cyberSanté Ontario
www.cybersanteontario.on.ca

Politique de sécurité de l'information

Numéro de document : 867

Version : 4.2

Ontario
cyberSanté Ontario

Table des matières

1 But et objectif

1.1 But

Le but principal de l'Agence cyberSanté Ontario (l'Agence) est d'offrir des services fiables de gestion de l'information, des technologies de l'information et des communications au secteur ontarien des soins de santé. En vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) et le Règlement 329/04, tel qu'il a été modifié par le Règlement 447/08 (le Règlement) cyberSanté Ontario fournit des services sous trois rôles distincts :

- à titre de fournisseur de biens et services afin de permettre à un dépositaire de renseignements sur la santé d'utiliser des moyens électroniques pour recueillir, utiliser, modifier, divulguer, conserver ou éliminer des renseignements personnels sur la santé;
- à titre de fournisseur d'un réseau d'information sur la santé(FRIS);
- à titre de tiers retenu par un FRIS pour participer à la prestation de services à un dépositaire de renseignements sur la santé.

La sécurité de ces services et des renseignements sur la santé visée est essentielle au succès de cyberSanté Ontario et à l'objectif stratégique d'améliorer l'efficacité des soins de santé en Ontario.

La perte de confidentialité, d'intégrité ou de disponibilité, ou de la disponibilité des renseignements ou des systèmes et services technologiques utilisés pour les communications et le traitement de l'information pourrait nuire à la poursuite des objectifs et à cyberSanté Ontario, ses clients, et autres intervenants.

La sécurité de l'information (souvent appelée « sécurité » ci-dessous) est la discipline de la gestion des risques inhérents à la sécurité afin de respecter les lois et règlements, d'atteindre les objectifs et de réduire les dommages potentiels.

La présente politique :

- définit les objectifs et la stratégie de l'entreprise en matière de sécurité de l'information;
- établit des principes de gestion de la sécurité de l'information;
- précise et attribue la responsabilité des éléments exigés et des résultats attendus du programme de sécurité de l'information de cyberSanté Ontario;
- accorde l'autorité d'émission et d'application de documents d'appoint à la gouvernance;
- précise les exigences fondamentales en ce qui concerne le contrôle de la sécurité de l'information.

1.2 Objectifs et stratégie

Un des principaux objectifs de la politique est de s'assurer que cyberSanté Ontario prévoit la responsabilisation et qu'elle met en place des processus et des mécanismes de contrôle conformes aux responsabilités déléguées à cyberSanté Ontario sous les trois rôles que l'Organisme peut jouer, comme le prévoient la *Loi de 2004 sur la Protection des renseignements personnels sur la santé* (LPRPS) et l'article 6.1 du Règlement de l'Ontario 329/04 (tel qu'il a été modifié).

La sécurité de l'information est un moyen par lequel les risques pour la sécurité peuvent être réduits à un niveau acceptable, alors que l'on augmente et conserve la confiance des parties qui s'y fient. Il n'est pas possible, ni souhaitable, d'éliminer tous les risques. La sécurité de l'information vise certains objectifs précis, soit réduire l'incertitude et gérer la probabilité, la nature et les conséquences des événements indésirables possibles, ce qui permet d'atténuer les dommages, de préserver la valeur et de permettre la bonification de la valeur à tirer de l'information, de la technologie de l'information et des services associés.

Des mécanismes et mesures de sécurité seront mis en œuvre afin de protéger adéquatement l'information recueillie, utilisée, conservée, transmise, divulguée ou échangée par cyberSanté Ontario, et afin de garantir la prestation continue de services à l'aide de systèmes d'information.

