Date entrée en vigueur : 30 août 2023
Date de mise à jour :

Politique – Protection des renseignements personnels

Approbation

La *Politique de protection des renseignements personnels* (la « *Politique* ») a été adoptée telle que déposée par le conseil d'administration de Norseco s.e.c./ W.H. Perron.

1. Objectif

Dans le cadre de ses opérations, l'*organisation* collecte, utilise et communique des *renseignements personnels* de ses employés, membres, clients ou partenaires.

L'*organisation* croit en l'importance de protéger la vie privée des individus avec qui elle interagit et s'engage à mettre en place, surveiller et maintenir des pratiques adéquates en matière de protection des renseignements personnels.

Ainsi, la présente politique (ci-après, la « politique ») établit les principes et les lignes directrices qui guident Norseco s.e.c. / W.H. Perron (ci-après « l'*organisation* ») dans la collecte, l'utilisation, la conservation et la divulgation des renseignements personnels conformément à la Loi 25 sur la protection des renseignements personnels. Cette politique s'applique à tous les employés, membres, clients, fournisseurs et autres parties prenantes de l'entreprise. Elle expose les principes que l'*organisation* applique lorsqu'elle traite des *renseignements personnels* et poursuit les objectifs suivants :

- Établir un cadre de gouvernance à l'égard du traitement des *Renseignements personnels*.
- Établir les rôles et responsabilités des parties prenantes impliquées dans l'application de la politique.
- Établir des directives pour la gestion des renseignements personnels, lesquelles visent notamment à :
  - ✓ mettre en place des mesures organisationnelles et techniques afin d'assurer la protection des *renseignements personnels*, le tout selon les risques afférents à leur traitement;
  - ✓ mettre en place des mécanismes pour que les personnes concernées puissent exercer leurs droits quant à leurs *Renseignements personnels*, et être informées en conséquence.

2. Définitions, portée, conformité et dérogations

La définition des termes utilisés, soit des mots en italiques et débutant par une majuscule, dans cette politique est consignée dans l'Annexe C prévue à cet effet.

La présente politique s'applique à l'*organisation* Norseco s.e.c. / W.H. Perron. Plus spécifiquement, elle s'applique à ses employés, consultants et fournisseurs (le « *personnel* ») qui traitent des *renseignements personnels* pour le compte de l'*organisation*.

La conformité à cette politique est obligatoire et Norseco s.e.c. / W.H. Perron s'engage à la respecter. Toute demande de dérogation doit être dûment justifiée et doit être présentée au *responsable de la protection des renseignements personnels.*

3. Structure du Cadre de gouvernance

Cette Politique encadre des pratiques en matière de protection des *renseignements personnels* de *l'organisation.* D'autres *politiques* et documents de *directives* découlent de la politique afin de l'appuyer.

- La politique énonce la vision et met en place les principes de protection des *renseignements personnels* de l'*organisation* et ses fondements.
- Afin de soutenir la politique, l'*organisation* a mis en place des *directives* visant à documenter les orientations, les exigences et les attentes, c'est-à-dire le « quoi faire ».
- L'*organisation* peut mettre en place des processus, guides et procédures afin de fournir une liste et une séquence détaillée des activités nécessaires à la mise en œuvre des *directives*.

La protection des *renseignements personnels* passant obligatoirement par la mise en place de mesures de sécurité appropriées et adéquates, la politique doit également être lue et interprétée en corrélation avec la *politique de sécurité de l'information* de l'*organisation* ainsi que ses directives afférentes.

4. Contenu complémentaire pour assurer la protection des renseignements personnels

En plus de la présente politique, Norseco s.e.c. / W.H. Perron met en place une *politique de sécurité de l'information* qui a un rôle complémentaire pour assurer le respect de la protection des renseignements personnels et la conformité réglementaire.

Pour préciser certains sujets et outiller les employés afin qu'ils puissent assurer le respect de la présente politique, voici les directives qui ont également été mises en place:

- Directive sur le transfert de renseignements personnels à l'extérieur du Québec (autres provinces canadiennes et/ou à l'étranger);
- directive sur la rétention des données;
- directive sur l'évaluation des facteurs relatifs à la vie privée;
- directive sur l'obtention de consentement;
- directive de confidentialité – employés;
- directive de confidentialité – recrutement;
- directive sur la gestion des tiers;
- directive sur les droits des individus et la gestion des plaintes;
- directive sur l'usage acceptable des actifs informationnels
- directive sur la destruction, l'anonymisation et la dépersonnalisation de renseignements personnels.

