Régie du logement
Québec

Directive sur le traitement des demandes d'accès à l'information

Mars 2018

1. Objectifs

- Uniformiser le traitement des demandes d'accès à l'information;
- Optimiser le processus de traitement des demandes d'accès à l'information en rendant notamment l'allocation des ressources plus efficiente;
- Rencontrer nos obligations en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* tout en visant, à long terme, la réduction du nombre de demandes en orientant les citoyens vers les ressources disponibles sur internet afin qu'ils obtiennent eux-mêmes l'information recherchée lorsqu'elle est disponible conformément à l'article 13 de la Loi.

2. Cadre administratif et légal

La présente directive s'appuie sur la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

La directive sur le traitement des demandes d'accès à l'information prend en considération le cadre légal qui institue la Régie du logement. Elle tient également compte des autres lois et règlements, règles d'éthique et valeurs gouvernementales.

3. Champ d'application

La présente directive s'applique aux demandes d'accès à l'information transmises à la Régie du logement par écrit.

Elle s'applique, avec les adaptations nécessaires, aux demandes verbales d'accès à un document.

Aux fins de la présente directive, le vocable « demande d'accès à l'information » englobe toute demande visant à obtenir accès à un document ou à des renseignements personnels adressées au président, au responsable de l'accès aux documents et de la protection des renseignements personnels ou incluant toute mention qu'il s'agit d'une demande d'accès au sens de la loi.

4. Principes directeurs

Le traitement des demandes d'accès à l'information s'effectue conformément aux prescriptions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

En plus de respecter les valeurs organisationnelles de la Régie du logement, le traitement de ces demandes repose sur trois valeurs : l'efficience, l'accessibilité et la transparence.

5. Responsabilités administratives

Le président est responsable de l'application et du respect de la présente directive.

La personne désignée comme responsable de l'accès aux documents et de la protection des renseignements personnels à la Régie du logement exerce les fonctions qui lui sont conférées par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

Ainsi, la personne désignée comme responsable de l'accès aux documents et de la protection des renseignements personnels (annexe 1) :

- reçoit et centralise les demandes d'accès à l'information;
- informe le requérant que seule une décision sur une demande écrite peut faire l'objet d'une révision par la Commission d'accès à l'information, s'il s'agit d'une demande verbale d'accès à un document,
- accuse réception des demandes écrites;
- ouvre un dossier physique pour chacune des demandes;
- analyse les demandes d'accès à l'information;
- détermine le suivi approprié à donner;
- assure le suivi auprès de la Présidence, le cas échéant;
- détermine si des frais sont exigibles conformément au *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements personnels* et en informe le requérant, le cas échéant;
- s'il s'agit d'une demande écrite, envoie la décision, l'avis de recours ainsi que les documents, le cas échéant;
- s'il s'agit d'une demande verbale d'accès à un document, informe le requérant de sa décision selon le mode qu'il détermine et envoie les documents, le cas échéant;
- répertorie, classe et tient à jour les dossiers;
- diffuse sur le site Internet de la Régie du logement les documents transmis dans le cadre des demandes d'accès et les décisions anonymisées, sous réserve des exceptions prévues au *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels.*

Le responsable de l'accès aux documents et de la protection des renseignements personnels implantera le nouveau processus.

6. Commission d'accès à l'information

Le citoyen qui a formulé une demande écrite peut, s'il est insatisfait de la décision rendue, en demander la révision auprès de la Commission d'accès à l'information du Québec.

7. Entrée en vigueur

La présente directive entre en vigueur le jour de sa signature par le président.

Patrick Simard, président

22 mars 2018
Date

Annexe 1 : Processus de traitement des D.A.I formulées par écrit

Le responsable du traitement des D.A.I :

1) Reçoit la demande d'accès à l'information;
2) Ouvre le dossier;
3) Envoie un avis de date au requérant (accusé de réception) accompagné de l'avis de recours;
4) Analyse la demande afin de décider des démarches qui doivent être effectuées.

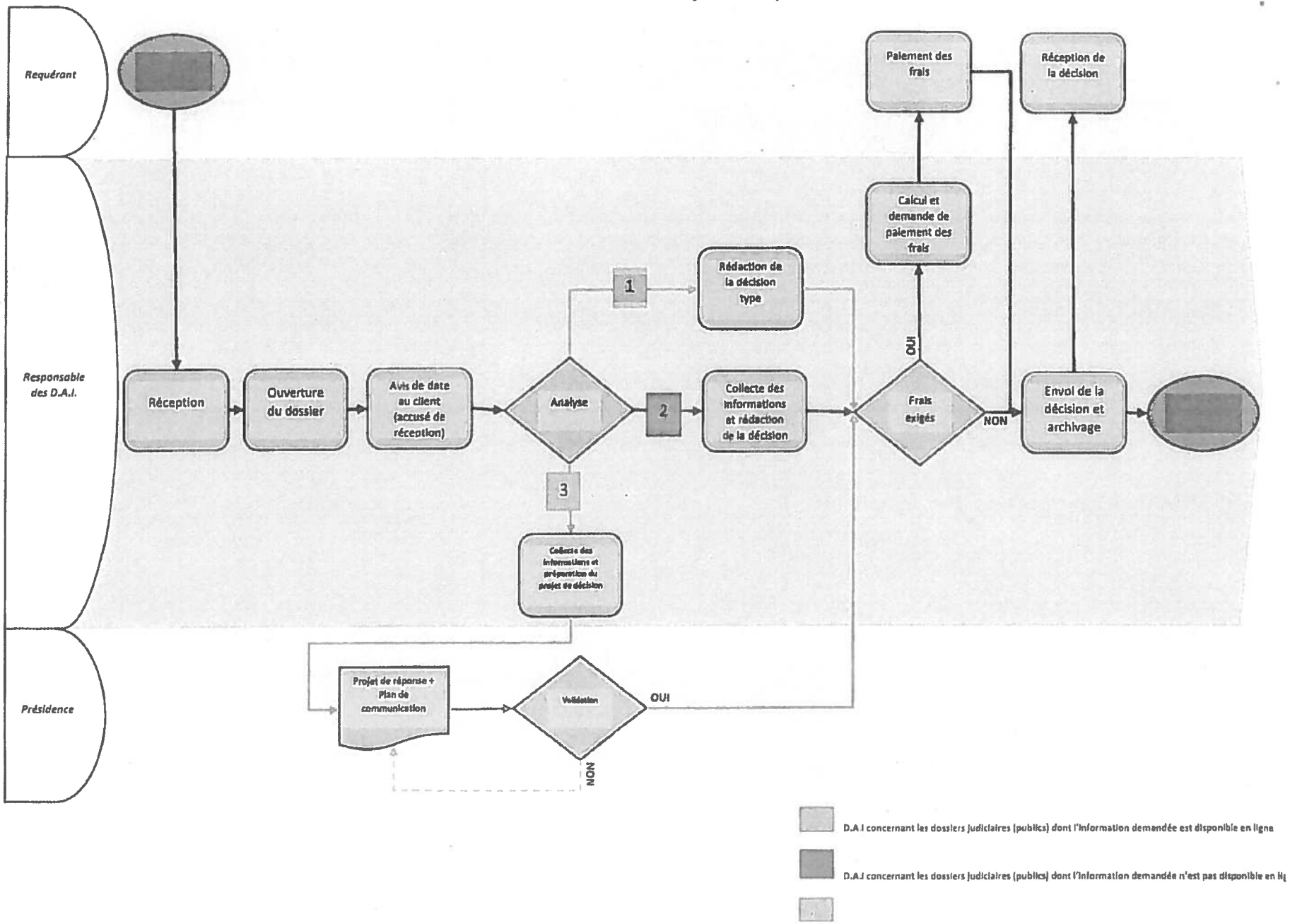
À la suite à cette analyse, 3 cheminements sont possibles :

1 *D.A.I concernant les dossiers judiciaires (publics) dont l'information demandée est disponible en ligne*	2 *D.A.I concernant les dossiers judiciaires (publics) dont l'information demandée n'est pas disponible en ligne*	3 *D.A.I concernant les dossiers autres que les dossiers judiciaires*
Le responsable du traitement des D.A.I :	***Le responsable du traitement des D.A.I :***	***Le responsable du traitement des D.A.I :***
4.1.1- Utilise la banque des lettres types pour rédiger la décision. Cette dernière indique au requérant comment accéder à l'information demandée sur le site web de la RDL.	4.2.1- Collecte les informations demandées. 4.2.2- Rédige la décision à envoyer au requérant.	4.3.1- Collecte les informations demandées. 4.3.2- Rédige un projet de décision. 4.3.3 Prépare un plan de communication 4.3.4 Transmet le dossier à la Présidence pour validation Si le projet est validé : 4.3.5.- Passe à l'étape suivante. Si le projet n'est pas validé : 4.3.5.- Retour à l'étape 4.3.2.

