Gestion de l'information pour les conférences et les conseils par les lois et en pratique

Société de Saint-Vincent de Paul (SSVP)

La gestion de l’information de la Société de Saint-Vincent de Paul, à tous les niveaux, est régie par les exigences définies par le gouvernement, les meilleures pratiques de l’industrie et la Société.

SEPTEMBRE 2021

Pourquoi?

Pour aider les membres à clarifier et à comprendre.

Compte tenu de la réalité d'un **accès inapproprié des données à caractère personnel** dans notre environnement social, il existe une **obligation de protection contre l'utilisation abusive** d'informations à des fins telles que le vol d'identité.

- Protèger les informations personnelles
- Protèger la réputation de la société et son statut d’organisme de bienfaisance

---

- Protèger les informations personnelles
  - Partager les meilleures pratiques actuelles démontrées par la Règle et les statuts et le manuel des opérations
- Gestion adéquate des informations de la Société
  - Aider à la rédaction de rapports appropriés et exactitude au sein de la Société et auprès des gouvernements.

Approche

- **Principes de la SSVP élaborés** basés sur les principes de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) du gouvernement canadien;
- La LPRPDE a été examiné avec emphase autour des sections et approches mises en évidence sur le site Web du gouvernement;
- **Examen** des lois provinciales sur la protection de la vie privée **concernant les organismes de bienfaisance;**
- Alignement des parties pertinentes avec la **Règle et statut**;
- Consultation avec des **avocats** sur certaines des questions et réponses;
- Recherche des exigences de l'Agence du revenu du Canada (**ARC**);
- Recherche des **meilleures pratiques** de l'industrie;
- **Expérience vincentienne.**

Avant-propos:

Les principes qui suivent, concernant la gestion de l'information en fonction de la protection de la vie privée et de la sécurité au sein de la Société de Saint-Vincent de Paul (SSVP) **s'appliquent à tous les renseignements recueillis et utilisés par les personnes qui agissent au nom de la Société**, peu importe la façon dont ces renseignements sont conservés, **que ce soit sous forme de savoir, de document imprimé ou en version électronique**. Les principes de la Société s'inspirent de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRDPDE) et reflètent les statuts provinciaux ainsi que les exigences de l'Agence du revenu du Canada (ARC). Nous devons porter attention aux renseignements concernant **nos clients, membres, bénévoles, employés et donateurs ainsi que toute information relative au fonctionnement de la Société, aux procès-verbaux, aux rapports et aux statistiques et de nature financière.**

Principes de gestion de l'information de la SSVP

Principe 1 - Responsabilité

La Société de Saint-Vincent de Paul, à tous les niveaux, est responsable des informations personnelles et opérationnelles sous son contrôle. Chaque président est responsable et doit désigner une personne responsable du respect de ces principes et procédures d'information.

Principes de gestion de l'information de la SSVP

Principe 2 - Détermination des fins de la collecte de renseignements

Le but pour lequel les informations personnelles sont accumulées doit être identifié par l'organisation avant ou au moment de la collecte. Il faut aviser l'individu, oralement ou par écrit, de ces fins.

Principes de gestion de l'information de la SSVP

Principe 3 – Consentement

La connaissance et le consentement de l'individu sont requis pour la collecte, l'utilisation ou la divulgation de renseignements personnels, sauf lorsque cela est inapproprié (voir les paragraphes 7 (3) d.1) et 7 (3) d.2 de la LPRDPDE)* S'il existe une intention de divulguer des informations personnelles à des tiers ou à toute autre fin secondaire dont les ménages ne seraient pas raisonnablement au courant, un consentement écrit doit alors être obtenu.

- source https://laws-lois.justice.gc.ca/fra/lois/P-8.6/index.html

Principes de gestion de l'information de la SSVP

Principe 4 - Limitation de la collecte

La collecte de renseignements personnels doit être limitée à ce qui est nécessaire pour la Société et nécessaire aux fins identifiées. Les informations doivent être recueillies par des moyens justes et légaux. En général, les informations personnelles sensibles ne doivent pas être recueillies .