En plus des politiques et directives précédemment nommées, certains guides et procédures pourront être élaborés au besoin par les secteurs concernés pour assurer le respect de la réglementation.

5. Considérations légales et réglementaires

Norseco s.e.c / W.H. Perron fait affaire dans plusieurs provinces canadiennes et est, par conséquent, assujettie à différentes lois et différents règlements provinciaux et fédéraux en matière de protection des *renseignements personnels* (la « *réglementation* »).

- **Au niveau fédéral** : Norseco s.e.c. / W. H. Perron est assujetti à la *LPRPDE* pour les transferts de *renseignements personnels* entre les différentes provinces canadiennes ainsi que pour les autres cas où le droit provincial en matière de protection des *renseignements personnels* ne peut trouver application, par exemple, lorsque les provinces n'ont pas adopté de lois substantiellement similaires à la *LPRPDE*. Norseco s.e.c. / W.H. Perron est également assujettie à la *LCAP*, une loi qui encadre notamment l'envoi de messages électroniques commerciaux tels que les courriels destinés à vendre un produit ou un service et l'installation de témoins de connexion ou de « pixels de suivi ».

- **Au niveau provincial :** Norseco s.e.c. / W. H. Perron est assujetti à la réglementation applicable en matière de protection des *renseignements personnels* des provinces canadiennes à l'intérieur desquelles elle exerce ses activités, lorsque celles-ci impliquent le *traitement* de *renseignements personnels*. Plus spécifiquement et, sans limiter la généralité de ce qui précède, l'organisation est assujettie à la *LPRPSP*, la *PIPAAB* et la *PIPABC*, ainsi qu'à la *LNE*.

6. Principes en matière de protection des renseignements personnels

L'organisation s'engage à implanter, appliquer et maintenir les mesures techniques et organisationnelles nécessaires à la mise en œuvre des principes ci-après énumérés qui s'appliquent aux traitements de renseignements personnels. Ces principes s'alignent avec les exigences de la LPRPDE, de la LPRPSP, de la PIPAAB et de la PIPABC et sont connus comme les « 10 principes relatifs à l'équité dans le traitement de l'information » (les « principes »).

6.1 Premier principe – Responsabilité

L'*organisation* est responsable des *renseignements personnels* dont elle a la gestion. Elle doit nommer une personne qui devra s'assurer de sa conformité à ces principes. Cette personne assume la fonction de *responsable de la protection des renseignements personnels* conformément à la LPRPSP et à la *LPRPDE*.

L'organisation établit et met en place les *documents* appropriés afin d'être en mesure de démontrer sa conformité à la *réglementation*.

6.2 Deuxième principe – Détermination des fins de la collecte des renseignements

Les fins auxquelles des *renseignements personnels* sont recueillis doivent être déterminées par l'*organisation* avant la collecte ou au moment de celle-ci. L'*organisation* ne peut recueillir que les *renseignements personnels* nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

6.3 Troisième principe – Consentement

Toute personne doit être informée de toute collecte, utilisation ou communication de *renseignements personnels* qui la concernent et y consentir y compris la collecte de ses *renseignements personnels* auprès d'un tiers à moins qu'il ne soit pas approprié de le faire. Lorsque des renseignements personnels sont recueillis, l'organisation s'efforce d'obtenir le consentement éclairé, explicite et volontaire de la personne concernée, sauf lorsque la loi l'autorise ou l'exige autrement.
Il peut arriver que l'*organisation* obtienne de tels consentements par le biais de tierces parties, comme des partenaires ou des fournisseurs.

6.4 Quatrième principe – Limitation de la collecte

L'organisation recueille des renseignements personnels de ses clients, fournisseurs, membres et employés dans le cadre de ses activités commerciales et opérationnelles. Les types de renseignements recueillis peuvent inclure, mais sans s'y limiter, les noms, les adresses, les numéros de téléphone, les adresses courriel, les numéros d'identification gouvernementale, les informations financières et les antécédents de crédit.

L'organisation ne recueille que les renseignements personnels nécessaires à la réalisation des fins pour lesquelles ils sont recueillis et s'assure que les personnes concernées en sont informées au moment de la collecte.