Le responsable de traitement des D.A.I :

5) Vérifie si des frais sont exigibles
   5.1) Si oui : envoie une demande de paiement au requérant
   5.2) Si non : passe à l'étape suivante
6) Envoie au requérant la décision et les informations demandées, le cas échéant, ainsi que l'avis de recours.
7) Archive la documentation.
8) Publie, dans les 5 jours ouvrables, la décision et les documents sur le site web de la Régie du logement (seulement pour les demandes qui ne concernent pas les dossiers judiciaires ou sauf s'il n'a pas à être diffusé)
9) Fermeture du dossier.

Processus de traitement des D.A.I formulées par écrit



Régie du logement Québec

Guide à l'intention des consultants	
Objet	Guide à l'usage des consultants qui accomplissent un mandat à la Régie du logement
Date d'approbation	20-03-2013
Note	*Ce guide est une version modifiée du guide réalisé à la SAAQ*

Ce guide, à l'usage des consultants qui accomplissent un mandat à la Régie, fait un rappel des obligations en matière d'éthique, de sécurité de l'information et de protection des renseignements personnels.

1. L'ÉTHIQUE

L'éthique est une façon de diriger nos comportements en faisant appel à notre jugement et à notre sens des responsabilités. Elle met l'accent sur les valeurs pour donner un sens à nos décisions et à nos actions. Ainsi, les valeurs apportent un éclairage dans la réflexion préalable à la prise de décisions. L'enjeu premier de l'éthique pour une organisation de services publics est de maintenir et de renforcer collectivement la confiance que les citoyens ont envers elle.

Ainsi, le consultant qui travaille à la Régie est incité à appuyer ses actions et ses décisions sur les valeurs de l'organisation, soit le respect, la diligence, la loyauté et la qualité.

1.1. Chacun témoigne de son engagement en adhérant à la vision, à la mission et aux valeurs de la Régie et en s'en inspirant quotidiennement.

Manifester son engagement c'est :

- *faire preuve de leadership et influencer le milieu de travail par son comportement exemplaire, son sens critique et le dialogue ;*
- *établir des relations interpersonnelles constructives visant le maintien d'un bon climat de travail ;*
- *mettre en commun les efforts et prendre en compte les compétences particulières et les préoccupations des autres dans la réalisation de la mission de l'organisation.*

L'engagement suppose une motivation du consultant à mettre ses idées et ses habiletés au service de la mission de l'organisation.

1.2. Chacun agit avec rigueur, c'est-à-dire avec professionnalisme, intégrité et équité.

Agir avec professionnalisme, c'est :

- *s'assurer de respecter les délais prévus, avec tout le soin et toute l'attention nécessaires à un travail de qualité ;*
- *chercher à tenir à jour et à améliorer ses connaissances ;*
- *mettre à profit son habileté et son expérience pour atteindre les résultats visés.*

Agir avec intégrité, c'est :

- *travailler avec honnêteté ;*
- *utiliser de façon judicieuse l'information ou le matériel disponible pour l'exécution de son contrat, et non à des fins personnelles ou au profit d'un tiers ;*
- *préserver son objectivité, son impartialité et sa crédibilité :*
  - *en s'abstenant d'accorder, de solliciter ou d'accepter toute faveur ou tout avantage indu pour soi-même ou pour une autre personne (par exemple, s'abstenir de communiquer avec un membre du comité de sélection d'adjudication de contrats afin d'influencer le processus d'adjudication ou de tenter d'obtenir plus de détails quant au résultat d'adjudication),*
  - *en évitant toute situation de conflit d'intérêts, réel ou apparent, et si une telle situation se présente, en informer immédiatement la Régie.*

Agir avec équité, c'est :

- *apprécier avec justesse ce qui est dû à chacun, en faisant preuve :*
  - *d'égalité de traitement (égalité devant la loi),*
  - *d'impartialité (intervenir sans préjugé, ni discrimination),*
  - *de jugement (reconnaître les particularités et les différences de certaines personnes pour assurer un juste traitement de leur dossier).*

1.3. Chacun agit en toute cohérence avec la Régie.

Agir avec cohérence, c'est :

- *favoriser l'esprit d'équipe ;*
- *communiquer efficacement afin de favoriser la coordination des interventions et la production de services de qualité au meilleur coût ;*
- *être responsable, c'est-à-dire :*
  - *respecter les lois et les normes applicables au travail confié,*
  - *arrêter ses choix en considérant les conséquences sur les parties impliquées,*
  - *pouvoir justifier ses décisions et en assumer les conséquences.*

1.4. Chacun agit avec respect en maintenant une relation de confiance.

Agir avec respect, c'est :

- *être poli et courtois dans ses gestes et ses paroles ;*
- *faire preuve de transparence et d'écoute ;*
- *faire preuve de discrétion et de retenue ;*
- *s'abstenir de toute violence ou de tout harcèlement ;*
- *dans ses communications, se présenter en précisant son statut et son mandat, y compris lors des réunions ;*
- *permettre au personnel de la Régie de respecter ses obligations de confidentialité et de protection des renseignements personnels ;*
- *permettre aux professionnels de la Régie de respecter leur obligation au secret professionnel ;*
- *si un avis juridique est requis, demander au gestionnaire responsable de son contrat de faire une demande.*

2. LA SÉCURITÉ DE L'INFORMATION

La Régie a mis en place diverses mesures de sécurité pour s'assurer de la confidentialité, de l'intégrité et de la disponibilité de l'information qu'elle détient. Il est de votre responsabilité de respecter ces mesures et de se conformer aux exigences de sécurité énoncées dans ***la politique de sécurité de l'information*** et dans les directives, règles, procédures ou autres mesures qui en découlent, ainsi que les annexes (engagement de confidentialité, guide pour la destruction des documents renfermant des renseignements personnels, ...) joints à votre contrat de service.

2.1. UTILISATION DE VOTRE CODE D'UTILISATEUR

Ce code sert à établir votre identité et à vous permettre d'accéder aux données dont vous avez besoin pour effectuer votre mandat. Il vous est attribué lors de votre entrée en fonction à la Régie et est à votre usage exclusif. Vous êtes responsable des accès effectués sous votre code d'utilisateur.

> Il est essentiel de verrouiller votre session lorsque vous vous absentez de votre poste de travail.

2.2. UTILISATION DE VOTRE MOT DE PASSE

Le mot de passe sert à valider votre identité. Il est important de le garder secret, sans quoi une personne qui le connaît pourrait usurper votre identité. Elle pourrait ainsi consulter, modifier ou même détruire des données et effectuer des opérations qui vous seraient imputées.

> Si vous croyez que quelqu'un connaît votre mot de passe, vous devez immédiatement le changer

2.3. UTILISATION DE VOTRE MICRO-ORDINATEUR

Si vous utilisez votre propre micro-ordinateur lors de l'exécution de votre mandat à la Régie, vous devez vous assurer en tout temps de respecter les exigences mentionnées à votre contrat à cet égard (antivirus, système d'exploitation, mise à jour de logiciels, etc.).

2.4. UTILISATION D'UNE CLÉ USB

Si vous devez utiliser une clé USB pour le transport d'informations, vous êtes tenu d'utiliser une clé USB sécuritaire, qui :

- est pourvue d'un mécanisme de chiffrement ;
- permet le chiffrement automatique de toutes données copiées sur la clé ;
- est doté d'un algorithme de chiffrement robuste (AES 256 bits au minimum).

> À titre d'exemple, la clé USB « Kingston Data Traveler 5000 » répond aux exigences de sécurité de la Régie

2.5. UTILISATION DU COURRIEL

Seule l'adresse de courriel se terminant par « @rdl.gouv.qc.ca » doit être utilisée lors de communications effectuées au nom de la Régie.

> Il est interdit de transmettre à l'extérieur de la Régie – par courriel, par collecticiel, par Internet ou par un autre moyen – tout renseignement de nature confidentielle qui n'a pas fait l'objet d'un chiffrement.