(veuillez vous reporter à la section Questions et réponses pour une description plus explicite de la collecte d'informations personnelles sensibles)

Principes de gestion de l'information de la SSVP

Principe 5 - Limitation de l’utilisation, de la divulgation et de la conservation

À moins que la personne ne consente autrement ou que la loi ne l'exige, les informations personnelles ne peuvent être utilisées ou divulguées qu'aux fins pour lesquelles elles ont été recueillies. Les informations personnelles ne doivent être conservées que le temps nécessaire à ces fins.

Les informations sensibles sont toujours sujettes à la protection de la vie privée pendant les conversations ou le partage en prenant en compte qui, quoi, où, quand, pourquoi et comment.

Principes de gestion de l'information de la SSVP

Principe 6 - Exactitude

Les informations personnelles et opérationnelles doivent être aussi précises, complètes et à jour que possible afin de répondre correctement à l'objectif pour lequel elles sont utilisées.

Principes de gestion de l'information de la SSVP

Principe 7 - Mesures de sécurité

Les informations personnelles et opérationnelles doivent être protégées par une sécurité appropriée, relative à la sensibilité des informations, et qui doit couvrir :

- les connaissances (par exemple informations apprises);
- les exemplaires imprimés (par exemple, papier);
- les exemplaires numériques (par exemple, feuille de calcul Excel, stockage en ligne).

Principes de gestion de l'information de la SSVP

Principe 8 - Transparence

La SSVP, à tous les niveaux, doit être prête à fournir des informations sur ses politiques et pratiques en matière de gestion des informations personnelles. Cette approche est conforme aux politiques et pratiques décrites dans le site web national, www.ssvp.ca

Principes de gestion de l'information de la SSVP

Principe 9 - Accès aux renseignements personnels

Sur demande, un individu doit être informé de l'existence, de l'utilisation et de la divulgation de ses informations personnelles et avoir accès à ces informations. Une personne doit pouvoir contester l'exactitude et l'exhaustivité des informations et les faire modifier le cas échéant. Ce principe est aligné sur le principe n° 3 « Consentement ».

Principes de gestion de l'information de la SSVP

Principe 10 - Possibilité de porter plainte à l'égard du non-respect des principes

Une personne doit pouvoir contester le respect des principes ci-dessus par une organisation. Leur contestation devrait être dirigée à la personne responsable de la conformité des informations de la Société.

Q & R. **Principe 1 - Responsabilité**

Q : Quelles seraient les définitions de « ***imputable*** » et « *responsable* » en lien avec l'application et l'implantation?

R : **Imputable** : la personne ayant pour mandat de voir à ce que **la politique et la procédure** soient mises en place. **Responsable** : la personne qui doit **voir à implanter et mettre en pratique** la procédure ayant trait au respect de la politique. Dans certains cas, il pourrait s'agir de la même personne, bien qu'en général, ce sont deux personnes différentes.

Q : Qui est responsable de la bonne gestion des données?

R : En fin de compte, **chacun est responsable** de la bonne gestion des données. Pour la SSVP, cela inclut des informations concernant les clients, les volontaires, les membres, les employés et les donateurs.; les informations opérationnelles de la Société telles que les données financières, les procès-verbaux, les rapports, les statistiques, etc. peuvent également nécessiter des dispositions spéciales.

Q & R. **Principle 1 - Responsabilité**

Q : Qui est sujet à la **Loi sur la protection des renseignements personnels et les documents électroniques** (LPRPDE)?

R : Même si certaines organisations à but non lucratif ne sont pas sujettes à la Loi parce qu'elles n'exercent pas d'activités commerciales, l'adoption de politiques et procédures visant à protéger l'information n'en demeure pas moins une **bonne pratique** à observer.