L'organisation peut recueillir des renseignements personnels auprès de tiers, tels que des agences d'évaluation de crédit, uniquement avec le consentement de la personne concernée ou si cela est autorisé par la loi.

6.5 Cinquième principe – Limitation de l'utilisation, de la communication et de la conservation

À moins que la personne concernée n'y consente ou que la loi ne l'exige, les *renseignements personnels* ne doivent être utilisés ou communiqués qu'aux fins auxquelles ils ont été recueillis, à moins que la personne concernée n'ait consenti à une utilisation ultérieure ou que la loi ne l'exige. L'organisation ne conserve les *renseignements personnels* qu'aussi longtemps que nécessaire pour répondre à ces fins. De plus, les *renseignements personnels* ne sont utilisés par l'organisation qu'à des fins éthiques.

L'organisation s'engage à ne pas utiliser les renseignements personnels à des fins de marketing direct sans le consentement préalable de la personne concernée. L'organisation peut utiliser les renseignements personnels pour communiquer avec les personnes concernées, gérer les comptes clients et fournisseurs, offrir des produits et services, réaliser des analyses de marché et mener des enquêtes de satisfaction.

L'organisation peut partager les renseignements personnels avec des tiers, tels que des fournisseurs de services et des partenaires commerciaux, seulement dans la mesure où cela est nécessaire à la réalisation des fins pour lesquelles les renseignements ont été recueillis ou si cela est autorisé par la loi.

L'organisation conserve les renseignements personnels aussi longtemps que nécessaire pour atteindre les fins auxquelles ils ont été collectés, à moins qu'une période de conservation plus longue ne soit requise ou autorisée par la loi. Elle établit des périodes de conservation appropriées pour les renseignements personnels qu'elle détient. Ces périodes de conservation sont déterminées en tenant compte des exigences légales, des finalités pour lesquelles les renseignements ont été collectés, ainsi que des besoins opérationnels et commerciaux de l'organisation. Une fois que les renseignements personnels ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés et légalement autorisés, l'organisation prendra les mesures appropriées pour les détruire de manière sécurisée ou les rendre anonymes, sauf si leur conservation ultérieure est requise ou autorisée par la loi.

6.6. Sixième principe – Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que possible afin de satisfaire aux fins auxquelles ils sont destinés. Si les renseignements personnels détenus par l'organisation sont inexacts, incomplets ou périmés, celle-ci procède aux corrections nécessaires dans les meilleurs délais. Si l'organisation refuse une demande de correction, elle informe la personne concernée des motifs de ce refus.

6.7 Septième principe – Mesures de sécurité

Les *renseignements personnels* doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. L'organisation applique à cet effet une ***politique sur la sécurité de l'information***.

Cette politique mentionne notamment que l'organisation reconnaît l'importance de préserver la confidentialité et l'intégrité des renseignements personnels qu'elle détient. L'organisation met en place des mesures de sécurité appropriées pour protéger ces renseignements contre tout accès non autorisé, perte, vol, utilisation abusive, divulgation, altération ou destruction. Ces mesures de sécurité incluent des contrôles physiques, techniques et administratifs raisonnables et appropriés.

Les mesures de sécurité incluent, mais ne se limitent pas à :

- La mise en place de politique et de procédures de sécurité des renseignements personnels pour sensibiliser et former les employés à la gestion sécurisée de ces informations.
- La limitation de l'accès aux renseignements personnels aux seuls employés autorisés qui en ont besoin pour l'exécution de leurs tâches.
- L'utilisation de mots de passe, de pare-feu, de chiffrement et d'autres technologies de sécurité pour protéger les renseignements personnels contre les accès non autorisés.
- La sauvegarde régulière des données afin d'assurer leur disponibilité en cas de perte ou de destruction accidentelle.
- La surveillance continue des systèmes informatiques et des réseaux pour détecter et prévenir les violations de sécurité.

Confidentialité en ligne

Si l'organisation collecte des renseignements personnels par le biais de son site web ou d'autres plateformes en ligne, elle met en place des mesures appropriées pour protéger la confidentialité de ces informations, telles que des certificats de sécurité SSL, des pare-feux et des protocoles de cryptage. L'organisation informe les utilisateurs de ses sites web sur la collecte et l'utilisation des renseignements personnels, les «cookies» (témoins) et les technologies similaires utilisées.

