	POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DES SŒURS DU BON-PASTEUR DE QUÉBEC
	Instance responsable : Direction générale
	Adoptée par le Conseil général le 3 juillet 2024
	Entrée en vigueur le 3 juillet 2024
	Version officielle 1 (2024-07-03)

TABLE DES MATIÈRES

1. FONDEMENT

En 2020, le gouvernement du Québec a déposé le projet de loi n°64 pour moderniser la législation provinciale sur la protection des renseignements personnels. Cette loi s'applique aux organismes publics et aux entreprises privées établies au Québec ainsi qu'à toute entreprise ayant une présence numérique au Québec.

La loi 25 est une loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, la loi sur la protection des renseignements personnels dans le secteur privé, ainsi que plusieurs autres lois.

Sanctionnée le 22 septembre 2021, cette loi a pour objectif d'offrir un meilleur contrôle aux citoyens sur leurs renseignements personnels. Elle modernise le cadre législatif pour l'adapter à la réalité technologique d'aujourd'hui.

2. PRINCIPES

L'utilisation des renseignements personnels doit être adéquate et faire l'objet d'une protection en lien avec sa valeur. Les Sœurs du Bon-Pasteur de Québec reconnaissent détenir ou avoir sous leur responsabilité de tels renseignements, ce qui exige une vigie rigoureuse de l'organisation, puisqu'elle doit respecter plusieurs lois et règles particulières.

3. OBJECTIFS

La présente politique de protection des renseignements personnels est essentielle afin d'orienter l'organisation en matière de sécurité. Elle est le premier jalon d'un cadre de gestion de la sécurité de l'information. Elle établit notamment les mesures de sécurité logiques, physiques, humaines et organisationnelles à appliquer. De plus, elle détermine pour l'ensemble des utilisateurs les comportements à adopter afin de s'assurer de l'utilisation appropriée de ces renseignements personnels.

La protection des renseignements personnels s'articule autour de cinq grands axes, à savoir : *collecte, utilisation, communication, conservation* et *destruction*.

Cette politique sert de principal fondement et permet à l'organisation d'assurer le respect et la protection des renseignements personnels sous sa responsabilité tout au long des cinq grands axes de leur cycle de vie.

La présente politique vise à assurer :

- Le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère personnel relatifs aux religieuses, à la clientèle et aux personnes qui exercent leur fonction ou leur profession au sein de l'organisation;

- La sécurité de l'information au regard de l'utilisation des réseaux informatiques de

l'organisation, notamment l'Internet, l'infonuagique et le courrier électronique;

- La conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales;

- La mise en place d'une culture de sécurité de l'information, particulièrement par la sensibilisation et la responsabilisation accrue des utilisateurs quant aux risques et enjeux entourant l'utilisation de l'information.

4. CHAMP D'APPLICATION

Cette politique s'applique à toute personne physique ou morale dûment autorisée à avoir accès aux renseignements personnels détenus par les Sœurs du Bon-Pasteur de Québec, et ce, peu importe l'endroit où elle se trouve ou la localisation des renseignements personnels.

L'information visée par la présente politique est celle que l'organisation détient dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

Toutefois, cette politique ne s'applique pas aux renseignements détenus par un membre de l'organisation à des fins personnelles, même s'ils sont conservés dans les locaux ou sur une plateforme technologique de ladite organisation.

5. DÉFINITIONS

Voir les définitions présentées à l'***Annexe 1***.

6. MODALITÉS

Tout utilisateur au sein de l'organisation ayant accès à des informations assume des responsabilités en matière de sécurité. Il doit respecter et appliquer les principes énoncés dans la présente politique et est redevable de ses actions auprès de la Direction générale. Toute information générée par les utilisateurs est la propriété exclusive de l'organisation. Le principe du privilège d'accès minimal est appliqué en tout temps lors de l'attribution d'accès aux renseignements personnels.

La mise en œuvre et la gestion de la sécurité reposent sur une approche holistique. Cette approche tient compte des aspects humains, organisationnels, financiers, juridiques et techniques. Les mesures de protection, de prévention, de détection et de correction doivent être assurées en conformité avec les cinq axes du cycle de vie des renseignements personnels. Ces mesures doivent notamment prévenir les incidents, les erreurs, la malveillance ou la destruction d'information sans autorisation.

Une évaluation annuelle des risques et des mesures de protection des renseignements personnels doit être effectuée afin d'obtenir l'assurance qu'il y a adéquation entre les risques, les menaces et les mesures de protection déployées.

6.1. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

L'organisation s'engage à assurer la protection des renseignements qu'elle collecte, utilise, communique, conserve et détruit.

Les utilisateurs doivent respecter l'encadrement légal et réglementaire en matière de protection des renseignements personnels et confidentiels.

Un utilisateur conserve le droit au respect de sa vie privée et de sa dignité lorsqu'il œuvre au sein de l'organisation. Toutefois, la protection à la vie privée ne limite pas les actions que l'organisation a le droit de prendre afin de se protéger, de gérer, de protéger ses membres ainsi que le personnel et d'obtenir des renseignements sur ces derniers, et ce, à plus forte raison lorsqu'ils en sont avisés au préalable.

Afin de permettre la détection de logiciels malveillants, l'organisation est autorisée à surveiller tout trafic transitant par ses réseaux informatiques incluant toutes les connexions cryptées. Ceci inclut la surveillance des services courriels en ligne ainsi que tout autre service à usage personnel. Seuls certains sites jugés de confiance absolue sont exempts de ce type d'audit.

À moins que leur divulgation ne soit de nature à nuire ou à entraver le travail d'une personne ou d'un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime, ou que la personne responsable des renseignements personnels ait des motifs raisonnables de croire que ces renseignements seront utilisés à des fins illégitimes, les renseignements personnels suivants ont un caractère public :

- Le nom, le titre, la fonction, la classification, l'adresse de courrier électronique professionnelle ainsi que l'adresse et le numéro de téléphone du lieu de travail d'un membre de l'organisation;

- Un renseignement concernant une personne en sa qualité de partie à un contrat de service conclu avec l'organisation, ainsi que les conditions de ce contrat.

