confiance et autres actes jugés criminels

Ensemble d'actions illégales qui enfreignent les lois en vigueur. Cela peut inclure une variété d'infractions, telles que le vol d'information ou de biens, l'extorsion, ou d'autres comportements considérés comme répréhensibles par la loi.

economie.gouv.qc.ca

Économie,
Innovation et Énergie
Québec