Pour garantir l'efficacité et la cohérence de la gestion de la sécurité à l'échelle de l'Organisme, cyberSanté Ontario mettra en œuvre un système de gestion de la sécurité de l'information (SGSI) respectant largement les normes ISO 27001:2005 et ISO 27002:2005. Si la responsabilité de l'élaboration et de mise en œuvre du SGSI incombe au directeur de la sécurité et de la protection de la vie privée (DSPVP), toutes les unités organisationnelles doivent investir suffisamment et adapter leurs procédés pour intégrer, adopter et appuyer le SGSI.

2 Champs d'application

La présente politique s'applique à:

- tous les éléments d'organisation de cyberSanté Ontario (divisions, services, etc.);
- tous les membres du personnel de cyberSanté Ontario, y compris les cadres, les employés, les travailleurs indépendants et les employés à contrat;
- tous les renseignements dont cyberSanté Ontario est propriétaire ou qu'elle contrôle, ou sous son administration ou sa garde;
- tous les actifs et immeubles possédés, loués, licenciés, ou gérés par cyberSanté Ontario;
- tous les services fournis par cyberSanté Ontario, à l'interne comme à la clientèle;
- tous les services fournis à cyberSanté Ontario par des entités du secteur public ou du secteur privé et dont dépend cyberSanté Ontario pour la conduite de ses affaires.

3 Principes de gestion

3.1 Approche intégrée

Les mécanismes de contrôle de la sécurité de l'information, destinés à se défendre contre les menaces, à préserver la valeur, à permettre la prestation fiable de services de qualité, et à prévenir les dommages, sont mis en œuvre par le concours intégré de personnes, de procédés et de la technologie.

3.2 Tolérance aux risques définies par le Conseil d'administration

cyberSanté Ontario gèrera ses activités de façon à ce que les risques de l'entreprise résiduels et relatifs à la sécurité soient cohérents avec la tolérance envers les risques définie par le Conseil d'administration et délégué aux unités organisationnelles par la haute direction.

3.3 Conformité aux exigences juridiques et réglementaires

Une norme raisonnable sur les meilleures pratiques en matière de sécurité de l'information, conséquente aux menaces et risques perçus sera appliquée en conformité aux exigences des lois et règlements sur la protection de l'information.

3.4 Responsabilisation et autorité de prendre des décisions en matière de risque

Les décisions sur la gestion des risques de l'entreprise associés à la sécurité doivent être prises par ceux qui ont la responsabilité et l'autorité d'accepter les risques résiduels, d'allouer des ressources à l'atténuation du risque et à la reprise à la suite d'éventuels événements nuisibles. Les risques feront l'objet d'un rapport à la direction dans le but d'obtenir des directives stratégiques de la part des cadres immédiats, du Comité de gestion du risque et du Comité de vérification du Conseil.

3.5 Les interdépendances doivent être gérées

Chaque division et service est responsable de la gestion des risques de l'entreprise en matière de sécurité qui influent directement sur l'atteinte des objectifs de l'unité. Le réseau de services interdépendants fournis par toutes les unités organisationnelles doit être géré de façon à ce que les dépendances de sécurité d'un service sur les autres soient explicites, comprises et comblées, et de façon à ce que le système général de contrôle de sécurité soit conçu et mis en œuvre, efficace et robuste.

3.6 Approche holistique

La sécurité de l'information et les services de l'entreprise afférents seront traités et analysés de façon holistique, avec une attention portée sur les aspects humains, les processus et la technologie tout au long de la durée de vie utile de l'information, des technologies de l'information et des services afférents. Les ressources seront

allouées selon les pratiques normales de gestion des affaires afin de garantir la cohérence des capacités et services de sécurité et des besoins de l'entreprise.