De plus, l'organisation s'engage à coopérer à toute requête en provenance des forces de l'ordre ou de tout autre organisme mandaté à cet effet.

6.2. COLLECTE

La collecte est le moment où le renseignement personnel est :

- Recueilli (ex. : formulaire d'abonnement, sondage, outils analytiques Web);

- Créé (ex. : no de permis de conduire, no assurance sociale);

- Inféré (ex. : profil de consommateur), c'est-à-dire déduit à partir d'autres

renseignements.

Le fait de visualiser un renseignement personnel, comme ceux contenus sur une pièce d'identité, constitue également une collecte, même s'il n'y a pas de conservation par la suite.

À cette étape, les obligations suivantes doivent être respectées afin de protéger les renseignements personnels :

- Déterminer les fins de la collecte;
- Limiter la collecte de renseignements personnels aux fins déterminées. En cas de doute, un renseignement personnel est réputé non nécessaire;
- Recueillir les renseignements personnels par des moyens légaux et légitimes : sauf exception, la collecte doit se faire auprès de la personne concernée;
- Avant de constituer un dossier, la personne concernée doit être informée de:
    - L'objet du dossier;
    - L'utilisation qui sera faite des renseignements personnels et des moyens par lesquels ils sont recueillis (Ex. : formulaire, captation vidéo, enregistrement biométrique);
    - Catégories de personnes qui devront y avoir accès au sein de l'entreprise ou des fournisseurs de services;
    - L'endroit où ils seront détenus et pendant combien de temps;
    - Ses droits d'accès et de rectification;
    - Son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis;
    - La possibilité que les renseignements soient communiqués à l'extérieur du Québec (Ex. : information stockée sur des serveurs hors Québec).
- Obtenir le consentement des personnes concernées avant de collecter leurs renseignements personnels, directement ou auprès d'un tiers, à moins d'une exception prévue par la loi.

  Ce consentement peut être complété, modifié ou retiré à tout moment par la suite, étant entendu qu'une telle modification ne vaut que pour l'avenir. Le refus de donner ou maintenir un consentement requis peut notamment entrainer la cessation du traitement d'un dossier, par exemple un dossier relié à l'emploi ou celui relatif à une prestation de services.

  Tout consentement requis d'une personne concernée doit être manifeste,

libre, éclairé et donné à des fins spécifiques. Le consentement lié à des renseignements sensibles doit être manifesté de manière expresse.

Le consentement ne vaut que pour la période nécessaire à la réalisation des fins auxquelles il a été demandé.

Une entreprise ne peut refuser d'offrir un service ou un emploi à une personne qui refuse de fournir un renseignement personnel, sauf exception prévue par la loi.

Il est interdit à tout utilisateur de recueillir un renseignement personnel ou confidentiel si cela n'est pas nécessaire à l'exercice de ses fonctions ou à la mise en œuvre d'un programme dont il a la gestion.

Dans l'éventualité où l'organisation recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie, tels les témoins de connexion (« *cookies* »), comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage, elle doit, au préalable, l'informer du recours à une telle technologie et des moyens offerts pour activer ou désactiver de telles fonctions.

6.3. UTILISATION

L'utilisation est la période où le renseignement personnel est utilisé par les personnes autorisées au sein de l'organisation.

Les obligations suivantes doivent être respectées :

- Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de l'organisation lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions. Les privilèges d'accès sont attribués par les personnes autorisées et/ou les personnes qu'elles délèguent.

  Toute personne utilisant les renseignements personnels de l'organisation doit s'assurer que tout document confidentiel mis à sa disposition, quel que soit son support, soit hors d'atteinte en le conservant en lieu sûr.

  Le détenteur de l'information, avec l'appui du responsable de la sécurité de l'information ou toute autre personne autorisée, peut réviser, suspendre ou révoquer un privilège d'accès lorsque, entre autres raisons, l'utilisateur :

  - Ne respecte pas la présente politique ou les directives et les procédures qui en découlent;
  - Change de fonction à l'intérieur de l'organisation;
  - Termine son contrat ou son assignation;
  - Quitte définitivement l'organisation ou est congédié;
  - Divulgue des renseignements personnels ou confidentiels pour des raisons autres que celles prévues dans l'exercice de ses fonctions;

- Fait l'objet d'une suspension.

- Limiter l'utilisation des renseignements personnels. Ils ne doivent être utilisés et ne servir qu'à des fins pour lesquelles ils ont été recueillis ou obtenus. À moins d'une exception prévue par la loi, l'organisation doit obtenir le consentement de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli.

  L'organisation peut utiliser un renseignement à une autre fin que celle pour laquelle il a été collecté, sans le consentement de la personne concernée, dans les seuls cas suivants :

  - Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli, c'est-à-dire, qu'il doit y avoir un lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli;
  - Lorsque son utilisation est manifestement au bénéfice de la personne concernée;
  - Lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi;
  - Lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques pour l'organisation et qu'il est dépersonnalisé.

  Lorsqu'un membre de l'organisation utilise un renseignement personnel au nom de celle-ci aux trois premières fins mentionnées ci-dessus, il doit écrire à la personne responsable de la protection des renseignements personnels à rprp@sdbp.ca afin d'inscrire cette utilisation dans le registre approprié, en l'informant des points suivants :

  - La fin pour laquelle ce renseignement est utilisé (qui doit faire partie des exceptions énumérées);
  - La catégorie de personnes qui a accès au renseignement aux fins de l'utilisation indiquée.

6.3.1. Utilisation d'internet et des réseaux informatiques de l'organisation

Les renseignements personnels sont mis à la disposition des utilisateurs par l'organisation uniquement à des fins professionnelles, plus spécifiquement pour des tâches reliées à l'exercice de leurs fonctions. La présente politique émet des règles afin que chacun les utilise avec vigilance en respectant les droits d'auteur, la propriété intellectuelle, les règles de licences de logiciels, les droits de propriété, la confidentialité des informations, le bon emploi des ressources et les lois et règlements en vigueur au Québec et au Canada.

Les outils Internet ainsi que les actifs informationnels et de télécommunication accessibles à l'aide des réseaux informatiques de l'organisation ne doivent pas être utilisés en violation des lois et réglementations en vigueur.