Vous ne devez jamais rediriger un « courriel RDL » sur un réseau non protégé (par exemple sur

un téléphone intelligent, à votre entreprise, à un autre ministère ou organisme, ou à votre domicile). De même, vous ne devez jamais inciter un employé de la Régie à vous transmettre des documents confidentiels sur des réseaux externes.

Toute information stockée ou consignée sur l'équipement électronique de la Régie à l'aide d'un courriel, d'un collecticiel, d'Internet, ou par tout autre moyen, est réputée constituer une information à laquelle la Régie a accès. Ainsi, la Régie peut récupérer le contenu des boîtes de courriel si elle le juge opportun.

Enfin, au terme de votre mandat, vous devez effacer de votre boîte de courriel les renseignements personnels et les autres informations qui vous appartiennent. L'utilisation du courriel est un privilège qui peut vous être enlevé en tout temps, pour tout motif jugé raisonnable.

2.6. UTILISATION D'INTERNET

L'utilisation d'Internet est permise uniquement pour l'accomplissement de votre mandat à la Régie

Seules les personnes autorisées peuvent avoir accès et utiliser les réseaux électroniques et Internet dans les limites des privilèges qui leur sont accordés par la Régie. L'utilisation de ce privilège doit être raisonnable et efficace.

La Régie tient un registre quotidien des sites Internet visités par chaque utilisateur. Rappelez-vous que certains sites recueillent l'adresse de leurs visiteurs et publient parfois des statistiques à ce sujet.

Pour plus d'information, consultez la ***Politique sur l'utilisation des réseaux électroniques, d'internet, d'intranet et du courrier électronique à la Régie du logement.***

2.7. SIGNALEMENT DES INCIDENTS

Vous devez rapporter rapidement tout problème de sécurité informatique (ex. code malveillant, virus informatique) au centre d'assistance aux utilisateurs (CAU) en composant le (514) 864-4427

2.8. CONFIDENTIALITÉ DE L'INFORMATION

L'information communiquée par la Régie est confidentielle, de même que celle que vous devez produire dans le cadre de votre mandat. À titre d'exemple, il peut s'agir de documentation ou d'information concernant des projets de développement, des plans d'action, des façons de faire actuelles ou envisagées, des mécanismes de sécurité, des contrôles ou des problèmes à corriger. Sauf si votre contrat de service prévoit le contraire ou si vous obtenez l'autorisation d'un représentant de la Régie, cette information appartient à la Régie et doit demeurer dans ses bureaux.

- Vous ne pouvez pas utiliser cette information à d'autres fins que la réalisation de votre mandat.

- Il vous est interdit de faire des copies des documents, que ce soit pour un usage personnel ou professionnel, ou pour une référence future.

- Vous ne pouvez pas communiquer l'information à d'autres personnes, à moins que cela ne soit requis pour l'exécution du mandat.

2.9. CONFIDENTIALITÉ DES DONNÉES INFORMATIQUES

La Régie détient de nombreux renseignements sur les citoyens, son personnel et ses fournisseurs. Malgré la nature publique de la plupart des renseignements détenus par la Régie, une partie des informations peut être considéré comme personnelle et confidentielle.

- Il vous est strictement interdit de consulter et d'utiliser ces renseignements à d'autres fins que la réalisation de votre mandat.

- Avant de pouvoir accéder à des renseignements confidentiels sur les clientèles, le personnel ou les fournisseurs de la Régie, vous devez signer un formulaire d'engagement à la confidentialité.

- Vous devez utiliser des données fictives pour les essais de système et les autres tests.

3. PROTECTION DES RENSEIGNEMENTS PERSONNELS

Afin d'assurer la confidentialité des renseignements personnels, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels énonce des règles précises.

Ces règles concernent :

3.1. L'ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Toute personne physique a droit à la confidentialité des renseignements qui la concernent. Elle (ou son représentant autorisé) a le droit d'y accéder, d'en demander copie, ou de les faire rectifier.

Remarque : Vous n'êtes pas autorisé à traiter les demandes d'accès ou de rectification. Elles doivent être adressées à la Régie le plus rapidement possible.

3.2. LA COLLECTE DE RENSEIGNEMENTS PERSONNELS

La personne à qui l'on demande un renseignement personnel doit être informée :

- du nom et de l'adresse de la Régie ;
- des fins pour lesquelles ce renseignement est recueilli ;
- des catégories de personnes qui auront accès à ce renseignement ;
- du caractère obligatoire ou facultatif de la demande ;
- des conséquences en cas de refus de répondre à la demande ;

- des droits d'accès et de rectification.

Un avis à cette fin doit être inclus dans tout formulaire de collecte de renseignements personnels, ou joint à celui-ci. Son contenu doit être approuvé par la Régie.

Lorsque votre contrat de service vous autorise à recueillir des renseignements personnels pour le compte de la Régie, vous ne pouvez le faire que si ces renseignements sont nécessaires au traitement du dossier de la personne concernée ou à l'exécution de votre contrat.

3.3. L'UTILISATION DES RENSEIGNEMENTS PERSONNELS AU SEIN DE LA RÉGIE

L'utilisation de renseignements personnels sans le consentement de la personne concernee est strictement encadrée.

- Seules les personnes préalablement autorisées par la Régie peuvent accéder aux renseignements personnels nécessaires à l'exercice de leurs fonctions, selon les accès qui leur sont attribués.

- Vous ne devez ni prendre connaissance ni utiliser les renseignements personnels détenus par la Régie, sauf lorsqu'ils sont nécessaires à l'exercice des fonctions et des tâches qui vous sont confiées.

- La curiosité ou l'intérêt personnel ne justifient pas la consultation ou l'utilisation de renseignements personnels.

- Les renseignements personnels détenus par la Régie doivent être à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été recueillis.

3.4. LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À UN TIERS

La communication de renseignements personnels à des tiers doit être préalablement approuvée par la Régie et respecter les exigences administratives et de sécurité fixées par la Régie.

3.5. LA CONSERVATION ET LA DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Les exigences de la Régie relatives à la conservation et à la destruction des documents sont indiquées dans votre contrat de service.

Vous ne pouvez pas utiliser à des fins personnelles des documents qui contiennent des renseignements personnels ou des informations confidentielles destinés à être jetés ou détruits. Le mode de destruction des documents contenant des renseignements personnels doit assurer la protection de la confidentialité.

Pour obtenir plus d'information, consultez le guide qui est joint à votre contrat de service.

3.6. L'UTILISATION DU TÉLÉCOPIEUR

La Régie déconseille l'utilisation du télécopieur pour la transmission des documents contenant des renseignements personnels. Toutefois, avant d'entreprendre une communication par télécopieur, il est nécessaire de :

- s'assurer que le destinataire est autorisé à obtenir les renseignements devant lui être communiqués ;
- indiquer visiblement le caractère confidentiel des renseignements ;
- bien vérifier le numéro du destinataire ;
- vérifier le rapport de transmission à la fin de la communication ;
- contacter en cas d'erreur la personne qui a reçu le document pour lui demander de le retourner par la poste et l'aviser qu'elle ne peut reproduire, diffuser ou utiliser autrement le contenu du document, sous peine de sanction.

4. CONSÉQUENCES DU NON-RESPECT DE CES RÈGLES

Le non-respect de ces règles constitue un manquement aux obligations de confidentialité du consultant.

Un bris de confidentialité résultant du non-respect de ces règles aurait des conséquences néfastes pour la Régie. Il en aurait aussi pour le consultant, qui s'exposerait à des poursuites civiles, voire pénales, dans le cas d'un bris intentionnel, en plus d'autres conséquences prévues au contrat.

Régie du logement
Québec

Directive de sécurité	
Objet	**Collecte, utilisation, conservation et destruction des informations confidentielles**
Approbation	**Comité de direction**
Date d'approbation	**21-06-2013**
Mise à jour	

PREAMBULE

Dans l'accomplissement de sa mission, la Régie du Logement, ci-après nommé « RDL », doit maintenir auprès du public l'image d'impartialité essentielle à tout tribunal, et maintenir la relation de confiance qu'elle a établie auprès des citoyens et des entreprises. Ces objectifs reposent sur l'engagement du personnel à adopter un comportement respectueux et exemplaire en matière de protection des renseignements personnels qui va au-delà de la simple application de la loi.