3.7 Établissement de la confiance par la sécurité

La confiance envers le caractère approprié et l'efficacité des attributs de sécurité de l'information des services internes et publics de cyberSanté Ontario sera obtenue et préservée à l'aide de l'application rigoureuse de processus efficaces sur :

- la détermination des objectifs et exigences de sécurité de l'entreprise;
- Le développement de l'architecture et modèles de soutien des objectifs qui respectent les exigences;
- la définition détaillée des services, y compris les engagements en matière de sécurité, les règles d'utilisation et de comportement, ainsi que la surveillance opérationnelle et la production de rapports;
- la mise en œuvre et l'exploitation conformément à la conception et à la définition de service;
- la détermination, le suivi et la résolution des problèmes de sécurité;
- la validation par des tests et des évaluations des menaces et des risques en temps opportun, ainsi que des vérifications de sécurité indépendantes;
- profilage formel de risques et l'acceptation formelle de risques importants, ainsi que la communication de cette information aux intervenants et aux clients touchés.

3.8 Établissement progressif des capacités

Des stratégies de sécurité, des mécanismes et des compétences seront progressivement conçus et mis en œuvre pour améliorer les offres de service et la capacité en soutien aux objectifs de l'entreprise. Les paramètres de rendement seront dévelopés et appliqués; le DSPVP rendra régulièrement compte de la progression au Comité exécutif et au Conseil d'administration.

4 Politique

La politique de cyberSanté Ontario est de :

- protéger la confidentialité, l'intégrité et la disponibilité de l'information conformément aux exigences de la loi et des demandes raisonnables des parties qui contrôlent l'information, des dépositaires de l'information, et des utilisateurs autorisés;
- protéger l'intégrité et la disponibilité des services technologiques;
- tenir chaque utilisateur responsable de son accès non autorisé ou inapproprié, de l'utilisation, de la divulgation, de l'élimination, de la modification, ou de l'altération de renseignements ou services importants. Tout membre du personnel de cyberSanté Ontario,

consultant ou employé d'un distributeur qui enfreint cette politique s'expose à des sanctions, voire au renvoi ou à la fin de contrat;

- déterminer des responsabilités et de mettre en œuvre des processus et des mécanismes de contrôle qui assurent la conformité à l'article 6.1 de la LPRPS, le Règl. de l'Ont 329/04 (tel qu'il a été modifié par le Règl. de l'Ont. 447/08), et avec la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et autres exigences législatives, politiques et opérationnelles propres aux domaines d'activité de cyberSanté Ontario.

L'information et les services afférents doivent être sécurisés conformément aux exigences juridiques et de l'entreprise et tout au long de leur cycle de vie, afin d'optimiser la combinaison de la valeur nette dérivée et du risque couru.

La sécurité de l'information doit être gérée conformément aux normes internationales suivantes :

- ISO/IEC 27001:2005, Technologie de l'information – techniques de sécurité – systèmes de gestion de la sécurité – exigences.
- ISO/IEC 27002:2005, Technologie de l'information – techniques de sécurité – Code de pratique pour la gestion de la sécurité de l'information

4.1 Programme de sécurité de l'information

Un programme de sécurité de l'information doit être développé et mis en œuvre dans le but :

- d'assurer un leadership en matière de sécurité de l'information et d'apporter une expertise;
- de susciter et de coordonner la participation des principaux intervenants;
- de développer, d'interpréter et de mettre en œuvre une gestion complète;
- d'orienter et de promouvoir la stratégie de sécurité et l'architecture de sécurité, dans l'esprit des objectifs, stratégies et exigences de l'entreprise;
- de susciter une conscience, une motivation et une capacité organisationnelles et individuelles appropriées;
- de rapporter et de recommander des actions ou des améliorations à la haute direction et au Conseil d'administration en matière de posture sécuritaire, d'incidents de sécurité et à l'égard de l'état et de l'efficacité du programme de sécurité de l'information.

4.1.1 Gestion de programme

La responsabilité première du développement et de la gestion du programme de sécurité de l'information et du système de gestion de l'information de sécurité (SGIS), y compris les ressources humaines

spécialisées nécessaires, les processus et la technologie, est attribuée au directeur de la sécurité et de la protection et de la vie privée (DSPVP).