6.3.2. Utilisation du courrier électronique

Les règles en vigueur dans l'organisation, relatives à l'utilisation du courrier électronique, font partie intégrante de la présente politique.

Les utilisateurs ayant des privilèges d'accès au courrier électronique organisationnel doivent l'utiliser uniquement pour des raisons professionnelles.

- La transmission de renseignements personnels ou confidentiels par courrier électronique (Internet, texto ou autres) est interdite, à moins que l'utilisateur n'ait pris les mesures requises de chiffrement prévues par l'organisme. Par ailleurs, l'utilisateur doit également être conscient que les courriers électroniques qu'il envoie peuvent, à son insu, être redirigés, imprimés, sauvegardés ou affichés sur d'autres médias ou d'autres systèmes informatiques;

- Aucune information concernant une religieuse ne peut être acheminée par courrier électronique (Internet, texto ou autres), à moins :

    - Que ce moyen réponde aux exigences établies par le service informatique;
    - Que la religieuse ait préalablement consenti à ce que l'on communique ses renseignements personnels à d'autres intervenants, sauf dans les cas où cette communication est autorisée par la loi.

- La modification d'un message avant sa retransmission à un autre destinataire est interdite.

- L'usage du courrier électronique pour faire des envois massifs de messages sans autorisation est interdit. Dans le cas où un envoi de masse doit être fait, les adresses des destinataires ne doivent pas être visibles (utiliser *Cci*).

- L'usage du courrier électronique est interdit aux fins de propagande (syndicale, politique, etc.).

6.3.3. Utilisation des outils personnels au travail

La venue de l'utilisation massive d'outils personnels au travail (ex. : tablettes, téléphones intelligents, applications dans les navigateurs Web, etc.) oblige les organismes à gérer les risques liés au partage des renseignements personnels. L'utilisateur ne doit pas se servir d'outils personnels à des fins professionnelles, sauf avec l'autorisation du responsable de la sécurité de l'information.

6.3.4. Utilisation des médias sociaux

Les règles relatives à la *Politique encadrant l'utilisation des médias sociaux* en vigueur dans l'organisation font partie intégrante de la présente politique.

Voir l'article 27 – Politique encadrant l'utilisation des médias sociaux du *Guide du personnel* des Sœurs du Bon-Pasteur de Québec.

6.3.5. Utilisation des actifs informationnels pour des fins syndicales ou associatives

Il est interdit d'utiliser les actifs informationnels de l'organisation à des fins syndicales ou associatives sans qu'une entente formelle soit faite avec les Sœurs du Bon-Pasteur de Québec.

6.3.6. Utilisation du télétravail

Seules les personnes expressément autorisées par leur supérieur immédiat à utiliser le télétravail ont accès aux services ou aux logiciels qui leur seront explicitement autorisés par le responsable de la sécurité de l'information selon des modalités précises. L'utilisateur doit respecter les ententes formelles de l'organisation et les directives qui en découlent afin d'assurer le respect de la présente politique.

6.3.7. Utilisation des imprimantes et des télécopieurs

Toute personne qui achemine ou imprime un document contenant des renseignements à caractère personnel et confidentiel doit en assurer la protection.

Les imprimantes et les télécopieurs doivent être placés de façon à éviter toute utilisation et observation non autorisées, soit dans un endroit surveillé ou non accessible par le public.

6.4. COMMUNICATION

La communication est la période où le renseignement personnel est communiqué avec le consentement de la personne concernée.

Tout utilisateur détenant un privilège d'accès s'engage à ne pas divulguer, sauf dans le cadre de ses fonctions, les renseignements personnels ou confidentiels dont il a pu prendre connaissance. Sans accès autorisé, il est interdit de consulter, de diffuser, de divulguer ou d'imprimer des informations concernant toute personne. En cas de violation de cet engagement, l'organisation peut imposer des sanctions disciplinaires ou administratives.

Selon les balises prévues à la loi, certains renseignements peuvent ou doivent parfois être protégés et ne pas être accessibles au public. Il s'agit de renseignements qui

pourraient avoir une incidence économique, politique ou légale pour l'organisation. Le responsable de l'accès à l'information évalue ces demandes particulières et applique, si requis, les restrictions à l'accès prévues à la loi.

En vertu de la loi, toute personne a le droit de consulter son dossier ou d'en obtenir copie. Les systèmes informatiques doivent prévoir cette possibilité. Les droits d'accès demeurent les mêmes que lorsque le dossier est détenu sur papier. Ces accès doivent être possibles, quelle que soit la forme des documents (écrite, graphique, sonore, visuelle, informatisée ou autre).

Une communication de renseignements personnels peut être effectuée par l'organisation sans le consentement de la personne concernée lorsque la loi l'exige ou le permet. Sauf en cas d'urgence, la communication est permise, après approbation du responsable de la protection des renseignements personnels, dans les circonstances suivantes :

- Au procureur de l'organisation, au directeur des poursuites criminelles et pénales, à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, uniquement si les renseignements personnels sont nécessaires aux fins, selon le cas, d'une poursuite pour infraction à une loi applicable au Québec ou pour d'une procédure judiciaire;

- À une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police ou par une personne ou un organisme agissant en application d'une loi qui exige un rapport de même nature, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement;

- À toute personne ou organisme si cette communication est nécessaire à l'application d'une loi au Québec, ou à l'application d'une convention collective, d'un décret, d'un arrêté, d'une directive ou d'un règlement qui établissent des conditions de travail;

- À un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion ou lorsque la communication est manifestement au bénéfice de la personne concernée;

- À un tiers si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne;

- Communiquer un renseignement sur l'identité d'une personne afin de recueillir des renseignements personnels déjà colligés par un tiers, uniquement si la personne responsable de la protection des renseignements personnels a informé la *Commission d'accès à l'information* au préalable.

L'organisation peut communiquer des renseignements personnels, sans le consentement des personnes concernées, en vue d'assurer la protection des personnes, dans les deux cas et aux conditions qui suivent :

- À une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée, uniquement lorsque l'organisation s'est assurée du caractère urgent et dangereux de la situation;

- À une personne exposée à un danger, son représentant ou toute autre personne susceptible de pouvoir leur porter secours, 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. On entend par « 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.