À moins qu'elles ne s'engagent dans des activités commerciales n'ayant aucune fonction essentielle en lien avec leur mandat et impliquant des informations personnelles, la LPRDPDE, règle générale, ne s'applique pas aux groupes de bienfaisance et à but non lucratif.

Sources de référence:

- https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/
- https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/

Q & R. **Principe 1 - Responsabilité**

Q : Pour la bonne gestion des données en matière de confidentialité et de sécurité, envers qui la SSVP est-elle responsable?

R : La SSVP est responsable **envers ceux que les principes protègent**. La SSVP doit adhérer à la **réglementation gouvernementale**. De plus, il est de **bonne pratique** de s'assurer que les informations personnelles sont correctement protégées.

Q & R. **Principe 1 - Responsabilité**

Q : Quelle loi provinciale sur la protection des renseignements personnels concerne la SSVP et comment?

R : Il peut y avoir des variations entre les provinces. Les législations provinciales réputées essentiellement **similaires** à la LPRDPDE (n'incluant pas la Saskatchewan, le Manitoba, l'I.-P.-E. ou les territoires) se retrouvent dans le site suivant

https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/lois-provinciales-essentiellement-similaires-a-la-lprpde/

Q : Quelle **loi provinciale inclut les organismes de bienfaisance?**

R : Veuillez consulter vos lois provinciales respectives pour plus de détails. Des détails supplémentaires dans l'annexe de la politique seront fournis.

- Pour la **Colombie-Britannique**, veuillez consulter la Section 2 : http://www.bclaws.ca/civix/document/id/complete/statreg/03063_01
- Pour le **Québec,** veuillez consulter la Section 1, points 17-24 : http://www.legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1

Q & R. **Principe 2 - Détermination des fins de la collecte de renseignements**

- **Noter toutes les fins de collecte identifiées** afin de retrouver facilement cette information dans le cas où une personne demanderait de rendre compte à ce sujet. Veuillez à ce que ces **fins se limitent** à ce qu'une personne raisonnable serait en droit de s'attendre dans les circonstances.
- Définissez à quelles fins vous **recueillez des informations aussi clairement et précisément que possible**, afin que les gens puissent comprendre comment l'information sera utilisée ou divulguée.

Exemples de fins de collecte :

- Vérification des détails concernant les niveaux d'aide et suivi;
- Maintien de données d'aide afin de se conformer aux politiques de la conférence;
- Remplir un formulaire de remboursement;
- Prendre position en faveur d'une famille.

Q & R. **Principe 3 - Consentement**

- La Société considère que tous les **renseignements** recueillis auprès des **ménages est personnelle** et, dans certains cas, de nature **délicate**. Par conséquent, la Société exige que le **consentement soit obtenu dans tous les cas** où des informations personnelles sont recueillies par un conseil ou une conférence. Ce consentement doit être **explicite** et obtenu **verbalement ou par écrit** (consentement explicite tel que défini par la LPRDPDE).
- S'il existe une intention de **divulguer des informations personnelles** à des tiers ou à toute autre fin secondaire que les ménages ne seraient pas raisonnablement au courant, un consentement écrit doit être obtenu.
- Dans certains cas, le consentement n'est pas nécessaire, par exemple lorsque des informations sont divulguées pour détecter et prévenir la fraude ou pour aider les forces de l'ordre.
- La collecte de renseignements personnels comprend les **discussions** lors desquelles de l'information personnelle est fournie, que cette dernière soit **physiquement consignée ou non.**
- Les conférences et conseils doivent conserver une **preuve documentaire du consentement**, y compris la date et les membres présents.

Q & R. **Principe 3 - Consentement**

Q : Doit-on obtenir le consentement d'une personne pour utiliser une photo ou une vidéo la représentant?

R : **Dans tous les cas**, il est important d'obtenir le consentement individuel et, dans le cas d'enfants de moins de 18 ans, il faut obtenir le consentement des parents.