4.1.2 Gouvernance

Dans le cadre des responsabilités à l'égard du programme de sécurité de l'information, le DSPVP développera et gèrera un cadre complet de documents de politiques et de lignes directrices afférentes, ainsi que la procédure d'exception.

- Cette Politique de sécurité de l'information (PSI) doit être révisée à tous les deux ans et mise à jour au besoin. La PSI doit être approuvée par le président directeur général.
- Les directives d'opérations en matière de sécurité de l'information (DOSI) doivent aider la PSI en définissant le programme de sécurité de l'information et le SGSI plus en détail, en clarifiant les responsabilités de la direction et en précisant les résultats escomptés de la part de la gestion de la sécurité de l'information. Les DOSI doivent être approuvées par le président-directeur général sur recommandation du DSPVP.
- Les pratiques standard en matière de sécurité de l'information (PSSI) doivent aider les DOSI et la PSI en étayant les responsabilités particulières des personnes et des postes, et en précisant les pratiques uniformes à adopter par cyberSanté Ontario afin d'atteindre les résultats précisés dans les DOSI. Les PSSI doivent être approuvées par le DSPVP sur recommandation du directeur de la sécurité de l'information.

Le DSPVP mettra sur pied et présidera un comité directeur où siégeront des représentants des principales divisions de l'Organisme, et qui fournira des directives d'affaires et établira les priorités tactiques du programme de sécurité.

4.1.3 Stratégie et plans

Le DSPVP doit fournir le leadership et son expérience, et collaborer avec les autres dirigeants à la planification et à la mise en œuvre de l'architecture et des initiatives stratégiques d'entreprise, dans le but

d'atteindre les objectifs de sécurité et d'offrir les services requis en matière d'infrastructure de sécurité.

4.1.4 Développement des capacités

Le programme de sécurité de l'information doit comprendre des éléments pour favoriser la conscience, la motivation et les capacités de l'organisation et de ses membres.

4.1.5 Assurance et surveillance

Le programme de sécurité de l'information doit incorporer la surveillance, les paramètres, la production régulière de rapports, ainsi qu'une vérification et des directives de la direction pour effectuer le suivi et apporter une amélioration progressive du programme et de ses résultats.

Le directeur des services de sécurité doit effectuer une vérification périodique du programme et de sa mise en œuvre à l'échelle de cyberSanté Ontario pour évaluer l'à-propos et l'efficacité du programme et pour vérifier la conformité aux exigences de cette politique et de politiques connexes.

Le programme de sécurité de l'information sera soumis à une vérification externe quinquennale ou plus fréquente.

4.2 Processus

L'exécution uniforme de processus bien définis sera un indicateur de capacité organisationnelle et de maturité en matière de sécurité de l'information. Les DOSI et les PSSI définiront les processus et pratiques standards que chaque division, service et employé doit mettre en œuvre dans l'élaboration et la prestation de services sécurisés et pour garantir une sécurité adéquate de l'information.

Dans la mesure du possible et de l'efficacité, les processus de sécurité de l'information seront mis à contribution et intégrés à d'autres processus d'affaires tels que : l'élaboration de stratégies et plans d'affaires, la gestion du risque, l'évaluation des possibilités, le lancement de nouveaux produits, l'analyse des exigences, l'architecture, la conception, l'élaboration, l'assurance de la qualité, la gestion de projets, la gestion de l'information, la gestion de l'actif, la gestion des services, la gestion de la clientèle, l'approvisionnement, la gestion des contrats, le perfectionnement et la gestion du rendement.

Le directeur des services de sécurité aidera les directeurs généraux à développer, réviser (au besoin), lancer progressivement, dans leurs divisions respectives, et à surveiller l'efficacité de ces processus de sécurité de l'information et pratiques standards.