Lorsqu'un membre de l'organisation communique un renseignement personnel pour celle-ci aux fins mentionnées ci-dessus, il doit écrire au responsable de la protection des renseignements personnels à l'adresse rprp@sdbp.ca afin d'inscrire cette communication dans le registre approprié, en l'informant des points suivants :

- La nature ou le type de renseignement communiqué;

- La personne ou l'organisme qui reçoit la communication;

- La fin pour laquelle ce renseignement est communiqué et préciser si ces renseignements personnels ont été communiqués à l'extérieur du Québec.

L'organisation est également responsable des renseignements personnels qu'elle communique et qui lui sont confiés par ses tiers fournisseurs dans le cadre de ses activités. À cet effet, les contrats passés avec les fournisseurs doivent inclure les clauses nécessaires pour assurer la protection des renseignements personnels.

Lorsqu'un membre de l'organisation doit communiquer un renseignement personnel à l'extérieur du Québec pour celle-ci, avec ou sans le consentement de la personne concernée, il doit écrire au responsable de la protection des renseignements personnels à l'adresse rprp@sdbp.ca afin qu'il détermine si ces renseignements peuvent être

communiqués tel que demandé, en procédant à une évaluation des facteurs relatifs à la vie privée. Avant d'autoriser la communication de renseignements personnels à l'extérieur du Québec, il devra tenir compte de la sensibilité du renseignement, de la finalité de son utilisation, des mesures de protection dont bénéficierait le renseignement et le régime juridique applicable à l'endroit où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables. Si la communication est autorisée, elle se fera en accord avec les conditions exigées par la *Commission d'accès à l'information*.

6.5. CONSERVATION

La conservation est la période durant laquelle l'organisation garde des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

L'organisation doit respecter les obligations suivantes :

- Assurer la qualité des renseignements personnels qu'elle détient en veillant à ce qu'ils soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée;

- Prendre des mesures de sécurité propres à assurer la sécurité des renseignements personnels détenus.

Tout document appartenant à l'organisation doit être conservé de manière sécuritaire. Tout utilisateur doit respecter les règles en vigueur ainsi que les procédures qui les accompagnent, la structure de classification et le calendrier de conservation de l'organisation.

6.6. DESTRUCTION

Le cycle de vie du renseignement personnel se termine lors de sa destruction.

L'organisation doit détruire les renseignements personnels de manière sécuritaire dès que la finalité pour laquelle ils ont été collectés est accomplie, sous réserve du délai prévu par la loi ou par le calendrier de conservation établi.

7. SÉCURITÉ, ACCÈS ET RECTIFICATION

L'organisation doit :

- Mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels;

- Permettre l'exercice des droits d'accès et de rectification et répondre avec diligence, dans les 30 jours, aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées. L'absence de réponse dans ce délai équivaut à un refus. Toute personne peut contester un refus ou une réponse jugée insatisfaisante en exerçant son droit de recours devant la Commission d'accès à l'information.

7.1. EXERCICE DES DROITS D'ACCÈS ET DE RECTIFICATION

À l'égard des renseignements personnels qui la concernent, toute personne a le droit :

- D'obtenir les informations collectées la concernant;
- D'être informée de leur existence au sein d'un fichier de l'organisation;
- D'y accéder et d'en obtenir communication. Plus précisément, la personne concernée qui a le droit d'accéder à un renseignement personnel peut le faire sur place pendant les heures habituelles de travail ou à distance. Elle peut également en obtenir une copie et demander qu'un renseignement personnel informatisé lui soit communiqué sous la forme d'une transcription écrite ou intelligible. L'exercice de ce droit est gratuit;
- De les faire corriger et compléter. Plus précisément, la personne concernée qui reçoit confirmation de l'existence d'un document comprenant un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que ce document soit rectifié. Si une telle demande est refusée, la personne concernée peut demander que la demande soit enregistrée. Si une telle demande est acceptée, l'organisation délivre sans frais à la personne concernée, une copie de tout renseignement personnel modifié ou ajouté, ou, selon le cas, une attestation du retrait d'un renseignement personnel;
- D'être informée d'un incident de confidentialité qui peut lui causer un préjudice sérieux;
- De restreindre ou retirer son consentement à la collecte, l'utilisation ou la communication des renseignements personnels ou de les faire supprimer, si la loi le permet.

Pour exercer les droits d'accès et de rectification ci-dessus, la personne concernée doit faire sa demande par écrit et justifier son identité à titre de personne concernée, à titre de représentant, d'héritier ou de successible de cette dernière, à titre de liquidateur de la succession, à titre de bénéficiaire d'assurance vie ou d'indemnité de décès, à titre de titulaire de l'autorité parentale même si l'enfant mineur est décédé ou à titre de conjoint

ou de proche d'une personne décédée. La demande doit être adressée à la personne responsable de la protection des renseignements personnels par courriel à l'adresse rprp@sdbp.ca et doit inclure :

- Dans le cas d'une demande d'un conjoint ou d'un proche parent de la personne concernée dans son processus de deuil :
    - Identification de la personne requérante à titre de conjoint ou de proche parent en fournissant un document faisant état de son lien avec la personne décédée, par exemple, un certificat de mariage ou d'union civile, une preuve de résidence à la même adresse, un certificat de naissance ou tout autre document permettant d'établir son lien familial;
    - Renseignements personnels pour l'identification de la personne décédée en fournissant un document faisant état du décès, par exemple, un certificat de décès ou une publication de décès;
    - Description des informations demandées;
    - Illustration de la façon dont ces renseignements sont susceptibles d'aider la personne requérante dans son processus de deuil.