En cas de violation de données personnelles, l'organisation s'engage à prendre les mesures appropriées pour remédier à la situation. Cela inclut la notification rapide des personnes concernées, des autorités compétentes et, le cas échéant, de l'Office de la protection du consommateur du Québec, conformément aux exigences légales en vigueur.

L'organisation encourage les personnes concernées à jouer un rôle actif dans la protection de leurs renseignements personnels. Elle les informe de l'importance de maintenir la confidentialité de leurs informations d'identification, de choisir des mots de passe robustes et de signaler toute activité suspecte ou toute violation de sécurité.

6.8 Huitième principe – Transparence

L'organisation s'assure que sa politique de protection des renseignements personnels soit facilement accessible au public. L'*organisation* peut également mettre à la disposition de ceux qui en font la demande ses autres politiques et directives en matière de protection des renseignements personnels.

En mettant en place des mesures d'accès et de correction des renseignements personnels, l'organisation démontre son engagement envers la transparence, l'exactitude et l'intégrité des données personnelles qu'elle détient, conformément aux exigences de la Loi 25 et aux droits des individus sur leurs informations personnelles.

6.9 Neuvième principe – Accès aux Renseignements personnels

L'organisation informe toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettent de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements personnels et d'y faire apporter les corrections appropriées.

Divulgation interne

L'organisation s'engage à limiter l'accès aux renseignements personnels aux seuls employés qui en ont besoin pour remplir leurs responsabilités. La divulgation interne de renseignements personnels est strictement contrôlée et surveillée.

Divulgation externe
L'organisation ne divulgue les renseignements personnels à des tiers qu'avec le consentement de la personne concernée, sauf lorsque la loi l'exige ou l'autorise. Lorsque des renseignements personnels sont divulgués à des tiers, l'organisation prend des mesures pour s'assurer que ces tiers offrent un niveau de protection adéquat des renseignements personnels.

L'organisation reconnaît le droit des personnes concernées d'accéder à leurs renseignements personnels détenus par l'organisation et de demander des corrections si ces renseignements sont inexacts, incomplets ou périmés. Pour exercer leur droit d'accès ou de correction, les personnes concernées peuvent soumettre une demande écrite ou orale à l'organisation. Cette demande doit être accompagnée de suffisamment de détails permettant d'identifier les renseignements personnels en question et de valider l'identité du demandeur.

L'organisation répond aux demandes d'accès et de correction dans les délais prescrits par la Loi 25. Lorsqu'une demande d'accès est reçue, l'organisation fournit à la personne concernée une copie de ses renseignements personnels dans un format compréhensible, sauf si la loi permet ou exige autrement. L'organisation veille à ce que les procédures d'accès et de correction des renseignements personnels soient claires, transparentes et facilement accessibles aux personnes concernées. Elle s'engage à fournir un soutien adéquat et à répondre à toutes les questions et préoccupations liées à l'accès et à la correction des renseignements personnels.

6.10 Dixième principe – Possibilité de porter plainte à l'égard du non-respect des principes

Toute personne est en droit de se plaindre du non-respect par l'organisation des principes énoncés ci-dessus. Les plaintes à l'égard du non-respect de ces principes sont adressées au responsable de la protection des renseignements personnels.

7. Formation et sensibilisation

La formation et la sensibilisation des employés en ce qui concerne la protection des renseignements personnels sont cruciales afin que l'organisation soit en mesure d'assurer le respect des principes énoncés à la politique ainsi que ses obligations juridiques et contractuelles en matière de protection des renseignements personnels. Par conséquent, l'organisation applique un programme de formation et de sensibilisation. L'organisation s'engage à fournir une formation à ses employés sur la protection des renseignements personnels, les lois en vigueur et les politiques internes associées. Cette formation vise à sensibiliser les employés à l'importance de la confidentialité et de la sécurité des renseignements personnels et à leur fournir les connaissances nécessaires pour les traiter correctement.

8. Maintenance de la politique

L'organisation s'assure qu'elle maintient, mesure, analyse, évalue et mène des révisions ponctuelles de la Politique, des procédures afférentes ainsi que de ses pratiques en matière de protection des renseignements personnels. Des mises à jour sont donc effectuées au besoin, en tenant compte des changements législatifs, technologiques et opérationnels, ainsi que de meilleures pratiques en matière de protection des données. L'organisation s'assure qu'une vigie de la réglementation soit effectuée afin de prendre en compte adéquatement tout changement en la matière.

