1. OBJET

Le présent document a pour objet de décrire les modalités de protection des renseignements personnels en application chez DUCHESNE ET FILS LTÉE (ci-après « l'Entreprise »).

Les prescriptions de la présente politique s'appliquent exclusivement aux activités d'affaires réputées comme normales de l'Entreprise, effectuées dans le cadre de ses opérations.

Ces prescriptions s'adressent à toute personne pouvant être en contact avec des renseignements personnels, dans le cadre d'activités impliquant directement ou indirectement l'Entreprise.

Les objectifs de cette politique sont :

- Assurer la conformité de l'Entreprise aux obligations de Loi sur la Protection des Renseignements Personnels dans le secteur privé (R.L.R.Q, c. P-39.1, ci-après « LPRPSP »).
- Protéger les droits du personnel, des clients et des partenaires de l'Entreprise en vertu des articles 35 à 40 du Code civil du Québec en matière de protection des renseignements personnels.
- Prévenir les risques à la disponibilité, l'intégrité ou la confidentialité des renseignements personnels détenus, utilisés ou entreposés par l'Entreprise dans le cadre de ses activités.

Ce document contient des Informations classifiées comme étant **INTERNES**. Son contenu ne doit pas être diffusé ou distribué à l'extérieur de l'Entreprise et doit faire l'objet de contrôles appropriés à son classement.

2. RESPONSABILITÉ DE LA POLITIQUE

La responsabilité de la mise en œuvre de cette politique incombe au Président et Chef de la direction.

La responsabilité de supervision en vue de la conformité de cette politique revient conjointement au Directeur des services informatiques et à la Spécialiste assurance qualité (RPRP).

3. DÉFINITIONS

- **Autorisation :** permission d'effectuer une action spécifique.
- **Confidentialité**: propriété d'une information qui est accessible seulement par les personnes autorisées.
- **Confidentiel** : catégorie de classification de l'information à risque élevé, disponible à l'intérieur des secteurs désignés de l'Entreprise et qui, si elle est révélée, peut définitivement porter atteinte à l'intégrité financière, judiciaire, physique ou morale de l'Entreprise ou de ses employés, fournisseurs et clients.
- **Classification de l'information** : processus de distribution de l'information selon des catégories prédéfinies.
- **Disponibilité**: propriété d'une information pouvant être utilisée en temps voulu et de manière adéquate par les personnes autorisées.
- **Incidents:** tout événement qui compromet potentiellement la confidentialité, l'intégrité, la disponibilité ou qui constitue une déviation significative des fonctions normales d'un système d'information contenant des renseignements personnels.
- **Information :** ensemble de données susceptibles d'être conservées, traitées ou communiquées.
- **Intégrité**: propriété d'une information n'ayant pas été altérée, modifiée ou détruite sans autorisation.
- **Interne** : catégorie de classification de l'information à risque moyen, disponible à l'intérieur des secteurs désignés de l'entreprise et qui, si elle est révélée, peut potentiellement porter atteinte à l'intégrité financière, judiciaire, physique ou morale de l'Entreprise ou de ses employés, fournisseurs et clients.
- **Publique** : catégorie de classification de l'information à faible risque, disponible au grand public et qui, si elle est révélée, est sans atteinte à l'intégrité financière, judiciaire, physique ou morale de l'Entreprise ou de ses employés, fournisseurs et clients.
- **Système d'information:** ensemble de supports (physiques ou numériques) ayant pour fonction la conservation, le traitement ou la communication d'information.
- **Tierce partie**: personne ou entreprise qui ne possède pas de lien d'emploi contemporain avec l'Entreprise.
- **DUCHESNE ET FILS LTÉE** : ensemble regroupant les compagnies DUCHESNE ET FILS LTÉE et toute autre entreprise externe ayant fait l'objet d'une acquisition.
- **Renseignements personnels:** En vertu de la Loi sur la protection des renseignements personnels dans le secteur privé, un renseignement personnel « est […] tout renseignement qui concerne une personne physique et permet de l'identifier » (R.L.R.Q., c. P-39.1, a.2).