(Remarque: basé sur consultation d'un avocat)

L'avis de consentement implicite lors d'un événement peut être précisé par exemple lors de l'inscription, en ligne ou à la table d'inscription. Les participants doivent informer les organisateurs s'ils ne veulent pas être pris en photo.

Q & R. **Principe 3 - Consentement**

Q : Les communications par courriel **doivent-elles inclure un énoncé de confidentialité?**

R : Il **serait approprié** que les communications de la Société comportent dans la signature un énoncé comme suit :

> Avis de confidentialité : Le présent message, ainsi que tout fichier qui y est joint, est envoyé à l'intention exclusive de son destinataire ou du mandataire chargé de le lui transmettre; il est de nature confidentielle. Si le lecteur du présent message n'est pas le destinataire prévu, il est prié de noter qu'il ne doit ni divulguer, ni distribuer, ni copier ce message et tout fichier qui y est joint, ni s'en servir à quelque fin que ce soit. Merci d'en aviser l'expéditeur par courriel et de supprimer ce message ainsi que tout fichier joint.

Q & R. **Principe 4 - Limitation de la collecte**

- Il est important d'identifier dans les politiques et pratiques quels sont les renseignements personnels **normalement requis** et de veiller à ce que tous les bénévoles les connaissent bien. La **collecte d'un moins grand nombre de données** réduit d'autant les risques associés à une divulgation non autorisée.
- Les **renseignements personnels de nature délicate (RPND)** sont définis comme étant de l'information qui, **si égarée, compromise ou divulguée,** peut causer à la personne un préjudice, un embarras, une gêne ou une injustice substantiels.
- Bien qu'il soit nécessaire dans certaines circonstances de recueillir des RPND, de manière générale, les membres de la Société **ne devraient pas recueillir les RPND suivants** :

  - Numéro d'assurance sociale (NAS); - Numéro de compte bancaire; - Information relative au passeport ou à la citoyenneté; - Numéro de carte d'assurance maladie; **- Information relative aux soins de santé;** - Information relative à l'assurance maladie; - Information relative à une carte étudiante; - Numéro de carte de crédit ou de débit - Numéro de permis de conduire; - Dossier médical; - États financiers;

Rappelez-vous que **toute information peut être de nature délicate**, selon le contexte.

Q & R. **Principe 4 - Limitation de la collecte**

Q : L'information concernant une date de naissance devrait-elle être recueillie?

R : En lien avec le principe no 2 (Détermination des fins de la collecte de renseignements), la **date de naissance comme telle n'est pas vraiment pertinente** pour le travail de la Société. Cependant, **l'année de naissance** peut être utile pour les interventions relatives à certains programmes, particulièrement les programmes destinés aux jeunes.

Q & R. **Principe 4 - Limitation de la collecte**

Q : Quels renseignements devons-nous inclure dans un formulaire de consentement?

R : La collecte de renseignements personnels doit se limiter aux informations **requises** par la Société et nécessaires à des fins d'identification. Les informations doivent être recueillies de **manière juste et légale**.

Q : Quelles sont les **directives** à suivre au moment de la collecte d'information permettant d'accomplir une œuvre de charité

R : Points à considérer :

- **Penser sécurité** – Besoin de savoir ce qui se passe ou ce qui s'est passé avant la visite ou l'interaction;
- **Penser bienveillance** – Mieux interagir, faire preuve de sympathie et parfois anticiper les besoins – Préférable de poser des questions avant d'aider; historique limité.
- **Penser preuve** – Registre d'actes de charité; décisions inscrites dans les procès-verbaux, etc.

Q & R. **Principe 4 - Limitation de la collecte**

Q : En matière de sécurité, **quel niveau** de vérification des dossiers de police (VDP) doit être **obtenu auprès des membres** pour vérifier leur autorisation à contacter le client et à collecter des informations personnelles sur le client?