La Politique doit être revue au minimum annuellement par le comité d'audit de l'organisation. Les modifications importantes de la politique sont communiquées aux personnes concernées de manière appropriée et l'organisation

rend disponible la version la plus récente de la politique aux employés de la façon jugée appropriée ainsi que sur son site web.

9. Mise en application

*L'*organisation met en place des mécanismes permettant d'évaluer l'adoption et l'efficacité de la politique, de ses directives et de tout autre document qui en découle. Ces mécanismes permettent d'assurer l'amélioration continue en matière de protection des renseignements personnels de l'organisation.

La conformité à la politique est obligatoire pour l'ensemble des employés. L'employé qui ne se conforme pas est sujet à des mesures disciplinaires pouvant aller de l'avis disciplinaire au congédiement ou aux mesures et pénalités contractuelles prévues pour les consultants et les fournisseurs, lesquelles peuvent notamment prévoir la résiliation du contrat et la réclamation de dommages-intérêts. De la formation et de la sensibilisation supplémentaire peuvent également être offertes en cas de défaut de respecter la politique.

10. Organisation de la protection des renseignements personnels

10.1 Responsabilités du conseil d'administration de l'organisation

- Approuver les orientations stratégiques visant la protection des renseignements personnels;
- approuver la politique ainsi que toute autre politique importante découlant de la présente politique incluant leurs modifications et appuyer leurs applications à travers l'organisation;
- demeurer informé du niveau de maturité de l'*organisation* et des risques relatifs à la protection des renseignements personnels; et
- veiller à ce que soient octroyées les ressources suffisantes pour que l'organisation puisse se conformer en continu à la *réglementation.*

10.2 Directeur général

Le Directeur général est le plus haut dirigeant opérationnel de l'organisation et plus largement de l'organisation et à ce titre, en vertu de la *LPRPSP*, il est responsable de la protection des renseignements personnels des secteurs composant l'organisation.

Le directeur général est autorisé par le conseil d'administration de l'organisation à déléguer toutes ou une partie de cette fonction par le biais d'une délégation écrite de la fonction de responsable de la protection des renseignements personnels joint en annexe «A» de la présente politique.

10.3 Responsabilités du responsable de la protection des renseignements personnels

Le responsable effectue le suivi de l'exécution de la politique, se dote d'un plan d'action visant à gérer les risques de façon organisée et fait les suivis pour assurer une amélioration continue de la gestion des renseignements personnels au sein de l'organisation.

Aux fins de l'accomplissement de son mandat, le responsable dispose d'un pouvoir exécutif ou décisionnel relativement à

- La coordination des redditions de compte, ainsi que des exercices de surveillance et d'analyse de la conformité des employés, afin d'en faire rapport au comité d'audit de l'organisation;

- l'établissement d'un mécanisme d'évaluation de la conformité de l'organisation à la réglementation, à la fréquence et avec les métriques et les seuils de tolérance qu'il détermine;
- l'approbation et la coordination des demandes de dérogation;
- la coordination des réponses auprès des organismes de réglementation;
- la coordination de la rédaction, la révision, l'approbation et les modifications des politiques, directives et de tout autre document qui concerne la protection des renseignements personnels;
- l'établissement d'une méthode de documentation des décisions et des actions prises dans le cadre de son mandat et notamment quant à l'acceptation des risques, les remédiations et les suivis;
- de manière générale, faire des recommandations au comité d'audit de l'organisation quant à toute matière qui relève de son mandat.

Le responsable de la protection des renseignements personnels a également pour responsabilité d'

- assurer le respect et la mise en œuvre de la politique, des *directives* et de la réglementation applicable par la mise en place des mécanismes nécessaires afin de surveiller l'évolution du déploiement des pratiques de protection des renseignements personnels;
- effectuer la gestion courante des risques, effectuer des ajustements progressifs et vérifier ponctuellement l'adhésion à la politique,
- supporter le déploiement des directives applicables par l'attribution de ressources humaines, financières, technologiques;
- supporter la conduite des évaluations des facteurs relatifs à la vie privée conformément aux directives et *à la* réglementation applicables;
- effectuer une reddition de compte périodique au Comité d'audit sur les enjeux et les risques associés à la protection des renseignements personnels en incluant les non-conformités et les plans d'action afférents;
- capter et signaler au Comité d'audit les risques qui sont au-dessus du seuil de tolérance établi;
- analyser et approuver toute demande de dérogation;
- assurer sa formation continue afin d'exécuter ses responsabilités adéquatement;
- toute autre responsabilité lui étant attribuée par la réglementation et les directives.