4.3 Contrôles

Le système de contrôles de sécurité protégeant un bien ou un service doit être conçu et utilisé de façon à ce que :

- toutes les exigences en matière de gouvernance et de sécurité des affaires soient respectées;
- il y ait diversité et chevauchement dans les contrôles de sécurité afin qu'un arrêt imprévu de n'importe quel mécanisme de contrôle n'ait pas de conséquence sérieuse;
- les dommages découlant d'une faille de sécurité soient limités et contenus, et qu'ils aient le moins de potentiel possible de dépasser des limites prédéterminées;
- le cadre de contrôle présente des preuves de son efficacité et comprenne des mécanismes de correction des déficiences;
- les risques résiduels relatifs à la sécurité soient à la hauteur de la tolérance au risque et des conseils concernant l'intérêt pour le risque transmis par le Conseil d'administration.

Le système de contrôles de sécurité et les mécanismes de contrôle individuels doivent être évalués et testés avant d'être appliqués, puis de façon régulière par la suite. La technologie, les produits et outils mis à contribution doivent être configurés et utilisés adéquatement afin de garantir l'efficacité de tous les contrôles de sécurité.

Le PSI et les PSSI doivent définir les exigences et pratiques particulières en matière de contrôle dans chacun des domaines suivants, selon ce qui est jugé nécessaire pour respecter les objectifs en matière de sécurité :

- contrôle interne – responsabilité définie et délégation d'autorité, contrôles des processus, séparation des tâches, et vérifications indépendantes;
- gestion de l'actif – identification, administration, classification, étiquetage, règles et exigences en matière de sécurité, et inventaire;
- gestion du service – définition, responsabilité, cohérence avec les exigences de l'entreprise, et intégration du service;
- contrôles contractuels, y compris l'impartition;
- contrôles du personnel – présélection, modalités d'emploi, ententes de conformité, sensibilisation, formation, supervision, incitatifs et conséquences pour le personnel à temps plein et à temps partiel, les prestataires de services et le personnel des fournisseurs;
- contrôle de l'accès et responsabilisation – identification, vérification, autorisation, contrôle de séance, acceptation obligatoire, et audit;

- contrôles physiques et environnementaux, contrôle des lieux, des services publics et de l'entretien;
- contrôles cryptographiques – protocoles, algorithmes, gestion des clés et des certificats et produits;
- planification, architecture, développement, acquisition, acceptation et entretien;
- zones et barrières – sécurité physique et réseau, et accès à distance;
- contrôles des activités – gestion du service des TI, procédure d'exploitation, intégrité du système, supervision et production de rapports, détection des intrusions, et gestion des incidents;
- contrôles de l'assurance – évaluation, tests, vérification indépendante, et audit.

4.4 Continuité des affaires

Les processus de gestion de la continuité des affaires doivent être mis en œuvre afin de déterminer et de restreindre à des niveaux acceptables les risques et conséquences associés aux failles et catastrophes importantes, tenant compte de l'interruption des services de cyberSanté Ontario ainsi que de la capacité et du temps de relancer les opérations essentielles.

Les conséquences possibles des catastrophes, failles de sécurité et interruptions de service doivent être analysées afin de déterminer l'importance des services et des éléments d'infrastructure TI d'appoint. Des plans intégrés doivent être développés, mis en œuvre et testés pour s'assurer que tous les services essentiels à l'entreprise sont préservés ou peuvent être remis en place en priorité, à un niveau acceptable et dans les délais prescrits en cas d'interruption. Les engagements à assurer la continuité des activités des services essentiels doivent être incorporés aux ententes de niveau de service auprès des clients. Les plans de reprise à la suite d'une catastrophe devraient être mis à l'essai chaque année.

Les plans de contingence doivent prévoir :

- la restauration rapide des services interrompus par l'arrêt d'un système, d'un processus ou d'une fonction;
- la reprise de service d'urgence à un autre endroit en cas de catastrophe ou de panne prolongée au principal point de service;
- la reprise limitée des services essentiels en cas de perte importante de personnel.