- Dans le cas d'une demande du liquidateur de la succession, du bénéficiaire d'une assurance vie ou d'une indemnité de décès ou d'un héritier ou d'un successible de la personne concernée :
    - Précisions illustrant la nécessité d'obtenir les renseignements ou les documents en faisant valoir les intérêts ou les droits de la personne requérante;
    - Identification de la personne requérante à titre de liquidateur, bénéficiaire, héritier ou successible et renseignements personnels pour l'identification de la personne décédée :
        - Le liquidateur de la succession désigné dans un testament, l'héritier ou encore la personne successible ayant un testament doit produire:
            - Un certificat de décès;
            - Un testament;
            - Deux certificats de recherche testamentaire, délivrés par la *Chambre des notaires du Québec* et par le *Barreau du Québec*, pour confirmer qu'il s'agit du dernier testament.
        - Le liquidateur de la succession, l'héritier ou la personne successible sans testament doit joindre :
            - Un certificat de décès;
            - Deux certificats de recherche testamentaire, délivrés par la *Chambre des notaires du Québec* et par le *Barreau du*

Québec, pour démontrer que la personne décédée n'avait pas de testament;
- Pour le liquidateur, une désignation d'un liquidateur de succession par les héritières et les héritiers;
- Pour le liquidateur, une déclaration notariée qui atteste le statut du liquidateur de la succession.

- Le bénéficiaire d'une assurance vie ou d'une indemnité de décès doit fournir :
  - Un certificat de décès;
  - Un document qui atteste qu'elle ou qu'il est bénéficiaire de l'assurance vie ou de l'indemnité de décès.

La personne responsable de la protection des renseignements personnels rend sa décision par écrit et en transmet une copie à la personne requérante. La personne responsable de la protection des renseignements personnels doit motiver tout refus d'accéder à une demande et indiquer la disposition de la loi sur laquelle ce refus s'appuie. Elle doit également prêter assistance à la personne requérante qui le demande pour l'aider à comprendre sa décision et l'informer du recours en révision et du droit d'appel prévus à la loi et du délai pour les exercer.

7.2. PLAN DE CONTINUITÉ DES AFFAIRES

L'organisation doit élaborer un plan de continuité des affaires afin d'améliorer de façon proactive sa résilience face à la perturbation de sa capacité à atteindre ses objectifs clés. Elle doit poursuivre la livraison de ses prestations de services à des niveaux acceptables et s'assurer que ces plans soient disponibles, connus, testés et utilisés par ses utilisateurs.

7.3. PLANS DE RELÈVE INFORMATIQUE

Le responsable de la sécurité de l'information doit s'assurer que les détenteurs de renseignements personnels ont planifié, avec la collaboration du service des technologies de l'information, des plans de relève informatiques. Il doit aussi les tester, afin de s'assurer de la remise en marche des systèmes d'information essentiels en cas de panne majeure.

De plus, ces mesures de relève doivent être révisées annuellement.

7.4. GESTION DES INCIDENTS DE SÉCURITÉ INFORMATIONNELLE

Tout événement indésirable touchant la sécurité des renseignements personnels doit être rapporté au responsable de la sécurité de l'information, qui apportera les correctifs nécessaires en respectant le processus de gestion des incidents de confidentialité en vigueur selon la loi.

8. PROJETS DE DÉVELOPPEMENT OU DE MODIFICATION DES SYSTÈMES D'INFORMATION

Le responsable de la sécurité de l'information ou les personnes qu'il délègue doivent définir les mesures de sécurité à mettre en place pour tout nouveau projet, et ce, dès la rédaction des analyses préliminaires.

9. ENTENTES ET CONTRATS

Toute entente ou tout contrat doit répondre aux exigences de l'organisation en matière de sécurité de l'information.

10. SENSIBILISATION ET FORMATION

L'organisation doit, sur une base régulière, mettre sur pied des activités de sensibilisation et de formation concernant la sécurité de l'information afin de s'assurer d'une compréhension et d'une appropriation des objectifs de la présente politique.

11. ENGAGEMENT DE CONFIDENTIALITÉ

L'organisation fait signer un engagement de confidentialité par tous ses utilisateurs et ses tiers.

12. RÔLES ET RESPONSABILITÉS

La direction générale est l'ultime responsable de la protection des renseignements personnels, mais se réserve le droit de déléguer, en tout ou en partie, certaines des tâches inhérentes à cette responsabilité à des personnes de confiance mieux habilitées à les exécuter au sein de l'organisation.

Le responsable de la sécurité de l'information, nommé par la direction générale, est notamment responsable d'orchestrer la mise en œuvre de la sécurité de l'information de l'organisation.

Tous les utilisateurs doivent respecter la présente politique.

La structure fonctionnelle de l'organisation ainsi que les rôles et responsabilités des principaux intervenants en matière de sécurité de l'information sont décrits ci-dessous.

Voir l'organigramme de sécurité informationnelle à l'***Annexe 2***.

12.1. CONSEIL GÉNÉRAL

Le Conseil général approuve la présente politique et les orientations générales soumises par le comité exécutif en matière de sécurité de l'information. À la suite des recommandations de ce comité, le Conseil général adopte tout changement à la politique

de sécurité de l'information ayant un impact sur ses orientations générales.

12.2. COMITÉ EXÉCUTIF EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Le comité exécutif recommande au Conseil général l'adoption de la présente politique et les orientations générales en matière de sécurité de l'information. Il lui fait également un suivi sur leur mise en œuvre et leur application.

Il exerce un rôle-conseil. Il évalue les risques et impacts sur la sécurité de l'organisation que les nouveaux projets et les opérations courantes associées aux renseignements personnels pourraient rencontrer. Il propose des actions quant à la coordination et la mise en œuvre de la présente politique.

12.3. DIRECTION GÉNÉRALE

Ultime responsable de la protection des renseignements personnels détenus par l'organisation, la direction générale s'assure que les valeurs et les orientations en matière de sécurité de l'information soient partagées par l'ensemble des gestionnaires, des religieuses ainsi que des employés des Sœurs du Bon-Pasteur de Québec. Elle s'assure de l'application de la politique dans l'organisation, apporte les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique.

Elle soumet le bilan annuel concernant l'application de cette politique au Conseil général.

Elle exerce son pouvoir d'enquête et applique les sanctions prévues à la présente politique lorsque nécessaire.