  Renseignement personnel d'une personne (considérez si le renseignement est mentionné avec un autre renseignement concernant une personne ou lorsque sa seule mention révélerait l'identité de la personne concernée) :

- Nom;
- Numéro d'assurance sociale;
- Numéro de permis de conduire;
- Numéro d'assurance maladie;
- Adresse;
- Numéro de téléphone;
- Numéro matricule;
- Âge;
- Genre;
- Race, nationalité ou origine ethnique;
- Religion :
- État civil;
- Antécédents médicaux, scolaires ou professionnels;
- Identifiants en ligne;
- Numéro d'identification d'employé;
- Informations bancaires ou de cartes de crédit;
- Informations collectées permettant la vérification d'identité impliquant la biométrie;
- Informations permettant de géolocaliser une personne.

S'ajoutent à la liste plusieurs éléments propres à son identité physique (dont la photographie), physiologie, génétique, psychique, santé, économique, culturelle ou sociale.

Informations qui ne sont pas considérées comme des renseignements personnels:

- Renseignements qui ne concernent pas directement un individu (ex. code postal);
- Renseignements sur une entreprise;
- Renseignements anonymisés (dans la mesure qu'il est impossible de les relier à une personne identifiable);
- Renseignements gouvernementaux.

4. DROITS DES INDIVIDUS

a. L'Entreprise respecte les droits des individus concernant la protection des renseignements personnels, dans les limites des lois et réglementations. Les individus ont le droit:

   i. D'être informé du traitement de leurs données personnelles;

   ii. De savoir comment, quand et pourquoi leurs données personnelles sont partagées;

   iii. D'avoir accès à leurs données;

   iv. D'être oubliés;

v. De pouvoir recevoir une copie de leurs données personnelles;

vi. De refuser des services tels que la prise de décision automatisée, de recevoir des chaînes de courriels, et autres messages électroniques;

vii. De faire rectifier leurs données si elles sont inexactes;

viii. De limiter le traitement de leurs données.

ix. De se voir demander le consentement lorsque des données personnelles sont divulguées ou demandées à des tierces parties, si elles ne sont pas clairement exemptées par la loi.

b. L'Entreprise doit s'assurer de nommer un responsable de la protection des renseignements personnels qui répondra des droits individuels, du traitement des demandes et des plaintes en matière de renseignements personnels dans les délais prescrits par les lois et les réglementations en vigueur.

c. L'Entreprise doit s'assurer que les personnes sont conscientes que leurs données sont traitées et qu'elles comprennent comment elles peuvent exercer leurs droits.

d. L'Entreprise assure la récupération, la correction ou la suppression sécurisée des données suivant la réception d'une demande. Elle pourrait refuser une demande avec justification ou dans les limites de la Loi.

e. Un registre des demandes et des plaintes sera maintenu.

5. PROCESSUS DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

5.1 Rôles et responsabilités

Les rôles et responsabilités décrits ci-dessous sont requis par la LPRPSP. L'Entreprise a donc l'obligation de désigner des personnes occupant ces rôles. Un comité de gestion de la protection des renseignements personnels peut également être mis sur pied selon les besoins légaux, contractuels et contextuels de l'Entreprise.

5.1.1 Autorité exécutive de l'Entreprise

a. Doit absolument être la personne la plus en autorité de l'Entreprise;

b. Mise en œuvre des politiques et procédures en matière de protection des renseignements personnels;

c. Supervision en vue de conformité des politiques et procédures en matière de protection des renseignements personnels;

d. Nomination d'un délégué responsable de la protection des renseignements personnels;

e. Approbation des plans d'action et de distribution de ressources humaines et financières.

5.1.2 Délégué responsable de la protection des renseignements personnels

a. Documentation des incidents de confidentialité;

b. Maintien d'un registre des incidents de confidentialité;

c. Signalement des divulgations accidentelles des renseignements personnels aux autorités compétentes;

d. Compréhension et application de la législation portant sur la protection des renseignements personnels;

e. Formation continue et sensibilisation des employés dans le cadre du Programme de protection des renseignements personnels;

f. Participation aux exercices d'évaluation des facteurs relatifs à la vie privée (E.F.V.P.);

g. Gestion des demandes d'accès à l'information;

h. Gestion des plaintes concernant la protection des renseignements personnels.