Bien que les renseignements personnels obtenus par la RDL dans l'exercice de sa fonction juridictionnelle ne sont pas confidentiels, sauf s'ils sont obtenus alors que la Régie siége à huis-clos, ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion, la RDL s'engage néanmoins à protéger l'information qu'elle détient.

1 CHAMP D'APPLICATION

Cette directive vise tous les documents et renseignements détenus par la RDL. Tous les membres du personnel de la Régie doivent s'y conformer.

2 CADRE JURIDIQUE

Loi sur la Régie du logement (L.R.Q., chapitre R-8.1);

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., C.A-2.1 ;

La Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou un support informatique amovible[1].

3 DEFINITIONS

Renseignement personnel
Tous les renseignements qui concernent une personne et qui permettent de l'identifier. Sont notamment considérés comme des renseignements personnels l'adresse, le numéro de téléphone, le numéro d'assurance sociale, le dossier médical, le statut social.

Document confidentiel
Document qui contient des renseignements personnels.

Document à caractère public
Les documents qui ne contiennent pas des renseignements personnels, ainsi que tout document ou renseignement personnel qui a un caractère public en vertu de la loi.

4 RENSEIGNEMENTS PERSONNELS CONFIDENTIELS

Tout renseignement personnel est confidentiel sauf lorsque la personne concernée par ce renseignement consent à sa divulgation ou lorsque sa communication est autorisée par la loi.

4.1 Accès aux renseignements personnels

Seul un membre du personnel de la RDL à qui un renseignement personnel est nécessaire à l'exercice de ses fonctions peut avoir accès à un tel renseignement.

4.2 Utilisation des renseignements personnels

Il faut utiliser les renseignements personnels aux seules fins prévues par la loi, dans l'exercice des fonctions et selon la responsabilité professionnelle ; ne jamais utiliser ces renseignements à des fins personnelles.

4.3 Protection des renseignements personnels

Tous les membres du personnel de la RDL doivent prendre des mesures raisonnables de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués ou détenus par la RDL.

[1] En vigueur depuis le 19 octobre 1999.

4.4 Communication d'un renseignement personnel

Il ne faut pas communiquer, utiliser ou permettre que soit communiqué ou utilisé tout renseignement personnel, autrement que dans la mesure prévue par la loi.

4.5 Communication d'un renseignement personnel sans consentement

Un renseignement personnel peut être communiqué sans le consentement de la personne concernée en vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un danger imminent de mort ou de blessures graves menace une personne ou un groupe de personnes identifiables[2].

4.6 Demande d'accès à un document ou un renseignement personnel

Toute demande d'accès à un document ou à un renseignement personnel est reçue et analysée, conformément aux dispositions de la loi applicables, par le responsable de l'accès aux documents et à la protection des renseignements personnels désigné par le président de la RDL.

4.7 Perte ou vol de renseignements personnels

En cas de perte ou vol de renseignements personnels, référez vous à la directive de sécurité interne « *Perte ou vol de renseignements personnels* »

5 DESTRUCTION DE DOCUMENTS CONFIDENTIELS

Le service de gestion documentaire est responsable de la destruction des documents confidentiels sous réserve des délais prévus au calendrier de conservation des documents de la RDL.

Cette responsabilité est partagée. Chaque employé, à son poste de travail, est responsable d'assurer la protection des documents confidentiels qu'il traite. Il ne doit pas jeter au rebut les documents sur support papier ou sur support électronique (disquette, carte de mémoire flash, CD-ROM, rubans magnétiques, ...) qui contiennent des renseignements personnels, sans s'être assuré au préalable que leur contenu ne peut être reconstitué.

La destruction de ces documents peut se faire dans l'unité administrative avec les moyens appropriés (par exemple déchiqueteuse) dans le cas de destruction de petites quantités de documents.

Les unités ayant un grand volume de documents sur support papier doivent faire une demande à la direction générale de l'administration qui prendra les mesures nécessaires pour assurer la destruction sécuritaire des documents (ex. : location d'équipement, engagement de personnel).

Les documents sur support électronique doivent être acheminés séparément au service des ressources informationnelles qui s'assure de leur destruction selon un mode approprié.

---

[2] Voir les détails dans la « Directive sur la communication de renseignements confidentiels en vue d'assurer la protection des personnes»

6 ROLES ET RESPONSABILITES

6.1 Le Président

Le président est responsable de la présente directive.

6.2 Le personnel de la RDL

Tous les membres du personnel doivent respecter et appliquer les règles énoncées et signaler tout comportement qui va à l'encontre du contenu de la directive.

6.3 Le gestionnaire

S'assure d'informer le personnel de cette directive et de faciliter son application en garantissant le support nécessaire auprès du personnel de la RDL.

6.4 Le Service des ressources informationnelles

S'assure que l'information est détruite avant que le support éléctronique ne soit acheminé à la réparation, au recyclage ou au rebut. Si toutefois le support doit être détruit, il faut appliquer le mode approprié de destruction sécuritaire à chaque support.

Référez vous à la directive gouvernementale «*Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou sur un support informatique amovible*».

7 CONTROLE DE L'APPLICATION DE LA DIRECTIVE

7.1 Sanctions

Tout employé(e) qui enfreint les dispositions de la présente directive s'expose à des mesures administratives ou disciplinaires, en fonction de la gravité et des conséquences du geste, conformément aux dispositions des lois, conventions collectives et contrats de travail en vigueur.

7.2 Entrée en vigueur de la directive

La présente directive entre en vigueur le jour de son approbation.

Régie du logement
Québec

Directive de sécurité

Objet	**Perte ou vol de renseignements personnels**
Date d'approbation	21-06-2013
Mise à jour	

Préambule

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* impose aux organismes publics des obligations en ce qui a trait à la collecte, à la conservation, à l'utilisation et à la communication des renseignements personnels.

En règle générale, les renseignements personnels qu'une entreprise ou un organisme détient sont confidentiels, sauf exceptions prescrites par la loi. Les organismes et les entreprises ont l'obligation de prendre les mesures de sécurité propres à assurer la protection de ces renseignements personnels.

Des mesures de sécurité adéquates peuvent contribuer à limiter les risques d'utilisation ou de communication inappropriée de renseignements personnels. Toutefois, une perte ou un vol de ces renseignements personnels peut survenir et mettre en cause la confidentialité de l'information.

Lorsqu'une perte de renseignements personnels se produit, une des préoccupations de la RDL est d'éviter ou limiter le préjudice que les personnes concernées par les renseignements personnels peuvent subir.

Il est également essentiel que des mesures de sécurité adéquates soient prises afin d'éviter qu'un tel incident ne se reproduise plus.

Objectifs

Définir le cadre opérationnel à suivre au sein de la Régie du logement lorsqu'une perte ou un vol de renseignements personnels est constaté afin de limiter les préjudices et dommages pouvant résulter de la perte ou du vol de renseignements personnels.

Champ d'application

Tous les renseignements personnels ou les documents confidentiels détenus par la Régie.

Tous les membres du personnel de la Régie, son président ainsi que les gestionnaires doivent se conformer à cette directive.

Responsabilités

Président

Le président est responsable de la présente directive.

Employé(e)s

Chaque employé(e) est responsable d'assurer la protection des renseignements confidentiels ou personnels qu'il utilise dans le cadre de ses fonctions et doit immédiatement aviser son supérieur immédiat en cas de perte ou de vol de renseignements personnels.

Gestionnaire

Le gestionnaire doit s'assurer que les mesures de sécurité adéquates sont en place pour limiter les risques de perte ou de vol de renseignements personnels et aviser, le cas échéant, immédiatement le président et le responsable de l'accès.

Responsable de l'accès aux documents et de la protection des renseignements personnels

Le responsable de l'accès aux documents et de la protection des renseignements personnels de la RDL tient à jour cette politique et conseille toute personne sur son application.

Modalités

1- Dès que la perte ou le vol de renseignements personnels est constaté, tout employé doit en aviser immédiatement son supérieur immédiat.

2- Le supérieur immédiat doit sans délai informer le président de la Régie et le responsable de l'accès et de la protection des renseignements personnels.

3- Le président forme un comité pour gérer la situation lequel est formé du responsable de l'accès et de la protection des renseignements personnels, du gestionnaire responsable de l'unité administrative concernée, du responsable des communications et d'un conseiller juridique.