12.4. RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI)

À titre de représentant délégué de la direction générale en matière de protection des renseignements personnels, le responsable de la sécurité de l'information, gère et coordonne la sécurité des actifs informationnels au sein de l'organisation. Il doit donc superviser l'action des divers acteurs dans l'élaboration, la mise en place, la formation, le suivi et l'évaluation de la sécurité de l'information. Il doit :

- Veiller à l'élaboration et à l'application de la présente politique. Dans cette perspective, il collabore avec tous les gestionnaires;
- Évaluer la légitimité et la nécessité de recueillir des renseignements personnels, ainsi que leur niveau de sensibilité, avant d'en autoriser la collecte (« *Évaluation des facteurs relatifs à la vie privée* » (EFVP));
- Tenir un registre identifiant les détenteurs de renseignements personnels dans leur secteur respectif et les privilèges d'accès qui leur sont octroyés;
- S'informer des besoins en matière de sécurité auprès des détenteurs de

renseignements personnels et des gestionnaires, analyser les risques, leur proposer des solutions et coordonner la mise en place de ces solutions;

- Gérer les aspects relatifs à l'escalade des incidents de sécurité;
- Informer immédiatement le gestionnaire responsable, lorsqu'il constate qu'un utilisateur déroge à la présente politique;
- Suivre la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit;
- Produire annuellement, et au besoin, pour la direction générale, les bilans et les rapports relatifs à la sécurité des renseignements personnels appartenant à l'organisation;
- Gérer le *Registre des incidents de confidentialité*;
- Recevoir, traiter et répondre aux demandes d'accès à des documents (excluant les documents d'archives);
- S'occuper des communications avec la *Commission d'accès à l'information* (CAI).

12.5. SERVICE DES TECHNOLOGIES DE L'INFORMATION (STI)

Sous l'autorité du responsable de la sécurité de l'information, ce service agit comme conseiller en matière de sécurité des technologies de l'information. Il apporte son soutien au RSI sur le plan tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information.

Le service est notamment chargé de :

- Mettre en œuvre les orientations internes découlant des directives, des politiques internes et des pratiques généralement admises à cet égard;
- Produire les bilans et les plans d'action de sécurité de l'information numérique;
- Participer aux négociations des ententes de service et des contrats pour formuler des recommandations quant à l'intégration des dispositions garantissant le respect des exigences de sécurité de l'information numérique;
- Tenir à jour un registre des privilèges d'accès numériques contenant, entre autres :

- La liste des renseignements personnels qui doivent être protégés;
- La liste des détenteurs de renseignements personnels et leur substitut, leur rôle ainsi que les dates d'entrée en vigueur dans leurs fonctions.

- Fournir, implanter et maintenir en état les moyens technologiques de sécurité et de s'assurer de leur conformité aux besoins de sécurité déterminés par le détenteur;
- Conseiller, en collaboration avec le RSI, les détenteurs de renseignements personnels numériques en matière de protection desdits renseignements;
- Déterminer et gérer les risques d'atteinte à l'intégrité des renseignements personnels numériques en fonction des exigences de leurs détenteurs;
- Intégrer les orientations et les exigences en matière de sécurité de l'information et de protection des renseignements personnels lors de la conception, de la réalisation ou de l'entretien de processus d'affaires, des systèmes d'information et des infrastructures technologiques;
- Participer à la mise en place et à l'élaboration des solutions de sécurité associées aux demandes de développement de systèmes d'information, en partenariat avec les détenteurs de renseignements personnels et toutes personnes physique ou morale, qui, par engagement contractuel ou autre, accède aux renseignements personnels numériques;
- Assurer la disponibilité, l'intégrité, la confidentialité, l'accessibilité, l'irrévocabilité de l'information électronique selon les exigences et les droits d'accès définis par le détenteur des renseignements personnels;
- Prendre connaissance des événements, selon ses champs d'expertise, consignés dans le *Registre des incidents*, les analyser et formuler des recommandations.

12.6. RESPONSABLE DES ARCHIVES ET DE LA GESTION DOCUMENTAIRE

Le responsable des archives et de la gestion documentaire voit à l'établissement et au maintien du calendrier de conservation, du plan de classification et des outils de gestion documentaire de l'organisation qui permettent d'assurer la qualité et la conformité du cycle de vie des documents conformément à la Loi sur les archives (RLRQ, c. A-21.1) et aux règlements afférents.

Il est aussi responsable d'accorder l'accès aux renseignements personnels archivés dont il a la garde conformément aux lois en vigueur et de manière à ne pas causer préjudice à l'organisation.

12.7. GESTIONNAIRES

Les gestionnaires des divers services de l'organisation doivent :

- S'assurer que tous les employés sous leur charge connaissent et respectent leurs obligations découlant de la présente politique. Ils les informent précisément des normes, des directives et des procédures de sécurité en vigueur;
- Sensibiliser leur personnel à l'importance des enjeux de sécurité de l'information;
- Communiquer au RSI tout problème d'importance en matière de sécurité de l'information et tout incident relatif à la protection des renseignements personnels.

12.8. DÉTENTEURS DE RENSEIGNEMENTS PERSONNELS

Les détenteurs de renseignements de nature personnelle ou confidentielle doivent :

- S'assurer de la sécurité des renseignements personnels qui leur sont confiés;
- S'impliquer dans l'ensemble des activités relatives à la gestion des risques, notamment l'évaluation, la détermination du niveau de protection visé, l'élaboration des contrôles et la prise en charge des risques résiduels;
- S'assurer que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;
- Déterminer les règles d'accès aux renseignements dont ils assument la responsabilité.

12.9. SERVICE DES RESSOURCES HUMAINES

Le service des ressources humaines est responsable d'informer tout nouvel employé de ses obligations découlant de la présente politique. Il doit :

- Veiller à la formation et à la sensibilisation de l'ensemble du personnel quant à la sécurité des actifs informationnels, l'informer des conséquences d'une atteinte à la sécurité ainsi que des rôles et des obligations de tous en matière de sécurité et de protection de l'information;
- Définir le processus disciplinaire des employés relativement aux infractions à la présente politique;
- Procéder systématiquement à la révision et à la suppression, s'il y a lieu, de

tous ses accès aux systèmes d'information lors du changement de statut d'un employé ou tout autre événement concernant les tâches et les fonctions de ce dernier.