5.1.3 Employés, fournisseurs et autres tierces parties

a. Adhésion aux règles de gouvernance en matière de protection des renseignements personnels;

b. Participation au Programme de formation et de sensibilisation à la protection des renseignements personnels;

c. Signalement des incidents de confidentialité suspectés ou confirmés.

5.2 Obligations

Les obligations décrites ci-dessous sont décrites explicitement ou implicitement par la LPRPSP. L'Entreprise et son Programme de protection des renseignements personnels est contrainte de respecter ces obligations.

5.2.1 Générales

a. L'Entreprise a l'obligation de nommer une personne responsable du respect des lois applicables en matière de protection des renseignements personnels. Les coordonnées (courriel et téléphone) de cette personne sont publiées sur le ou les sites web de l'Entreprise.

b. L'Entreprise a l'obligation de protéger tous renseignements personnels, sans égard au support (physique ou numérique) ou à l'état (au repos, en transit ou en utilisation), requis par un ou plusieurs de ses processus d'affaires.

c. L'Entreprise a l'obligation de respecter tous les principes de protection des renseignements personnels édictés dans la LPRPSP et de leur démonstration dans le cadre d'évaluations ou d'audits.

d. L'Entreprise a l'obligation de rendre publiquement accessibles les renseignements précis sur ses politiques et ses pratiques concernant la protection des renseignements personnels.

e. L'Entreprise a l'obligation d'apporter les modifications pertinentes à son programme de protection des renseignements personnels selon la ratification, modification ou suppression des lois applicables.

5.2.2 Collecte de renseignements personnels

a. L'Entreprise a l'obligation de déterminer *a priori* les fins utiles des renseignements personnels avant toute collecte, utilisation, communication ou divulgation (non-accidentelle) de renseignements personnels.

b. L'Entreprise a l'obligation d'informer et d'obtenir *a priori* le consentement de tout individu visé par une collecte, une utilisation, une communication ou une divulgation (non-accidentelle) de renseignements personnels à moins qu'il ne soit pas approprié de le faire.

c. L'Entreprise a l'obligation de ne recueillir que les renseignements personnels qu'elle peut démontrer comme étant utiles à un ou des processus d'affaires de l'Entreprise.

d. L'Entreprise a l'obligation de détruire ou rendre anonymes les renseignements personnels une fois qu'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été recueillis.

e. L'Entreprise a l'obligation de divulguer l'existence, la nature et l'utilisation faites des renseignements personnels sous sa responsabilité, au propriétaire des renseignements personnels visés qui en fait la demande.

f. L'Entreprise a l'obligation de permettre la consultation des renseignements personnels sous sa responsabilité au propriétaire des renseignements personnels visés qui en fait la demande.

5.2.3 Inventaire des renseignements personnels

a. L'Entreprise a l'obligation de créer, mettre en place, documenter et maintenir un inventaire des renseignements personnels sous sa responsabilité. Cet inventaire doit traiter des caractéristiques suivantes pour chacun des renseignements personnels sous sa responsabilité:

i. Lieux d'entreposage
ii. Description des renseignements personnels
iii. Support utilisé pour la conservation
iv. Types de renseignements personnels
v. Schéma d'accès aux renseignements personnels visés
vi. Classification des renseignements personnels
vii. Liste des contrôles appliqués aux renseignements personnels visés

viii. Durée de conservation maximale
ix. Méthode de destruction prescrite

b. L'Entreprise a l'obligation de maintenir l'exactitude des renseignements personnels contenus dans l'inventaire.

c. L'Entreprise a l'obligation de maintenir l'exactitude de l'inventaire visant les renseignements personnels afin de satisfaire aux exigences législatives en matière d'utilisation, de conversation et de destruction des renseignements personnels.