10.4 Responsabilités des secteurs

Chaque secteur, en collaboration avec le responsable de la protection des renseignements personnels, est responsable :

- De soutenir le responsable de la protection des renseignements personnels dans la reddition de compte au comité d'audit;
- de mettre en place les capacités requises, aussi humaines, financières, que technologiques afin de déployer les pratiques en matière de protection des renseignements personnels (le « comment faire »);
- les secteurs sont responsables de suivre la conformité de la présente politique, des directives et autres documents qui en découlent, ainsi qu'à la réglementation.

Annexe «A»
Modèle

Délégation de la fonction de responsable de la protection des renseignements personnels

ATTENDU QUE la *Loi modernisante des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c. 25 sanctionnée le 22 septembre 2021 apporte des modifications à la Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c. P-39.1 (« **LPRPSP** ») lesquelles entrent en vigueur progressivement jusqu'en septembre 2024.

ATTENDU QUE la LPRPSP, à son article 3.1, lequel entrera en vigueur le 22 septembre 2022, rend responsable toute personne morale de la protection des renseignements personnels qu'elle détient.

ATTENDU QUE cet article spécifie également que la personne ayant la plus haute autorité au sein de l'entreprise doit veiller à assurer le respect et la mise en œuvre de la LPRPSP et que cette personne exerce la fonction de responsable de la protection des renseignements personnels.

ATTENDU QU'au sein de Norseco s.e.c. / W.H. Perron, la direction générale est la personne ayant la plus haute autorité.

ATTENDU QUE, l'article susmentionné prévoit également que cette fonction peut être déléguée par écrit, en tout ou en partie, à toute personne.

***

Par conséquent, conformément à la disposition susmentionnée et à titre de directeur général de Norseco s.e.c / W.H. Perron, je délègue l'intégralité de la fonction de responsable de la protection des renseignements personnels ainsi que les pouvoirs afférents à Monsieur Benoit Plante, responsable de la loi 25.

Cette délégation s'accompagne également de la responsabilité pour Monsieur Benoit Plante, responsable de la loi 25, de rendre compte à moi-même, sur demande, et conformément à la politique de protection des renseignements personnels, des risques liés à la protection des renseignements personnels au sein de Norseco s.e.c. / W.H. Perron, des mesures de mitigation prises et de l'état des travaux afférents.

Les pouvoirs et responsabilités délégués par les présentes peuvent également être sous délégués en tout ou en partie, par écrit, conformément aux modalités prévues à la LPRPSP et sous réserve de l'autorisation du soussigné.

SIGNÉ à Laval, ce 11e jour de septembre 2023.

Christian Chartrand
Directeur général

Annexe «B»