4- Le comité doit procéder à **une évaluation préliminaire de la situation**, notamment, en définissant sommairement le contexte de la perte ou du vol de renseignements personnels, soit :

- Identifier les renseignements personnels touchés ainsi que leur support ;
- Identifier les personnes, leur nombre ainsi que le groupe de personnes (clients, employés, etc.) touchées ;
- Établir le contexte des événements (date, heure, lieu, etc.) ;
- Identifier, si possible, les circonstances entourant la perte (cause, personnes susceptibles d'être impliquées dans l'incident, etc.) ;
- Répertorier les mesures de sécurité physiques et informatiques en place lors de l'incident ;
- Informer le service de police si les circonstances laissent croire à la possibilité d'un crime ;
- Aviser la Commission d'accès à l'information.

5- Le comité doit prendre sans tarder des mesures adéquates pour **limiter les conséquences pour les personnes concernées** d'une possibilité d'utilisation malveillante de leurs renseignements personnels, de l'usurpation ou du vol de leur identité, soit :

- Mettre fin à la pratique non-conforme, le cas échéant ;
- Récupérer les dossiers physiques ou numériques, selon le cas ;
- Révoquer ou modifier les mots de passe ou les codes d'accès informatiques ;
- Contrôler les lacunes dans les systèmes de sécurité.

6- Le Comité doit **évaluer les risques** en :

- Complétant une évaluation préliminaire des risques, en considérant la sensibilité des renseignements personnels en cause, tenant compte de leur nature, leur quantité, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc. ;
- Déterminant le contexte de l'incident incluant :
  - La cause (ex : le caractère délibéré ou non de la perte ou du vol de renseignements personnels, l'erreur humaine, une faille informatique, etc.) ;
  - Les auteurs connus ou probables des renseignements personnels perdus ou subtilisés (ex. organisation criminelle, public en général, etc.) ;
  - L'étendue de la situation (nombre de personnes touchées et secteurs touchés) ;
  - Le caractère systémique ou non de la disparition des renseignements personnels (particulièrement lorsque la perte n'est pas générée directement par une intervention humaine) ;
  - Une évaluation de la probabilité qu'un événement similaire se reproduise.
- Évaluant la possibilité que les renseignements personnels concernés fassent l'objet d'une utilisation préjudiciable pour les personnes concernées en tenant compte, notamment, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.) ;
- Évaluant le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels ;
- Évaluant si les mesures immédiates prises étaient adéquates pour limiter l'atteinte et les compléter si nécessaire ;
- Déterminant les préjudices potentiels, notamment en évaluant les possibilités d'utilisation future des renseignements personnels par des personnes malveillantes, notamment pour le vol d'identité ;
- Déterminant les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.

7- Le comité doit **aviser les organisations et personnes concernées** par la perte ou le vol de renseignements personnels. Pour ce faire, il doit déterminer qui doit être mis au courant de la perte ou du vol de renseignements personnels en fonction de l'évaluation des risques :

- **Service de police :** dans les cas où la disparition peut résulter de la commission d'un crime, le service de police concerné doit être avisé des éléments entourant cette disparition tout d'abord et, ensuite, de toutes les démarches subséquentes. Il est nécessaire de porter une attention particulière afin de ne pas nuire à l'enquête et de préserver les éléments de preuve pouvant être pertinents ;

- **Personnes concernées :** si la perte ou le vol de renseignements personnels présente un risque de préjudice pour les personnes concernées, celles-ci devraient en être avisées sans tarder. Il ne s'agit pas d'alarmer mais de prévenir afin de leur permettre de prendre les mesures pertinentes pour protéger leurs renseignements personnels (Voir annexe : *AVIS AUX PERSONNES CONCERNÉES PAR UNE PERTE OU UN VOL DE LEURS RENSEIGNEMENTS PERSONNELS*) ;

- **Commission d'accès à l'information :** si les personnes concernées par les renseignements personnels proviennent du Québec, la Commission pourrait amorcer une inspection ou une enquête et jouer un rôle de conseiller dans la recherche de solutions ;

- **Autres :** il peut également être nécessaire d'aviser d'autres intervenants, tels que les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc.

Toutefois, dans la diffusion des informations concernant la perte de renseignements personnels, une attention particulière doit être portée afin de ne pas aggraver le préjudice que pourraient subir les personnes concernées (ex : limiter au minimum les renseignements personnels dans les avis).

- Il doit également désigner les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone) et le cas échéant, identifier et consigner les motifs à l'origine de la décision de ne pas aviser les personnes concernées et les autres intervenants.

8- Le comité doit faire un rapport sur la perte ou le vol de renseignements personnels en :

- Approfondissant l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuant une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés ;

- Répertoriant et examinant les normes, politiques ou directives internes en place au moment de l'incident, autant au niveau de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels en général ;

- Vérifiant si ces normes ou directives internes ont été suivies par les personnes impliquées ; identifiant les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant ;

- S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, adapter les processus pour éviter qu'un tel incident ne survienne à nouveau ;

- Formuler les recommandations relatives aux solutions à moyen et long terme et aux stratégies de prévention et prévoir le suivi devant être accordé.

Contrôle de l'application de la directive

Approbation de la directive

La présente directive a été approuvée par le président de la Régie du logement, Me Luc Harvey, le 21-06-2013.

Entrée en vigueur de la directive

La présente directive entre en vigueur le jour de son approbation.

Annexe

AVIS AUX PERSONNES CONCERNÉES PAR UNE PERTE OU UN VOL DE LEURS RENSEIGNEMENTS PERSONNELS

Selon les circonstances, il pourrait s'avérer nécessaire d'aviser les personnes victimes de la perte ou du vol de leurs renseignements personnels. Cet avis pourrait inclure certains des éléments suivants :

- Le contexte de l'incident et le moment où il s'est produit ainsi qu'une description de la nature des renseignements personnels touchés ou potentiellement touchés, sans dévoiler de renseignements personnels spécifiques ;
- Une description sommaire des mesures prises afin de limiter ou de prévenir tout préjudice, ainsi que la liste des personnes qui ont été informées de la situation (Service de police, Commission d'accès à l'information, etc.) ;
- Les actions prises par la Régie du logement pour aider les personnes concernées (Service d'aide et d'information, etc.) ;
- Les mesures que les personnes concernées peuvent prendre afin de réduire les risques de préjudice ou pour mieux se protéger ;
- Documents d'informations générales conçus pour aider les personnes à se prémunir contre le vol d'identité ;
- Les coordonnées d'un interlocuteur de la Régie du logement qui peut répondre aux questions et à qui il est possible d'effectuer tout signalement ;
- Les principales mesures qui seront prises pour éviter que la situation ne se reproduise (changement de pratique ou de processus, formation du personnel, révision ou élaboration de politiques, vérification, suivi périodique, etc.).

Régie du logement Québec

Directive

Objet	Directive sur la communication de renseignements confidentiels en vue d'assurer la protection des personnes
Date	30 janvier 2018

Mise à jour de la directive déposée le 24 septembre 2012

1. Objet

La présente directive a pour objet d'établir, conformément aux dispositions du dernier alinéa de l'article 59.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1), les conditions et les modalités selon lesquelles peuvent être communiqués des renseignements personnels en vue de prévenir un acte de violence, dont un suicide.

2. Champ d'application

La directive s'applique à tout le personnel de la Régie du logement, y compris le président, la vice-présidente et le personnel d'encadrement.

3. Conditions

Un organisme public peut communiquer un renseignement personnel, sans le consentement des personnes concernées, en vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence.

Motif raisonnable : la menace doit reposer sur des faits objectifs. Une personne raisonnable ayant à juger de la même situation devrait également conclure à l'existence d'un risque sérieux de mort ou de blessures graves.

Risque sérieux : la nature de la menace doit inspirer un sentiment d'urgence, notamment en raison de sa gravité et de sa clarté. La notion d'urgence n'exige pas qu'un délai précis soit fixé pour la perpétration de l'acte appréhendé.

Blessures graves : toute blessure physique ou psychologique qui nuit d'une manière importante à l'intégrité physique, à la santé ou au bien-être d'une personne ou d'un groupe de personnes identifiable. La notion de violence inclut, dans le présent cas, celle d'une personne envers elle-même, et donc le suicide.

Personne ou groupe de personnes identifiables : il n'est pas nécessaire que la personne visée soit identifiée par son nom. Les faits doivent cependant permettre d'identifier la personne ou le groupe visé.

4. Évaluation

L'évaluation de la menace doit reposer sur des faits objectifs analysés selon les circonstances propres à chaque situation.