R : Il y a trois niveaux à considérer :

Niveau 1 - *Vérification du casier judiciaire à des fins civiles (VC)* Cette vérification est destinée aux candidats impliqués en tant que bénévole, employé ou dans toute situation dans laquelle une VC de base est demandé (par exemple, détaillant ou immigration). Ce contrôle N'EST PAS destiné aux candidats bénévoles et / ou d'un emploi auprès de personnes vulnérables (voir Niveau 3 ci-dessous).

Niveau 2 - *Vérification du casier et des antécédents judiciaires (VAJ)* Semblable au niveau 1 et inclut des accusations portées devant les tribunaux - non encore déclarées coupables.

Niveau 3 - *Vérification des antécédents en vue d'un travail auprès de personnes vulnérables (VAPV)* Cette vérification est réservée aux candidats à la recherche d'un emploi et / ou bénévoles dans une position d'autorité ou de confiance par rapport aux personnes vulnérables au Canada uniquement.

Tous les membres, y compris les membres auxiliaires de la Société, doivent avoir un VDP avec un contrôle de secteur vulnérable (CSV).

Q & R. **Principe 4 - Limitation de la collecte**

Q : Que signifie "**secteur vulnérable**"?

R : Aux termes de la **loi sur le casier judiciaire**, on entend par "secteur vulnérable" les personnes qui sont en **situation de dépendance** vis-à-vis d'autrui ou qui **risquent par ailleurs plus que l'ensemble de la population** d'être lésées par des personnes en position d'autorité ou de confiance. **L'âge, le handicap ou d'autres circonstances** (temporaires ou permanentes) d'une personne peuvent rendre une personne vulnérable. Les enfants, tels que définis par la loi sur le casier judiciaire, désignent les personnes âgées de moins de 18 ans.

Q & R. **Principe 4 - Limitation de la collecte**

Q : Quelle est la **politique de la Société** en matière de vérification des dossiers de police (VDP)?

R : Présentement, comme l'indique le **Manuel des opérations** (9.11 Convention de service et entente de confidentialité), tous les membres de la Société doivent avoir un VDP avec un contrôle de secteur vulnérable (CSV) tous les trois (3) ans.

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

- L'information de nature délicate est toujours sujette à la protection de la vie privée pendant les conversations ou le partage d'information, prenant en considération le **qui, quoi, où, quand et comment.**

- Il est à noter que la Société de Saint-Vincent de Paul **n'effectuera aucune divulgation, échange, vente ou location de renseignements personnels** à des tierces parties **sans consentement**.

Commissariat à la protection de la vie privée du Canada, obtention d'un consentement
https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

Q : Comment **protégeons-nous l'identité** des vincentiens lorsque nous communiquons avec les clients?

R :

- insérant un code avant le numéro de téléphone au moment de composer, par exemple *67 (ligne terrestrielle) #31(cellulaire);
- appelant d'un **téléphone au nom de la Société de Saint-Vincent de Paul ou du bureau de la paroisse.**
- ne se servant que de leur **prénom**.

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

Q : Comment protéger les copies imprimées?

R :

- conservées **en lieu sûr;**
- pendant le **transport**, **protection contre la perte ou l'accès non autorisé;**
- **non reconnaissable après destruction** - exemple: déchiquetage croisé;
- **accessible à au moins une personne secondaire** en cas d'incapacité ou d'indisponibilité du responsable principal;
- organisé et stocké **pour faciliter** le transfert lors de la succession.

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

Section 3.13 Conservation et archivage des dossiers de la Règle et statuts canadiens

Conférences ou conseils non incorporés				
Documents	**Durée de conservation**			
	3 ans	**3 ans après la fin du mandat du président de l'époque**	**6 ans**	**À perpétuité**
Formulaires d'agrégation, d'institution ou de jumelage				X
Demandes d'ahésion de membre				X
Agence du revenu du Canada : enregistrement à titre d'organisme de bienfaisance				X
Procès-verbal des réunions				X
Dossiers financiers			X	
Liste des membres du conseil d'administration				X
Correspondance générale durant le mandat de tout président		X		
Dossiers de cas	X			
Rapports annuels				X
Procurations durant le mandat de tout président		X		

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

Q : Dans la section 3.13 de la Règle et Statuts (Conservation et archivage des dossiers), que comprend la « Correspondance générale durant le mandat de tout président »?