12.10. UTILISATEURS

Toute personne visée par la présente politique a l'obligation de la respecter afin de protéger l'information mise à sa disposition. Elle doit signaler tout incident au RSI en matière de sécurité de l'information et de protection des renseignements personnels.

13. TRAITEMENT DES PLAINTES

Toute personne visée par un renseignement personnel recueilli, utilisé, communiqué ou conservé par l'organisation peut déposer une plainte à la personne responsable de la protection des renseignements personnels en cas de manquement aux obligations prévues à la présente politique. La plainte doit être formulée par écrit et indiquer la nature des faits reprochés, le nom de la ou des personnes en cause, la date à laquelle l'incident s'est produit, ainsi que ses attentes quant à l'issue de la plainte. La plainte doit être adressée à la personne responsable de la protection des renseignements personnels par courriel à l'adresse suivante : rprp@sdbp.ca.

La personne responsable de la protection des renseignements personnels accuse réception de la plainte et traite celle-ci dans un délai raisonnable. Lorsque la plainte est recevable, elle fait enquête sur les faits allégués par tout moyen approprié. Elle communique avec diligence une réponse écrite à la personne à l'origine de la plainte.

14. SANCTIONS

Lorsqu'un utilisateur contrevient ou déroge à la présente politique ou tout document qui en découlent, il s'expose à :

- Des mesures disciplinaires et administratives ou toutes autres sanctions appropriées pouvant aller jusqu'au congédiement conformément aux directives de l'organisation;
- La révocation de certains droits d'accès aux équipements et services visés par la présente politique;
- Un remboursement aux Sœurs du Bon-Pasteur de Québec de toutes sommes, y compris celles émanant d'un jugement prononcé par tout tribunal ou organisme réglementaire quelconque à l'endroit de l'organisation.

15. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le Conseil général.

16. RÉFÉRENCES ET CADRE JURIDIQUE

Voir les références présentées à l'***Annexe 3***.

17. MISE À JOUR DE LA POLITIQUE

La présente politique doit être révisée minimalement aux trois ans afin de s'assurer qu'elle est conforme aux lois, aux nouvelles pratiques et aux technologies utilisées au sein de l'organisation.

18. ANNEXES

Annexe 1 – Définitions

Annexe 2 –Organigramme de sécurité informationnelle

Annexe 3 – Références et cadre juridique

ANNEXE 1

DÉFINITIONS

Actif informationnel Banque d'information, système d'information, réseau de télécommunication, infrastructure technologique ou ensemble de ces éléments. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

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

Authentifiant Information confidentielle détenue par une personne et permettant son authentification.

Catégorisation Processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder en termes de disponibilité, d'intégrité et de confidentialité.

Chiffrement Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

Commission d'accès à l'information (CAI)
La CAI est à la fois un tribunal administratif et un organisme de surveillance qui veille à l'application de la Loi sur l'accès et de la Loi sur le privé. Elle voit aussi à la promotion et au respect des droits des citoyens à l'accès aux documents des organismes publics et à la protection de leurs renseignements personnels. (https://www.cai.gouv.qc.ca/a-propos/mission-vision-valeurs/)

Confidentialité Propriété d'une information accessible uniquement aux personnes autorisées.

Détenteur Personne qui a effectivement la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels de l'organisation.

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

Donnée biométrique Toute caractéristique physique, biologique ou comportementale permettant d'identifier une personne physique. Inclut également tout renseignement produit à partir d'une telle caractéristique (ex. : empreinte digitale).

Évaluation des facteurs relatifs à la vie privée (EFVP)
Démarche qui consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées. La réalisation d'une EFVP doit être proportionnée à la sensibilité des renseignements personnels concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. Une EFVP est concluante lorsque :

- Il existe un lien rationnel entre les objectifs et la solution proposée (c'est-à-dire qu'il s'agit d'un moyen efficace d'atteindre l'objectif visé, cette efficacité étant basée sur des données concrètes et probantes);
- L'atteinte à la vie privée est minimale ou il n'y a pas d'autres solutions efficaces moins intrusives;
- Les avantages concrets surpassent les conséquences ou les préjudices pour les personnes concernées.

Holistique Toute démarche globalisante où divers éléments, habituellement isolés, sont regroupés et coordonnés pour l'obtention plus efficace d'un résultat visé.

Incident de confidentialité

Correspond à tout accès, utilisation ou communication non autorisés d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection. En voici quelques exemples :

- Un membre du personnel consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions;
- Un pirate informatique s'infiltre dans un système;
- Une personne utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne;
- Une communication est effectuée par erreur à la mauvaise personne;
- Une personne perd ou se fait voler des documents contenant des renseignements personnels;
- Une personne s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

Incident de sécurité de l'information

Événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

Infonuagique Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services évolutifs, adaptables dynamiquement et facturés à l'utilisation.

Intégrité Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

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

Plan de continuité Ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la reprise d'un niveau de fonctionnement prédéfini à la suite d'une perturbation, et ce à plusieurs niveaux de la structure organisationnelle.

Principe du privilège d'accès minimal

Autorisation d'accès restreinte de manière que l'utilisateur puisse n'accomplir avec celle-ci que les seules tâches autorisées et nécessaires à l'exercice de ses fonctions.

Privilège d'accès Droit d'accès particulier généralement réservé à des usagers ayant la responsabilité de la protection et de la gestion de systèmes d'information.

Registre d'autorité Le répertoire, le recueil ou le fichier dans lequel sont notamment consignés les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information ainsi que les responsabilités qui y sont rattachées.

Registre d'incident Recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, les mesures prises pour le rétablissement à la normale et le suivi.

Renseignement personnel

Renseignement qui concerne une personne physique et permet de l'identifier. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne. Sont des exemples de renseignement personnel :

- Le nom d'une personne et sa date de naissance;
- Numéro d'employé
- Numéro d'assurance sociale;
- Numéro de carte de crédit;
- Numéro d'assurance maladie;
- Renseignement de nature médicale ou financière;
- Le nom d'une personne et son numéro de téléphone personnel;
- Le nom d'une personne et son adresse de domicile;
- Le nom d'une personne et ses résultats scolaires.