Le membre du personnel qui a un motif raisonnable de croire à l'existence d'un risque sérieux visant une personne ou un groupe de personnes identifiable, ou qui s'interroge sur l'existence d'un tel risque, doit communiquer le plus rapidement possible avec le membre de garde du service juridique afin que l'évaluation de la menace soit complétée et qu'une intervention appropriée soit assurée, le cas échéant.

En cas d'incapacité à joindre le membre de garde du service juridique, le membre du personnel doit communiquer avec son supérieur immédiat ou, à défaut, avec le bureau de la direction.

5. Communication

Les renseignements peuvent être communiqués à la ou aux personnes visées par la menace, à leur représentant ou à toute personne susceptible de leur porter secours.

Les ressources susceptibles de porter secours aux personnes menacées sont notamment les services de police. Le représentant d'une personne en danger peut être un parent. S'il s'agit d'un groupe, ce peut être, s'il existe, le dirigeant du groupe.

Seuls peuvent être communiqués les renseignements nécessaires à la prévention de l'acte de violence appréhendé. Ce sont, notamment, l'identité de la personne en danger, l'identité et les coordonnées de celle qui a proféré les menaces, ainsi que la nature de ces dernières et les circonstances dans lesquelles elles ont été proférées.

6. Registre des communications

Le membre du service juridique où, à défaut, la personne ayant communiqué les renseignements en avise le responsable de l'accès aux documents et de la protection des renseignements personnels par le biais du formulaire annexé à la présente directive.

Le responsable de l'accès aux documents et de la protection des renseignements personnels doit alors inscrire la communication dans un registre confidentiel conformément à l'article 60.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1).

7. Entrée en vigueur

La présente directive entre en vigueur le jour de sa signature par le président de la Régie.

Le président,

Patrick Simard

30 janvier 2018

REGISTRE TENU CONFORMÉMENT À LA DIRECTIVE SUR LA COMMUNICATION DE RENSEIGNEMENTS CONFIDENTIELS EN VUE D'ASSURER LA PROTECTION DES PERSONNES EN PRÉVENANT UN ACTE DE VIOLENCE

(ARTICLE 60.1 DE *LA LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, RLRQ, chapitre A-2.1*)

1. Date de l'événement :

2. Description du danger et des circonstances de l'événement :

3. Nom de la ou des personnes en danger :

4. Renseignements communiqués :

5. Nom du membre du personnel qui a communiqué les renseignements :

6. Nom de la personne à laquelle les renseignements ont été communiqués:

Renseignements transmis à :
Madame Josée Corbeil
Responsable de l'accès aux documents et de la protection des renseignements personnels
Régie du logement

Politique cadre sur la protection des renseignements personnels

TABLE DES MATIÈRES

Section I : Dispositions générales

1. Objet de la politique

La présente politique a pour objets :

D'assurer la confidentialité de l'information, lorsque requis, et l'accessibilité aux actifs informationnels limitée aux seules personnes habilitées dans le cadre de l'exercice de leurs fonctions; D'assurer l'intégrité des actifs informationnels; D'assurer la continuité des services.

2. Champ d'application

La présente politique s'applique aux actifs informationnels détenus par la Régie.

Cette politique s'adresse à tous les détenteurs des actifs informationnels, les utilisateurs de l'informatique, et les gestionnaires de la Régie.

3. Préalables

Politiques de la Régie du logement :

Politique sur l'accès et la protection de l'information; * Politique sur l'utilisation des réseaux électroniques, d'Internet et du courrier électronique.

Lois, règlements, directives et guide émanant du Gouvernement (liste non exhaustive)

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1); Loi sur les archives (L.R.Q., c. A-21.1); Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale;
Guide de gestion de la sécurité sur le RICIB. Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou un support informatique amovible. (CT 193953 du 19 octobre 1999)

4. Définitions

Dans cette politique, on entend par :

Actif informationnel : Banque de données, système d'information, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitué par la Régie.

Administrateur de la sécurité d'accès : Personne responsable de la gestion des codes d'identité et des règles d'accès.

Authentification : Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

Banque de données : Collection d'information relative à un domaine défini, regroupée et organisée de façon à en permettre l'accès.

Classification des actifs informationnels : Action de répartir les actifs informationnels en fonction de leur valeur administrative, légale, patrimoniale et économique et des impacts pouvant découler d'une atteinte à leur sécurité.

Confidentialité : Caractère des informations dont la diffusion doit être limitée aux seules personnes ou entités habilitées dans le cadre de l'exercice de leurs fonctions.

Continuité : Action visant à s'assurer que les opérations puissent se poursuivre en dépit de l'occurrence d'événements contraignants ou dommageables.

Détenteur : Personne à qui est assignée par délégation, la responsabilité de détenir un actif informationnel pour l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion.

Disponibilité : Propriété d'une information ou d'une technologie de l'information d'être accessible et utilisable en temps voulu et de la manière requise par une personne ou entité autorisée.

Fournisseur : Toute personne de l'extérieur de la Régie qui fournit des services à un détenteur ou un utilisateur.

Information : Information sous toute forme (textuelle, symbolique, sonore ou visuelle), dont l'usage l'accès, l'emmagasinage, le traitement et la communication n'est possible qu'au moyen de technologies de l'information.

Installation : Ensemble des objets, appareils, bâtiments et autres installés en vue de l'usage d'une technologie de l'information.

Intégrité : Propriété d'une information ou d'une technologie de l'information de n'être ni modifiable, ni altérable, ni destructible sans autorisation.

Irrévocabilité : Propriété d'un acte d'être définitif et qui est clairement attribué à la personne qui l'a posé ou au dispositif avec lequel cet acte a été accompli.

Micro-ordinateur en mode autonome : Micro-ordinateur qui n'est pas relié à d'autres ordinateurs ou qui est relié mais fonctionne de façon autonome.

Plan de reprise : Description intégrale des activités à réaliser, des ressources humaines, matérielles et financières à mobiliser et des procédures à suivre avant, pendant et après qu'une atteinte à la sécurité des opérations se soit produite et que cette atteinte rende pleinement ou partiellement inopérante la capacité de traitement d'un service informatique. Le terme "relève" est parfois utilisé par des intervenants pour désigner "reprise".

Registre d'événements : Recueil relatant les événements ayant mis en péril la sécurité de l'information et des technologies de l'information.

Système d'information : Ensemble organisé de moyens mis en place pour recueillir, traiter, stocker, communiquer et éliminer l'information en vue de répondre à un besoin déterminé, incluant notamment les technologies de l'information et les procédés aménagés pour accomplir ces fonctions.

Technologie de l'information : Tout logiciel, matériel électronique ou combinaison de ces éléments utilisé pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer de l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

Utilisateur : Toute personne dans une unité administrative ou à l'extérieur de la Régie qui utilise l'informatique pour colliger, traiter, stocker, accéder, transférer, détruire ou conserver les informations nécessaires à l'accomplissement de la mission de la Régie.

Section II : Gestion de la sécurité informatique

5. Principe général

La Régie reconnaît que les actifs informationnels sont vitaux pour le fonctionnement de son organisation. En conséquence, des mesures de prévention, de détection et de correction doivent être planifiées, appliquées et suivies en tenant compte des actifs informationnels à protéger et des coûts reliés à ces mesures.

6. Principes directeurs

6.1 Responsabilités générales

La coordination requise pour l'élaboration, la mise en place, le suivi et l'évaluation de politiques et procédures, de plans et, s'il y a lieu, de mesures partagées de sécurité est sous la responsabilité d'un responsable de la sécurité de l'information. La gestion des codes d'identité et des règles d'accès aux systèmes est confiée aux administrateurs de la sécurité d'accès. Pour toutes les applications décentralisées, (SAGIP, SYGBEC, ...) les utilisateurs ou les détenteurs sont responsables de la sécurité informatique dans la mesure de leurs moyens. Pour tous les autres cas, le service des Systèmes assume la responsabilité de la sécurité informatique. Tout problème concernant l'intégrité ou la continuité

ainsi que ses causes et conséquences connues doit être signalés au responsable de la sécurité de l'information. Seul le service des Systèmes peut faire l'installation des équipements et des logiciels. Il peut cependant déléguer cette responsabilité.

6.2 Planification de la sécurité informatique

Un programme de sécurité informatique doit être élaboré annuellement. Un programme de formation et de sensibilisation pour les gestionnaires et les utilisateurs doit être mis au point et entretenu. Un classement des actifs informationnels doit être effectué et maintenu à jour. Un plan de reprise des services doit être mis au point et entretenu.