R : **Toute correspondance en lien avec le travail des conférences et conseils est considérée comme de la correspondance.** Il y a habituellement dans les procès-verbaux une motion concernant la réception et le classement de la correspondance. Cependant, quand il s'agit de la disposition de **fonds** ou d'activités requises, la durée d'archivage est de **sept ans**, tout comme c'est le cas pour les dossiers financiers.

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

Q : Comment et pendant combien de temps devons-nous conserver les documents papier? Si vous numérisez un document ou le prenez en photo, pouvez-vous détruite la copie imprimée? Si des renseignements ont été recueillis sur un client, mais que ce client n'a reçu aucun service depuis plusieurs années, quelle est la procédure à suivre pour se défaire (/nettoyer) des documents **(tout média).**

R : Les renseignements sur les clients **peuvent être détruits après trois (3) ans après qu'ils aient été obtenus.** Trois (3) ans constitue un délai raisonnable car un délai plus long augmente le risque que de l'information non autorisée soit divulguée; par extension, si l'information est détruite, cela constitue une bonne mesure de la nature confidentielle de cette information.

Note: Un avocat a été consulté pour cette question.

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

Q : Comment se fait-il que nous devions conserver l'information financière pendant 7 ans?

R : La règle des 6 ans de l'ARC indique l'année courante + 6 années complètes, ce qui donne 7 ans.

Dans le document de l'ARC IC78-10r5-10e, se référer aux sections 26 & 27 -28 + annexe;

https://www.canada.ca/fr/agence-revenu/services/impot/entreprises/sujets/tenue-registres-comptables/conserver-vos-registres-pendant-combien-temps-comment-obtenir-permission-detruire-avant-fin-delai-conservation.html

Q & R. **Principe 5 –**
Limitation de l'utilisation, de la divulgation et de la conservation

Q : La règle de l'ARC comporte-t-elle des exceptions qui exigeraient de conserver les dossiers financiers pendant plus de 6 ans années complètes?

R : Oui, dans le cas où un donateur effectue un don direct, monétaire ou en nature, et que ce don comporte un but prévis ou des restrictions quant à l'usage qui en est fait, **les instructions du donateur et le reçu aux fins de l'impôt doivent être conservés en dossier pendant au moins 10 ans.** À titre d'exemple, un donateur donne de l'argent ou un terrain et indique que son don doit servir aux œuvres spéciales, par exemple un refuge, un magasin des logements.

Veuillez vous référer au document de l'ARC IC78-10r5-10e 5800 (1) (d) (iv).

Q & R. **Principe 6 - Exactitude**

Q : Est-ce qu'un client doit montrer des documents émis par le gouvernement lorsque nous le visitons?

R : Habituellement non, mais en pratique, cela aide à la précision.

Q & R. **Principe 6 - Exactitude**

Q : Les membres doivent remplir de **nombreux formulaires** issus du **Manuel des opérations**, dans le cadre du processus de **filtrage et de l'adhésion**. Tous ces formulaires sont-ils **absolument nécessaires**?

R : Il est important que ces documents soient **pertinents et exacts** et que lors des assemblées, les présidents de conseil rappellent aux membres que nous devons nous conformer à la **réglementation gouvernementale et aux exigences en des assureurs.**

Les formulaires clés issus du Manuel d'opérations sont :

- 9.9 Filtrage – Demande d'adhésion
- 9.10 Filtrage – Liste de contrôle d'entrevue/Rapport de vérification des références
- 9.11 Filtrage – Convention de service et entente de Confidentialité
- 9.23 Questionnaire et déclaration relatifs à la prévention de l'abus, de la discrimination et du harcèlement

Q & R. **Principe 7 - Mesures de sécurité**

Des mesures doivent être mises en place concernant tant la **cueillette que le transport** d'information; elles doivent couvrir:

- les connaissances (ex. : information apprise);
- les copies imprimées (ex. : le papier);
- les versions numériques (ex. : feuille de calcul Excel, stockage en ligne).