4.5 Services d'infrastructure de sécurité

La mise en œuvre de certains contrôles de sécurité est plus efficace en tirant avantage de services en gestion centrale qui sont mis en œuvre et gérés par des membres du personnel possédant une expérience spécialisée en sécurité et en séparant les tâches.

Les services d'infrastructure de sécurité suivants sont définis plus en détail dans les DOSI et les PSSI; ils sont nécessaires pour atteindre les objectifs de sécurité de l'entreprise et pour la prestation de services sécurisés à la clientèle :

- gestion de l'identité, authentification, et gestion des privilèges;
- infrastructure cryptographique – gestion des clés et des certificats;
- détection des intrusions et gestion des incidents;
- suivi et rapporté sur l'état de la sécurité
- assurance sécurité.

Les exigences, la stratégie, l'architecture et la conception de ces services doivent être développés en étroite collaboration avec le Service de la sécurité de l'information ou par le Service. Une attention particulière doit être accordée à la séparation des tâches dans la prestation de ces services.

5 Responsabilités

5.1 Comité d'audit du Conseil d'administration

Conseille et supervise le programme de gestion du risque de sécurité.

5.2 Président-directeur général

Vérifie et approuve la politique de sécurité de l'information, sur recommandation du DSPVP.

Vérifie et approuve les directives d'exploitation de la sécurité de l'information, sur recommandation du DSPVP.

5.3 Vice-président principal aux services aux entreprises et à la vie privée

Fournit des directives de l'entreprise et confirme les priorités d'opérations.

Assure les relations avec le Conseil d'administration et communique les directives du Conseil d'administration en ce qui a trait aux attentes en matière de gestion du risque de sécurité et à la tolérance au risque.

S'assure que le programme de sécurité est coordonné avec le programme de respect de la vie privée et que ses objectifs s'y conforment.

Approuve le financement et les ressources adéquats pour le programme de sécurité.

Assure le leadership et fournit des conseils concernant les incitatifs et la discipline des employés.

5.4 Directeurs généraux

Assurent la direction et la supervision de la gestion des risques d'affaires relatifs à la sécurité au sein de leurs sphères de responsabilité.

Accordent les ressources appropriées et adaptent les processus afin d'intégrer, d'adopter et de soutenir le SGSI.

S'assurent que toutes les activités de l'entreprise et la prestation des services sont conformes à la présente politique, aux DOSI et aux PSSI.

S'assurent que les processus et formations adéquates ainsi que les programmes de sensibilisation sont mis en œuvre afin que tous les employés, entrepreneurs et membres du personnel des distributeurs soient au fait de leurs obligations en vertu de la LPRPS et du Règlement, et s'assurent qu'ils signent une entente de confidentialité qui énonce clairement leurs obligations concernant l'accès aux renseignements personnels et aux renseignements personnels sur la santé, en conformité avec les articles 6 et 6.1 du Règlement.

5.5 DSPVP

Développe et dirige la gouvernance de la sécurité de l'information, le programme de sécurité de l'information, le SGSI, et les ressources humaines spécialisées, processus et technologies nécessaires.

Dirige et gère les processus et plans de continuité des affaires à l'échelle de l'entreprise.

Commande des vérifications externes du programme de sécurité de l'information.

5.6 Directeur des services de la sécurité

Développe et met à jour les documents de gouvernance en sécurité de l'information : PSI, DOSI, PSSI, et lignes directrices de soutien.

Développe et gère les politiques et pratiques conformément à l'alinéa 6(3)5 du Règlement en ce qui a trait à l'évaluation des menaces, des vulnérabilités et des risques pour la sécurité et l'intégrité des renseignements personnels sur la santé dans l'exécution des services de cyberSanté Ontario, et soutient les exigences en matière de divulgation et de production de rapport prévues au Règlement.

Gère le développement progressif de la capacité et l'introduction des processus et des pratiques définis aux DOSI et aux PSSI, et surveille leur efficacité à relever les possibilités d'amélioration.