Termes	Définitions
Actif informationnel	Toute information, *donnée* ou *métadonnée* que possède l'organisation (à titre de propriétaire ou de simple possesseur), peu importe son support (papier, électronique ou autre), ainsi que les *systèmes d'information*.
Actif informatique	Ensemble des systèmes et équipements technologiques de l'*organisation* utilisés pour *traitement*, utilisation, stockage, conservation et communication des *actifs informationnels.*
Confidentialité	La *confidentialité* est le caractère réservé d'une information ou d'un *traitement* dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou p*rocessus* autorisés.
Confidentiel(le)	Caractéristique d'un fichier, d'un *document*, d'un média ou d'une information, *donnée*, ou *métadonnée*, qui, par sa nature ou en raison des exigences de l'*organisation*, de la loi et des règlements, des contrats, des *directives* ou des *normes*, n'est et ne doit être ni disponible au public, ni divulguée aux personnes, entités ou *processus* non autorisés.
Rétention	Se définit comme la possession continue, l'utilisation ou le contrôle d'un *actif informationnel,* y compris d'un *renseignement personnel*, par l'*organisation,* ou une *tierce partie* pour le compte de l'*organisation*.
Consultant	Désigne habituellement un non-salarié qui a accès à un *actif informationnel* de l'*organisation* et qui occupe une fonction normalement attribuée à un *employé*. Il se distingue d'un *fournisseur* de service qui peut réaliser des activités à distance.
Dérogation	*Processus* de *demande* au comité de la vie privée qui permet d'outrepasser une exigence de protection des renseignements personnels. Une *dérogation* doit être formellement approuvée par le comité de la vie privée à la suite d'une analyse des *risques* et à l'identification des mesures compensatoires.
Destruction	Réfère à l'action de procéder à la *destruction* physique d'un média ou d'un support contenant des *actifs informationnels* de façon sécuritaire. Généralement, celle-ci peut consister au déchiquetage, à la désintégration, l'incinération, la pulvérisation, ou la fonte du support ou du média. Elle est généralement effectuée par le biais de *fournisseurs* de services.
Demandes	Toutes *demandes* d'exercice d'un droit (ex. : droit d'accès, de rectification, de mise à jour, de désindexation, de suppression, d'information, etc.) ou plaintes effectuées par une personne physique en vertu d'une loi ou d'un règlement en matière de protection des *Renseignements personnels* à l'égard de l'*organisation*.
Directive	Découle d'une politique et en précise le cadre. Un *document* corporatif ou départemental et précise les règles de conduite internes, les objectifs opérationnels à atteindre, le partage et les responsabilités entre les différentes unités d'affaires.

Document	Signifie les politiques, *directives, normes, processus,* guides et *procédures* détaillant la structure, les *processus* et contrôle de l'*organisation*. Les *documents* comprennent également les copies papiers et format numérique.
Donnée	Une *donnée* est un fait, une valeur ou une variable quantitative ou qualitative portant sur une chose ou un individu, qui, prise seule, peut ne pas avoir de signification particulière. La *donnée* peut également être agrégée dans un ensemble de *données*.
Employé	Désigne tout individu qui travaille pour le compte de l'*organisation* quel que soit son statut d'emploi (stagiaire, étudiant ou salarié permanent/temporaire).
Évaluation des facteurs relatifs à la vie privée	Analyse permettant d'identifier et de considérer tous les facteurs pouvant avoir un impact positif ou négatif pour le respect de la vie privée des personnes concernées et de suggérer des stratégies pour éviter ou mitiger les *Risques* identifiés. Cette définition réfère également aux *Évaluation des facteurs relatifs à la vie privée* prévues aux articles 3.3, 17 et 21 de la LPRPSP.
Fournisseur	Un *Fournisseur* est une personne physique ou morale qui fournit des biens ou des services à l'*organisation*. Ceci inclut, notamment les entrepreneurs et sous-entrepreneurs, les *Partenaires* (partenaires d'affaires), les prestataires de services et représentants qui utilisent habituellement leurs propres équipements informatiques. Les *consultants* sont expressément exclus de cette définition.
LCAP	Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique, modifiant la loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la loi sur la concurrence, la Loi *sur la protection des renseignements personnels* et la loi sur les télécommunications, LC 2010, c 23, communément appelée, la « *Loi canadienne antipourriel* ».
LNE	*Loi de 2000 sur les normes d'emploi* en Ontario, y compris les exigences ajoutées le 11 avril 2022 en matière de *Surveillance* électronique.
LPRPDE	*Loi sur la protection des renseignements personnels et documents électroniques*, LC 2000, c 5
LPRPSP	*Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1
Mesure de sécurité (de contrôle)	Dans le contexte d'une *Politique* ou d'une *Directive*, moyen concret qui assure, partiellement ou totalement, la protection des *Actifs informationnels* contre une ou plusieurs *Menaces* informatiques, et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces *Menaces* ou à minimiser les pertes qui en résultent.
Non-conformité	*Non-conformité* à un encadrement qui fait l'objet d'un plan d'action visant à mettre en place un correctif dans un délai défini, lorsque le *Risque* est moyen, élevé ou très-élevé.
Norme (voir *Standard*)	Les *normes* sont une description de bas niveau de la manière dont l'*organisation* appliquera sa stratégie en matière de *sécurité de l'information*. En d'autres termes, elles sont utilisées pour maintenir un niveau minimum de sécurité efficace. Elles sont également obligatoires. Les