Connaissances et copies imprimées avaient été discuté sous
Principe 5 – Limitation de l'utilisation, de la divulgation et de la conservation

Q & R. **Principe 7 - Mesures de sécurité**

Q : Y a-t-il des directives à suivre concernant l'utilisation des services d'une tierce partie?

R :

- aucun système n'est à l'abri du **piratage**;
- les services et systèmes de stockage en ligne tiers doivent **être évalués**;
  - **soutenir** les principes de **gestion de l'information** de la Société;
  - accompli par la **recherche** et par entrevue;
  - personnes qui ne sont pas de la Société qui ont accès;
  - le fournisseur a-t-il de bons **principes et pratiques de protection** de la vie privée pour protéger ses clients;
  - services à **plusieurs entités organisationnelles** dans une structure hiérarchique (plusieurs conférences et conseils, par exemple), des **contrôles** appropriés doivent être en place pour **limiter l'accès** aux seules informations **requises** par cette entité organisationnelle;
    - niveaux de permission;
    - points d'accès clairs pour chaque utilisateur;
      - assurer la confidentialité;
      - réduire l'impact en cas de violation.

Q & R. **Principe 7 - Mesures de sécurité**

R : Stockage en ligne :

- les dossiers de renseignements personnels doivent être stockés sur un **serveur canadien**;
- les originaux des dossiers financiers doivent, en vertu des règles de l'Agence du revenu du Canada (ARC), doivent être conservés au Canada;
- toute autre information peut être stockée ailleurs en ligne;
- on doit mettre en place et en action un plan visant à **éviter la perte** d'accès à un compte ou de données se trouvant dans un compte, en raison de **non-utilisation**. Par exemple, les informations obsolètes ou les comptes peuvent être effacés par des fournisseurs tiers.

Q & R. **Principe 7 - Mesures de sécurité**

Q : Quelles sont les mesures de sécurité à mettre en place?

R : Copie de sauvegarde:

- être **générée régulièrement et fréquemment** pour permettre à une conférence ou un conseil de **poursuivre ses opérations** sans perdre de dossiers ou devoir consentir un effort majeur de reconstruction;
- **une copie de sauvegarde conservée pleinement intacte à l'extérieur du site**, jusqu'à ce qu'elle soit remplacée par une copie de sauvegarde plus récente des informations numériques originales
- trois copies à gérer: l'original, la copie de sauvegarde à l'extérieur du site et la copie de sauvegarde la plus récente devant remplacer la copie se trouvant à l'extérieur du site.

Q & R. **Principe 7 - Mesures de sécurité**

R : Politique de mot de passe

Les techniques telles que les mots de passe forts, la limitation de distribution des mots de passe et le changement fréquent de mot de passe constituent les meilleures pratiques.

- Utiliser les «**mots de passe forts**» dans la section Définition du document;
- Les mots de passe comprennent les numéros d'identification personnelle (NIP) et les combinaisons sûres;
- L'information protégée par mot de passe, chiffrement des données ou toute autre méthode doit être **accessible** par au **moins un autre membre** responsable secondaire au cas où le premier responsable se trouverait en situation d'**incapacité** ou de non-disponibilité;

Ceci s'applique aux:

- sites web
- coffres-forts
- téléphone cellulaires
- messageries vocales
- connexions aux ordinateurs où sont entreposées les données.