Renseignement professionnel

Renseignement personnel qui concerne l'exercice par la personne concernée d'une fonction au sein d'une organisation tel que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail.

Renseignement sensible

Renseignement personnel qui, par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée. Il peut s'agir, par exemple, de renseignements médicaux, biométriques, génétiques ou financiers, ou de renseignements sur l'origine ethnique, les convictions politiques, l'orientation sexuelle, les convictions religieuses.

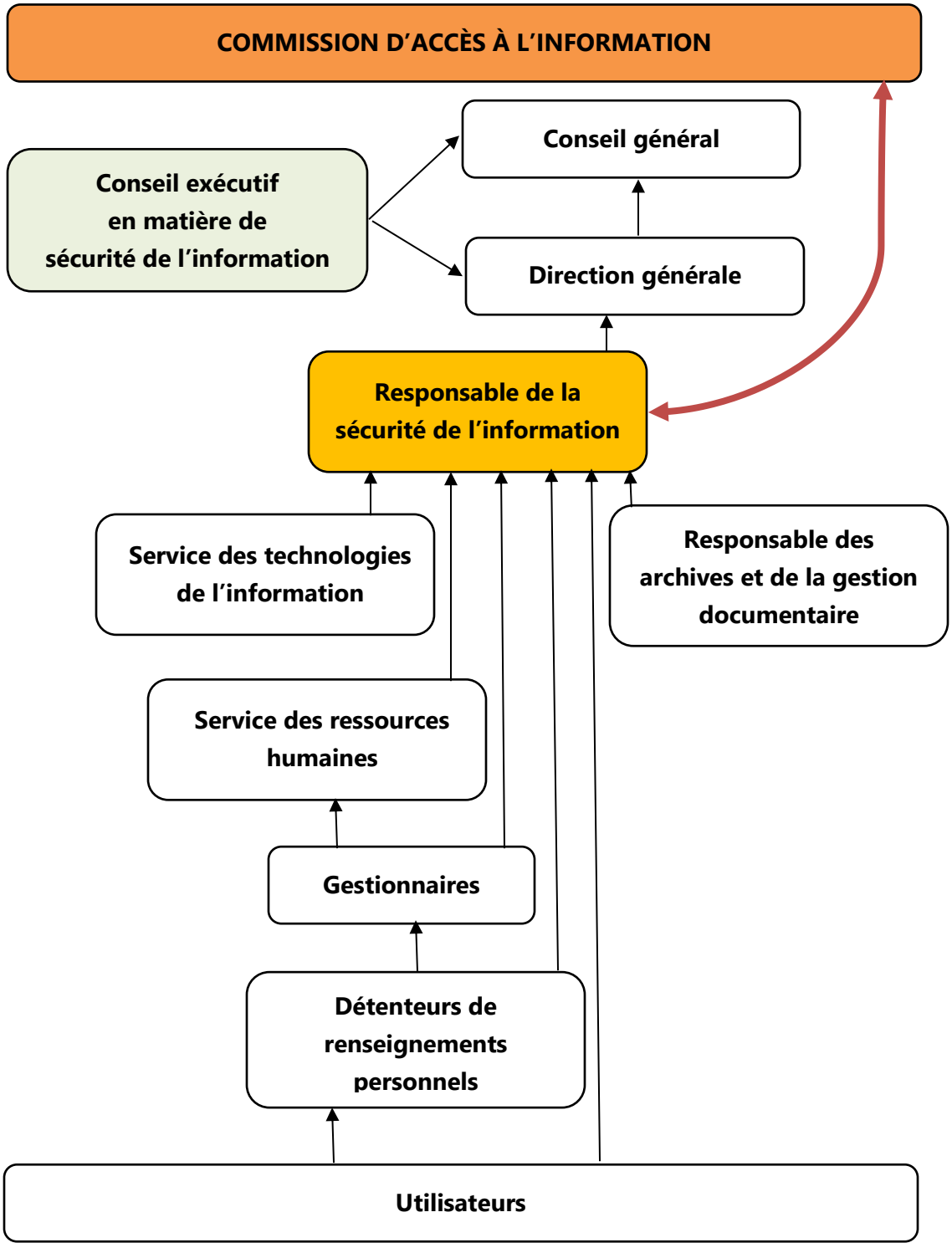
Technologie de l'information

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

Tiers	Toute personne morale ou physique ayant une personnalité juridique distincte de l'organisation ou qui exerce certaines fonctions hors mission à l'intérieur de l'organisation. Par exemple : les fournisseurs, les sous-traitants, les prestataires de services ou autres partenaires externes de l'organisation.
Usager	Toute personne qui utilise les services de l'organisation comme bénéficiaire ou dans le cadre de ses fonctions.
Utilisateur	Toute personne physique ou morale, tout groupe ou entité administrative qui fait usage d'un ou de plusieurs renseignements personnels sous la responsabilité de l'organisation.

ANNEXE 2

ORGANIGRAMME DE SÉCURITÉ INFORMATIONNELLE



ANNEXE 3

RÉFÉRENCES ET CADRE JURIDIQUE

- Charte des droits et libertés de la personne, RLRQ, c. C-12;
- Code civil du Québec, RLRQ c. CCQ-1991;
- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, L.Q. 2021, c. 25;
- Loi concernant le cadre juridique des technologies et l'information, L.R.Q., c. C-1.1;
- 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 la protection des renseignements personnels dans le secteur privé, RLRQ c. P-39.1;
- Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5;
- Loi sur les archives, L.R.Q., c. A-21.1;
- Institut universitaire de cardiologie et de pneumologie de Québec, *Politique relative à la sécurité de l'information*, 2016;
- Ville de Québec, *Politique de sécurité de l'information*, 2018;
- Université de Sherbrooke, *Directive relative à la protection des renseignements personnels*, 2023;
- Université Laval, *Règles de protection des renseignements personnels*, 2023;
- https://www.cai.gouv.qc.ca/entreprises/protection-des-renseignements-personnels-1/>