6.3 Application et suivi des mesures de sécurité informatique

L'application des mesures de sécurité informatique doit être assumée dès les études et analyses pouvant conduire à l'acquisition ou à la constitution d'un actif informationnel, pendant toute la durée de son utilisation et de sa conservation et jusqu'à son aliénation ou son élimination inclusivement. Plus précisément, la sécurité porte notamment mais non exclusivement sur les points suivants : la protection physique des actifs informationnels;
la protection des voies d'accès logique aux actifs informationnels de façon à ne permettre l'accès qu'aux personnes habilitées et en fonction des seuls droits qui leur sont reconnus; le bon fonctionnement des équipements informatiques, afin de prévenir les risques d'arrêts fortuits et, le cas échéant, d'assurer la reprise et le rétablissement des services; l'utilisation restreinte des renseignements personnels ou confidentiels; l'archivage ou l'élimination des actifs informationnels. Des mécanismes de suivi de gestion et de contrôle doivent être mis en place, tant à l'égard de l'élaboration et de l'implantation des mesures que de leur application systématique et continue.

7. Directives

7.1 Responsabilités générales

Des responsabilités générales touchant la sécurité informatique sont dévolues aux intervenants suivants :

La présidente doit :

nommer le responsable de la sécurité de l'information (anciennement RSGS) pour assurer la coordination de la sécurité; adopter les orientations et les solutions recommandées concernant les problèmes de la sécurité informatique; nommer les administrateurs de la sécurité d'accès; assurer la sécurité de l'information par une gestion adéquate des risques et de leurs impacts sur la disponibilité, l'intégrité et la confidentialité d'une information ainsi que de l'authentification et l'irrévocabilité d'un acte; assurer la gestion de la sécurité en : prenant les moyens nécessaires pour la mise en œuvre du plan de sécurité (leadership); obtenant l'adhésion à une vision et une compréhension commune de la sécurité; ayant une approche globale et intégrée de la sécurité qui tiennent compte des aspects humains, organisationnels, techniques et juridiques (cohérence); attribuant des responsabilités claires à tous les niveaux de l'organisation; mettant en place des mécanismes de coordinations et de contrôle permettant une reddition de compte adéquate (imputabilité); réévaluant périodiquement les solutions techniques retenues (adaptabilité); retenant des solutions techniques reconnues (universalité).

Le Comité de protection des renseignements personnels 1 doit :

assurer le suivi des actions pour se conformer aux recommandations formulées par la CAI; planifier, initier et de voir à la tenue d'activités régulières de sensibilisation auprès de tout le personnel, sur tous les volets de la protection des renseignements personnels; procéder à une évaluation annuelle du niveau de protection des renseignements personnels et en faire état dans le rapport annuel de la Régie.

Le Comité sur la sécurité de l'information doit :

définir clairement les valeurs organisationnelles, les faire partager par l'ensemble du personnel et les communiquer aux partenaires de l'organisation pour s'assurer qu'elles soient respectées; établir les politiques, les orientations et les réviser périodiquement; instaurer un mécanisme continu d'identification et d'évaluation des risques encourus ainsi que l'adéquation des mesures en vigueur par rapport à ces derniers; établir et actualiser une architecture-cible de sécurité et élaborer un plan des mesures à mettre en œuvre; attribuer formellement la responsabilité de l'information à des détenteurs élaborer les contrats et ententes de services auxquels ils sont partie de manière à garantir le respect des exigences de sécurité; assurer aux informations qu'ils reçoivent d'autres ministères ou organismes un degré de sécurité au moins équivalent à celui dont ils bénéficiaient à l'origine et s'assurer que les informations qu'ils transmettent à un tiers bénéficient du même degré de sécurité que celui qui leur est appliqué à la Régie; sensibiliser systématiquement l'ensemble du personnel et assurer sa formation; mettre en place des mécanismes d'évaluation et de contrôle impliquant des personnes indépendantes; tenir à jour un registre des événements ayant pu mettre en péril la sécurité et les documenter; produire un bilan annuel de sécurité conformément aux instructions du

Secrétariat du Conseil du trésor.

Le responsable de la sécurité de l'information doit :

planifier des mesures, des règles et des mécanismes de contrôle de sécurité nécessaires; élaborer des politiques et des procédures administratives appropriées avec la participation du service des Systèmes; coordonner l'application et le suivi du programme annuel et des mesures de sécurité; recommander des solutions aux problèmes de sécurité informatique en collaboration avec le service des Systèmes et les personnes concernées.

Le service des Systèmes doit :

supporter l'application des mesures de sécurité en mode de gestion décentralisée, et appliquer et faire respecter toutes autres mesures de sécurité; identifier et évaluer les solutions aux problèmes de la sécurité informatique; informer le responsable de la gestion de la sécurité de l'information de tout problème concernant l'intégrité des données, l'interruption de services ainsi que les causes et conséquences.

Le supérieur immédiat doit :

gérer la protection des actifs informationnels sous sa responsabilité; appliquer et faire respecter les mesures de sécurité en vigueur; sensibiliser ses employés à protéger les actifs informationnels; voir à ce que tout fournisseur de services respecte les règles de sécurité informatique de la Régie, tel que stipulé dans les ententes de services.

7.2 Planification de la sécurité informatique

Le programme de sécurité informatique est composé d'un bilan annuel qui permet de poser un diagnostic sur l'efficacité des mesures en place, d'ajuster les objectifs ou d'en formuler de nouveaux et d'un plan d'action pour l'année à venir. Ce programme doit notamment mais non exclusivement s'appuyer sur les éléments suivants :

une évaluation et un suivi des mesures qui ont déjà été mises en place; une évaluation des risques encourus par la Régie; un bilan des manquements; les recommandations des vérificateurs.

Le classement des actifs informationnels doit être fait en fonction de leur valeur administrative, légale, patrimoniale et économique ainsi que des impacts pouvant découler d'une atteinte à leur sécurité.

En regard de la planification de la sécurité informatique, des responsabilités précises sont dévolues aux intervenants suivants :

La présidente doit :

approuver le programme et le budget de la sécurité informatique ainsi que le programme de sensibilisation et le plan de reprise.

Le responsable de la sécurité de l'information doit :

élaborer le programme annuel de sécurité informatique; élaborer, entretenir et diffuser le programme de sensibilisation de la sécurité informatique destiné au personnel, aux mandataires, aux fournisseurs et aux organismes externes; coordonner le classement des actifs informationnels en collaboration avec le responsable de la Loi sur l'accès, le service des Systèmes et les détenteurs.

Le service des Systèmes doit :

élaborer et tenir à jour un processus de classement des actifs informationnels avec la collaboration du responsable de la sécurité de l'information et des détenteurs.

Le détenteur doit :

classer les actifs informationnels qu'il détient.

7.3 Application et suivi des mesures de sécurité informatique

Concernant les analyses d'impacts sur la sécurité informatique

Une analyse doit être réalisée avant de décider d'utiliser toute nouvelle technologie de l'information ou toute nouvelle utilisation d'une technologie déjà en place. Un choix de mesures de sécurité appropriées doit être fait à la lumière de cette analyse.

Des responsabilités incombent aux intervenants suivants :

Le responsable de la sécurité de l'information doit :

s'assurer de la réalisation d'une analyse d'impacts avant l'implantation d'une nouvelle technologie ou d'une nouvelle utilisation d'une technologie déjà en place.

Le service des Systèmes doit :

réaliser une analyse d'impacts sur la sécurité avant de décider d'utiliser toute nouvelle technologie d'information ou d'une utilisation nouvelle d'une technologie déjà en place, excluant celles prévues à l'article qui suit.

Le supérieur immédiat doit :

évaluer les impacts sur la sécurité avant de décider de l'utilisation nouvelle d'une technologie déjà en place, lorsqu'il s'agit de systèmes à gestion décentralisée.

Concernant la protection physique des actifs informationnels de même que la protection des voies d'accès logique

L'accès à l'actif informationnel est strictement limité aux seules personnes habilitées dans le cadre de l'exercice de leurs fonctions, plus précisément, nul ne peut exploiter les données pour une personne qui n'en a pas reçu l'autorisation.