Q & R. **Principe 7 - Mesures de sécurité**

Autres actions:

- **Changer le mot de passe** lorsque les membres partent;
- Utilisation du cryptage;
- Les **informations sensibles** acheminées par courrier électronique ou clé de mémoire doivent être protégées par un **mot de passe ou cryptées**;
- Pour minimiser la prolifération de documents protégés par d'anciens mots de passe, lorsque les documents se trouvent sur un **système informatique protégé, les documents individuels ne doivent pas être protégés;**
- **L'authentification en deux étapes** devrait être **plus largement utilisée à l'avenir** et **cette méthode devrait être envisagée selon les circonstances.**
- **Two-Step Authentication** is expected to become **more widely used in the future;**
- Sur les ordinateurs personnels, **séparez les données de la société de vos données personnelles.**
  - Option possible - cartes mémoire sauvegardées.

Q & R. **Principe 7 - Mesures de sécurité**

Q : Est-ce que les **dossiers financiers originaux en ligne** doivent être conservés au Canada?

R : Oui, le serveur doit se trouver physiquement **au Canada**. Veuillez vous référer à l'Agence du revenu du Canada (ARC) sous la rubrique « Tenue de registres comptables ».

https://www.canada.ca/fr/agence-revenu/services/impot/entreprises/sujets/tenue-registres-comptables/conserver-vos-registres-pendant-combien-temps-comment-obtenir-permission-detruire-avant-fin-delai-conservation.html

Q & R. **Principe 7 - Mesures de sécurité**

Q : Sur quel type de media devons-nous conserver les reçus aux fins d'impôt émis sous forme électronique?

R : Afin de protéger les reçus générés par ordinateur, les organismes de bienfaisance enregistrés doivent veiller à ce que :

- Le système informatique utilisé pour conserver les reçus est protégé par mot de passe et restreint l'accès aux dossiers des donateurs ainsi que leur modification;
- Les dossiers des donateurs sont conservés sur des **médias non destructibles**, tels que des CD-ROM ou des imprimés, et que des copies sont conservées hors site en vue de leur récupération au besoin;
- Des copies des reçus émis peuvent être imprimées sur demande.

Veuillez consulter l'Agence du revenu du Canada (ARC) au lien suivant :
https://www.canada.ca/fr/services/impots/bienfaisance.html

Q & R. **Principe 7 - Mesures de sécurité**

R : Redondance organisationnelle

- Dans le but de mettre en place et de **poursuivre à long terme la gestion des informations informatisée**, il faut prévoir que les responsables aient un niveau suffisant de **connaissances informatiques, d'expérience et de compétence**. Il faut éviter de mettre en place des pratiques de gestion des informations informatisée qui**, après le départ du membre responsable, se retrouvent dans les mains de membres moins expérimentés;**
- L'information doit être **organisée et conservée** afin d'en permettre le **transfert facilement** lors de la transition d'un dirigeant à un autre;
- Une fois que le transfert d'information est complété et que la **transition** est réussie, selon le rôle du membre sortant, **l'information devrait être supprimée des appareils de stockage personnels,** sauf les documents de correspondance de l'ancien président, sujets à une règle de conservation de trois ans.

Q & R. **Principe 8 - Transparence**

Q : Que doivent faire les conférences et conseils pour assurer que les principes de gestion de l'information de la Société soient connus?

R : La SSVP **doit être familière à tous les niveaux avec les politiques et pratiques ayant trait à la gestion des renseignements personnels,** lesquelles sont publiées dans le **site web national, et elle doit les partager sur demande.**

- La Règle et Statuts Canadien
- Manuel des opérations
- Site Web

Q & R. **Principe 9 – Accès aux renseignements personnels**

Q : Est-ce qu'une personne dont nous avons recueilli les informations personnelles peut demander à voir cette information?

R : **Oui** et en **temps opportun**, le responsable de la vie privée ou le délégué du président partagera ces données.

Q & R. **Principe 10 - Possibilité de porter plainte à l'égard du non-respect des principes**

Q : Qui devrait être responsable de traiter les défauts de conformité?

R : La **personne nommée par le président** pour être responsable de la vie privée et qui, en tant que telle, **doit traiter les défauts de conformité** et est le premier répondant en la matière. Il doit également tenir le président informé, car ce dernier imputable.