	normes découlent des *directives*. Elles peuvent varier selon la ligne d'affaires, la *division* ou la *filiale* concernée.
Organisation	Désigne la firme Norseco s.e.c. / W.H. Perron.
Organisme de réglementation	Réfère aux organismes désignés à la réglementation applicable à l'organisation en matière de protection des renseignements personnels pour veiller à son application. Cette définition inclut la commission d'accès à l'information du Québec, le Commissariat à la vie privée du Canada, le Commissariat à l'information et à la protection de la vie privée de l'Alberta et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique.
Partenaire	Individu ou groupes d'individus qui participent aux activités de l'*organisation* sans détenir le statut d'Employés, de consultants ou de fournisseurs. Dans certains cas, les activités d'un partenaire peuvent requérir l'utilisation d'un actif informationnel, propriété de l'organisation.
Personnel	Terme générique utilisé pour référer aux employés, consultants et fournisseurs de l'organisation.
PIPAAB	*Personal Information Protection Act*, SA 2003, c P-6.5
PIPABC	*Personal Information Protection Act*, SBC 2003, c 63
Politique de protection des renseignements personnels	Document qui sert de guide et de cadre aux décisions en matière de protection des renseignements personnels. La politique précise les grands principes et lignes directrices de l'organisation. Elle est approuvée par le conseil d'administration.
Politique de sécurité de l'information	Document qui sert de guide et de cadre aux décisions. La politique précise les grands principes et lignes directrices de l'organisation en matière de sécurité de l'information. Elle est approuvée par le conseil d'administration.
Procédure (voir *Processus*)	Une procédure décrit et formalise les tâches à accomplir pour mettre en œuvre le processus. Si la procédure n'est pas respectée, les données de sorties du processus ne seront pas conformes aux exigences attendues : elle précise le quoi, le comment, le quand et les intervenants. Les procédures viennent supporter les directives. Elles sont généralement approuvées par les directions ou services concernés.
Processus (voir *Procédure*)	Le processus est un ensemble d'opérations, décomposables en tâches, en vue d'un résultat déterminé. Un processus est une suite d'actions qui ne sont pas séquentielles comme l'est une procédure. Il se définit par sa nature transactionnelle: « produire X », « concevoir Y», «transporter Z de A à B», «facturer les prestations XYZ », etc. Les processus viennent supporter les directives. Elles sont généralement approuvées par les directions ou services concernés.

Programme de conformité	Programme visant à mettre en place et exécuter une stratégie relativement à la conformité et la gestion des risques en matière de renseignements personnels
Réglementation	Réfère aux lois et règlements en matière de protection des renseignements personnels applicables à l'organisation. La *LPRPDE*, la *LPRPSP*, la *LCAP*, la *PIPAAB,* la *PIPABC*, la *LNE* et leurs règlements font notamment partie de cette définition.
Renseignement	Un renseignement constitue une donnée renseignant sur quelque chose ou quelqu'un. Par exemple, un numéro de téléphone ou un nom sont des renseignements.
Renseignements personnels	Constitue tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier (ex. : nom, prénom, adresse postale, numéro de téléphone, numéro d'assurance sociale, etc.).
Responsable de la protection des renseignements personnels	Désigne le gestionnaire responsable de veiller à assurer le respect et la mise en œuvre de la politique de protection des renseignements personnels et de la réglementation de sa division. Son mandat est prévu dans la politique de protection des renseignements personnels et dans la réglementation de sa division.
Risque	Incidence potentielle d'un événement pouvant affecter négativement les activités de l'organisation *ou* nuire d'une quelconque façon à l'exécution de son mandat. L'évaluation d'un niveau de risque tient compte de la plausibilité d'un événement et de la *Criticité* de son impact potentiel sur l'organisation.
Tierce(s) Partie(s)	Acteur(s) ou organisation(s) collaborant directement ou indirectement avec l'organisation et disposant d'un accès aux actifs informationnels. Tierces parties inclut, mais non exhaustivement les fournisseurs, les vendeurs et les consultants.
Traitement (verbe traiter)	Signifie toute collecte, utilisation, communication, conservation, destruction ou tout autre type de manipulation de renseignements personnels.
Utilisateur	Toute personne qui utilise des actifs informationnels de l'organisation, incluant, mais ne se limitant pas aux employés, stagiaires, consultants ou fournisseurs.