Des mesures, règles et mécanismes de suivi de gestion et de contrôle doivent être intégrés tout au long de la durée de vie des actifs informationnels, notamment par l'emploi de prises de copies de sécurité et de mots de passe.

Les équipements et les logiciels ne doivent être utilisés que pour l'accomplissement du mandat de la Régie.

Des responsabilités incombent aux intervenants suivants :

Le responsable de la sécurité de l'information doit :

s'assurer de la mise en place des plans, des mesures, des règles et des mécanismes de suivi de gestion et de contrôle.

Le service des Systèmes doit :

réaliser les activités prévues au programme annuel de la sécurité informatique; intégrer les mesures, règles et mécanismes de suivi de gestion et de contrôle; recevoir toute demande de changement des équipements informatiques et des logiciels en regard de chacun des postes de travail et procéder aux installations en conformité avec l'ensemble des règles et des principes de sécurité en vigueur à la Régie; prendre des copies de sécurité de l'information selon une fréquence adaptée aux besoins; établir les critères de prises de copie de sécurité sur toutes les plates-formes; assurer l'entreposage à l'extérieur des locaux de la Régie des copies de l'ordinateur central, des serveurs des réseaux locaux, ainsi que de ce qui est transmis de la part des utilisateurs; fournir et gérer les outils nécessaires pour identifier les virus sur les ordinateurs de la Régie; tenir à jour un inventaire des équipements informatiques appartenant à la Régie; élaborer les procédures concernant les droits d'accès à la salle d'ordinateur et le lieu d'entreposage des fournitures informatiques et contrôler leur accès; gérer et contrôler les cartes d'accès de la salle d'ordinateur.

Le supérieur immédiat doit :

définir et autoriser aux utilisateurs uniquement les accès requis aux actifs informationnels nécessaires à l'exercice de leurs fonctions; lors d'un départ, récupérer la carte, les clefs et tout le matériel mis à la disposition de l'employé concerné; aviser les administrateurs de la sécurité d'accès de tout départ, absence prolongée ou transfert d'un employé dans une autre unité administrative; voir à la prise régulière de copies de sécurité; soumettre au service des Systèmes toute demande de changement des équipements informatiques et des logiciels en regard des postes de travail.

Les administrateurs de la sécurité d'accès doivent :

élaborer des procédures et des règles d'accès en collaboration avec le responsable de la sécurité de l'information; prendre action en regard des départs, absences prolongées ou transferts des employés qui lui sont signalés; émettre et annuler les codes d'utilisateur; contrôler les accès effectués par les utilisateurs.

Le Service des ressources matérielles doit :

assurer le maintien d'un état de situation des mesures de protection en place dans chacun des bureaux et proposer, au besoin, des règles particulières visant l'accès à certains locaux; gérer la protection des locaux contenant de l'équipement informatique contre les actes de vandalisme, le feu, le vol, etc.; s'assurer de la disponibilité d'un lieu d'entreposage externe des copies de sécurité.

L'utilisateur doit :

se conformer aux règles en sécurité informatique, notamment: clore sa session de travail dès qu'il quitte son poste de travail et garder confidentiel son mot de passe; assurer la protection des actifs informationnels qui lui sont assignés; se servir des équipements et des logiciels de la Régie uniquement pour l'accomplissement de son mandat; accéder uniquement à l'information dont il a besoin pour accomplir sa tâche; prendre des copies de sécurité de l'information en mode de gestion décentralisée selon une fréquence adaptée à ses besoins mais qui en cas de perte irrécupérable ne devrait pas dépasser plus de trois jours de travail.

L'utilisateur ne doit pas :

interroger des données réelles à d'autres fins que celles de son travail ni pour un autre utilisateur, à moins qu'une autorisation n'ait été donnée ou qu'une procédure ne le prévoit expressément; modifier les logiciels et le matériel mis à sa disposition; installer des logiciels qui n'ont pas été acquis par la Régie; copier pour son utilisation personnelle les logiciels installés.

Concernant la reprise et le rétablissement des services :

Des essais de systèmes doivent être faits périodiquement. En cas de pannes, de bris ou autres événements semblables, la reprise et le rétablissement des services doivent se faire dans les délais prescrits.

Des responsabilités incombent aux intervenants suivants :

La présidente doit :

déclencher, si nécessaire, le processus de reprise à la suite d'un sinistre.

Le responsable de la sécurité de l'information doit :

coordonner la mise en place et le fonctionnement du plan de reprise.

Le service des Systèmes doit :

effectuer, des essais de systèmes; établir des barèmes pour les délais lors de reprise; mettre au point, entretenir et assurer le fonctionnement des opérations informatiques au centre de reprise.

Le supérieur immédiat doit :

voir à la réalisation des essais ainsi que la reprise des systèmes essentiels qui le concernent.

Le Service des ressources matérielles de même que le Service des ressources financières doivent :

s'assurer de la disponibilité des instruments, des locaux et des fournitures requis pour les essais ainsi que la reprise des activités des systèmes essentiels.

Concernant l'utilisation restreinte des renseignements personnels ou confidentiels

Des responsabilités incombent à l'intervenant suivant :

Le détenteur doit :

s'assurer que les données qui concernent une personne physique et permettent de l'identifier ainsi que celles qui ont un caractère confidentiel ne puissent être utilisées à des fins de présentation, d'essais de système et de formation (sauf pour les cas ou il est impossible de faire autrement)et avec l'autorisation du supérieur immédiat; s'assurer de détruire les données ainsi utilisées de façon sécuritaire.

Concernant l'archivage ou l'élimination des actifs informationnels

La Régie ne doit colliger et conserver que l'information nécessaire à l'accomplissement de son mandat. Toute information désuète ou inutile doit être détruite.

Des responsabilités incombent aux intervenants suivants :

Le service des Systèmes doit :

élaborer et exécuter les procédures d'archivage ou d'élimination et de gestion des actifs informationnels pour l'ordinateur central et les serveurs des réseaux locaux.

Le supérieur immédiat doit :

voir à exécuter les procédures d'archivage ou d'élimination et de gestion des actifs informationnels relativement aux micro-ordinateurs en mode autonome; voir à appliquer les délais de conservation prévus au «calendrier de conservation de la Régie du logement».

Concernant la destruction des actifs informationnels déclarés bien meubles excédentaires

La Régie doit se conformer à la Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou un support informatique amovible (CT 193953 du 19 octobre 1999). Cette directive détermine les règles applicables au traitement et à la destruction de toute information emmagasinée :

sur un ordinateur déclaré bien meuble excédentaire par la Régie; sur un support informatique amovible, utilisé par le personnel de la Régie; sur un ordinateur ou sur un support amovible, confié à un fournisseur de service par la Régie.

Dans cette directive les responsabilités qui incombent aux différents intervenants sont clairement définies et ne seront pas reprises ici. Pour plus de renseignements, consulter le recueil des politiques de gestion volume 11, chapitre 2, sujet 2, pièce 3, émise le 23 décembre 1999.

Section III : Dispositions finales

8. Responsabilités administratives

Le comité de sécurité de l'information et de la protection des renseignements personnels est responsable de l'élaboration, du suivi et de l'évaluation de cette politique. Il devra produire une évaluation de l'application de cette politique au plus tard 2 ans après son adoption.

9. Dispositions générales de la politique

À moins d'une disposition expresse à l'effet contraire dans la présente politique, les dispositions suivantes s'appliquent.

Les titres utilisés dans la présente politique ne le sont qu'à des fins de référence et de commodité seulement. Ils n'affectent en rien la signification ou la portée des dispositions qu'ils désignent.

En tout temps et sans préavis, la présente politique peut être modifiée ou annulée, à la discrétion de la Régie.

Tous les mots et termes employés dans la présente politique doivent s'interpréter comme comprenant le masculin et le

féminin, ainsi que le singulier et le pluriel, suivant le contexte ou le sens de cette politique.

La présente politique s'ajoute à toutes les autres politiques de la Régie du logement, ainsi qu'à toutes les directives, normes et méthodes émises par celle-ci. Elle n'a nullement pour effet de remplacer ou de se substituer à une ou plusieurs desdites autres politiques, directives, normes et méthodes, à moins d'indication contraire dans la présente politique.

10. Entrée en vigueur de la politique

La présente politique entre en vigueur le 31 mars 2000.

11. Durée d'application de la politique

La présente politique demeure en vigueur tant et aussi longtemps qu'elle n'a pas été abrogée ou encore modifiée ou remplacée par une autre politique.

Fermer