Fournit des conseils avisés en matière de sécurité et des services de vérification et d'évaluation de sécurité indépendants pour aider les directeurs généraux et leurs organismes, projets et initiatives.

Développe un programme de sensibilisation à la sécurité qui garantira que tous les employés, entrepreneurs et membres du personnel des fournisseurs possèdent une conscience adéquate des menaces fréquentes pour la sécurité, des conséquences des incidents de sécurité, et des contrôles pour protéger l'information et la technologie de l'information, nécessaire à l'exercice de leurs fonctions.

Surveille, suit et rédige des rapports réguliers sur la position, les enjeux et les risques en matière de sécurité de l'information à l'échelle de cyberSanté Ontario.

Effectue une vérification annuelle du programme de sécurité de l'information et de sa mise en œuvre à l'échelle de cyberSanté Ontario.

6 Glossaire

Terme	Définition
Responsabilisation	La propriété qui garantit que les actions d'une personne peuvent être reliées uniquement à la personne, qui peut être tenue responsable de ses actions.
Agent	En ce qui a trait à un dépositaire de renseignements sur la santé, désigne une personne qui, avec l'autorisation du dépositaire, agit au nom du dépositaire en matière de renseignements personnels sur la santé dans l'intérêt du dépositaire et non de l'agent, que l'agent ait ou non l'autorité de lier le dépositaire, que l'agent soit ou non au service du dépositaire et que l'agent soit rémunéré ou non.
Assurance	Le résultat de processus par lequel une personne est convaincue que les objectifs, engagements et obligations sont respectés.
Vérifiabilité	La propriété qui permet de déterminer avec fiabilité les actions et les qualités en remontant, à l'aide des dossiers, à leurs origines ou sources dans leur contexte particulier.
Authentification	Le processus qui consiste à établir la validité d'une identité revendiquée.
Autorisation	Le processus qui consiste à accorder ou à refuser la permission à différents types d'accès ou d'activité, possiblement assorti de certaines contraintes ou conditions.
Disponibilité	La propriété des biens et services qui garantit qu'il est possible d'y avoir accès et de s'en servir au besoin, sans retard inutile.
DA	Directeur de l'administration
PDG	Président-directeur général
Certification	Évaluation complète des éléments et protections techniques et non techniques d'un service technologique, effectuée en soutien du processus d'approbation ou d'homologation, afin de déterminer la mesure dans laquelle le service répond à certaines exigences et certains engagements en matière de sécurité.
Conformité	Répondre aux exigences des lois, règlements, politiques et normes.
Confidentialité	La propriété qui fait que l'information est disponible ou communiquée uniquement aux personnes, entités ou processus autorisés.
DSPVP	Directeur de la sécurité et de la protection de la vie privée
Cryptographie	L'art ou la science des principes, moyens et méthodes permettant de rendre l'information incompréhensible et de remettre l'information

	cryptée dans une forme compréhensible.
Préjudice	Perte ou diminution du droit, de la propriété, des affaires, de la réputation ou du bien-être physique ou mental d'une personne
Dépositaire de renseignements sur la santé	Une personne ou une organisation décrite à l'article 2 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (la Loi), qui a la garde ou le contrôle de renseignements personnels sur la santé par suite ou à l'égard de l'exercice de ses pouvoirs ou de ses fonctions ou de l'exécution du travail visé à la Loi.
Identification	Le processus qui permet la reconnaissance unique d'une entité par une autre, généralement à l'aide de noms (p. ex., noms d'utilisateur, noms de système).
Identité	L'ensemble des caractéristiques physiques, personnelles, comportementales, contextuelles, relationnelles et autres, qui permettent de reconnaître ou de connaître irrévocablement une personne ou une chose.
Information	Signification cohérente tirée des dossiers; celle qui augmente la certitude de la connaissance. L'information est la signification de la représentation d'un fait (ou d'un message) pour l'acquéreur.
Intégrité de l'information	La propriété qui fait que l'information est valide (authentique, cohérente, complète, inchangée, et utile) et que sa validité peut être présumée au fil du temps.
Gestion de l'information	Direction et contrôle de la production, de l'utilisation, de la transformation, de l'échange, de la protection et de l'élimination de l'information par une entité.
Sécurité de l'information	Le sujet visé par les concepts, procédés et mesures visant à gérer le risque et à limiter les dommages afférents à une brèche, potentielle ou réelle, délibérée ou accidentelle, à la confidentialité, à l'intégrité ou à la disponibilité de l'information ou des services de technologie de l'information.
Technologie de l'information (TI)	Les technologies de l'information (TI) ou technologies de l'information et des communications (TIC) sont l'ordinateur, les communications, l'entrée/sortie, et les logiciels créés et utilisés pour acquérir, emmagasiner, jumeler, extraire, transformer, valider, protéger, échanger, consulter et utiliser l'information.
SGSI	Système de gestion de la sécurité de l'information
DOSI	Directives d'opérations en matière de sécurité de l'information
PSSI	Pratiques standards en matière de sécurité de l'information
Renseignements personnels	Renseignements consignés concernant une personne identifiable selon la définition contenue à l'article 2 de la *Loi sur l'accès à l'information et la protection de la vie privée*, 1990, tel qu'elle a été modifiée.

Renseignements personnels sur la santé	Renseignements identificatoires concernant un particulier qui se présentent sous forme verbale ou autre forme consignée, tel que le décrit l'article 4 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (la Loi).
Risque	Distribution combinée de la probabilité d'événements indésirables potentiels et des dommages qu'ils causent ou de leur inconvénient pour l'atteinte des objectifs.
Intérêt pour le risque	La quantité de risque, à grande échelle, qu'une entité accepte de courir dans sa quête de valeur et d'atteinte d'objectifs.
Évaluation du risque	Un processus d'analyse des menaces, des vulnérabilités, des scénarios et des conséquences potentielles afin de déterminer, de caractériser et d'estimer les risques et de comprendre l'importance des risques pour certaines actions de l'entreprise éventuelles ou certains changements environnementaux.
Gestion du risque	Direction et contrôle coordonnés des activités visant à assurer la compréhension des risques, à s'assurer qu'ils sont appropriés, conformes aux objectifs.
Tolérance au risque	Les limites qualitatives et quantitatives d'acceptabilité (supérieure et inférieure) du risque et des préjudices ou dommages potentiels qui y sont associés pour l'atteinte des objectifs.
Menace	Une cause potentielle d'un événement ou incident indésirable, pouvant causer préjudice à une personne ou à une entité, ou empêcher l'atteinte des objectifs.
Vulnérabilité	Une déficience ou faiblesse d'un bien, d'un processus ou d'un service qui pourrait être exploitée par une menace.

7 Références et documents associés

Référence	Lieu
Politique de gestion du risque	Bibliothèque des documents de politique d'entreprise de cyberSanté Ontario
Politique sur la vie privée et la protection des données	Bibliothèque des documents de politique d'entreprise de cyberSanté Ontario

8 Annexe A – Architecture du SGSI

La présente politique est fondée sur les normes ISO ISO27001 et ISO 17799. Ces deux normes définissent les exigences d'un système de gestion de la sécurité de l'information (SGSI) complet qui soit conforme aux objectifs de l'entreprise et qui reçoive l'approbation de la direction en matière de gestion du risque pour la sécurité.

La présente politique ne prétend pas et ne vise pas à définir les normes ISO; cependant, l'illustration suivante explique l'architecture conceptuelle d'un système de gestion de la sécurité de l'information telle que définie par les normes. La présente politique ne porte que sur un seul élément du cadre de gestion exigé par les normes. Il faudra se doter d'autres documents sur la gestion, les processus et les contrôles à la lumière des principes et responsabilités prévus à la présente politique.