5.2.4 Protection des renseignements personnels

a. L'Entreprise a l'obligation de créer, mettre en place, documenter et maintenir un processus de gestion du risque appliqué à la protection des renseignements personnels. Ce processus de gestion des risques doit traiter des caractéristiques suivantes pour chacun des risques:

i. Date d'identification
ii. Personne rapportant
iii. Type de menace
iv. Type de vulnérabilité
v. Actifs informationnels visés
vi. Mesure d'impact du risque
vii. Mesure de probabilité du risque
viii. Contrôles de sécurité en place
ix. Identification des risques résiduels
x. Contrôles de sécurité à mettre en place
xi. Plan d'action sur le risque résiduels
xii. Responsable du risque visé

b. L'Entreprise a l'obligation de mettre en place et d'utiliser les contrôles de sécurité nécessaires et prescrits par niveau de classification des renseignements personnels.

c. L'Entreprise a l'obligation de mesurer l'efficacité des contrôles de sécurité en place en tout temps.

d. L'Entreprise a l'obligation d'utiliser et de maintenir les systèmes, les outils technologiques et l'expertise nécessaires à la protection des renseignements personnels.

e. L'Entreprise a l'obligation de créer, mettre en place et entretenir un schéma d'accès aux renseignements personnels restrictif. Ce schéma doit veiller à ce que les individus aient seulement un accès minimal aux renseignements personnels nécessaires à l'accomplissement de leurs tâches, et seulement en temps opportun. Ce schéma d'accès doit traiter des caractéristiques suivantes pour chacun des accès:

i. Individu ou groupe visé par l'accès
ii. Renseignement personnel visé par l'accès
iii. Type de renseignement personnel
iv. Type de support contenant le renseignement personnel
v. Type d'accès (écriture / lecture / suppression)
vi. Date d'entrée en fonction de l'accès
vii. Dernière date de modification de l'accès
viii. Date de péremption de l'accès

5.2.5 Utilisation des renseignements personnels

a. L'Entreprise a l'obligation de s'assurer que les renseignements personnels ne soient pas utilisés autrement que de la manière déclarée lors de la collecte de ces renseignements personnels.

b. L'Entreprise a l'obligation de ne pas vendre, louer ou échanger les renseignements personnels sans le consentement explicite du propriétaire des renseignements personnels.

c. L'Entreprise a l'obligation d'obtenir le consentement du responsable à la protection des renseignements personnels avant toute communication interne ou externe des renseignements personnels.

d. L'Entreprise a l'obligation de mettre en place, d'utiliser et de maintenir les processus formels et nécessaires à la communication interne et externe des renseignements personnels. Cette obligation contient des exceptions prévues par les lois et réglementations en vigueur.

e. L'Entreprise a l'obligation de mettre en place, d'utiliser et de maintenir une liste de tous les tierces parties impliquées dans la collecte, le traitement ou la communication des renseignements personnels. Cette liste doit traiter des caractéristiques suivantes pour chacune des tierces parties:

i. Tierces parties visées par l'accès
ii. Renseignement personnel visé par l'accès
iii. Type de renseignement personnel
iv. Type de support contenant le renseignement personnel
v. Localisation géographique du stockage du renseignement personnel chez la tierce partie
vi. Type d'utilisation du renseignement personnel
vii. Type d'accès (écriture / lecture / suppression)
viii. Date d'entrée en fonction de l'accès
ix. Date de péremption de l'accès

f. L'Entreprise a l'obligation d'utiliser des ententes contractuelles avec les tierces parties encadrant toute action affectant les renseignements personnels sous la

responsabilité de l'Entreprise. Ces ententes définissent les obligations et les responsabilités de chacune des parties.

5.2.6 Transfert de données hors du Québec

a. L'Entreprise a l'obligation de limiter le transfert de renseignements personnels transfrontaliers sans égard au support.

b. L'Entreprise a l'obligation, dans l'inévitabilité d'un transfert de renseignements personnels transfrontalier, d'informer le propriétaire des renseignements personnels et d'obtenir son consentement *a priori*.

c. L'Entreprise a l'obligation de veiller à ce que toutes les exigences légales pour les transferts de renseignements personnels transfrontaliers soient respectées avant qu'un transfert ait lieu. Une évaluation des facteurs de la vie privée (E.F.V.P.) sera produite pour chaque cas.

5.2.7 Portabilité des données

a. Pour donner suite à une demande écrite du propriétaire des renseignements personnels, l'Entreprise a l'obligation de lui communiquer, dans un format technologique structuré et couramment utilisé, un renseignement personnel informatisé que l'Entreprise a en sa possession.

b. La communication du renseignement personnel pourra aussi se faire à une personne ou à un organisme autorisé à recueillir le renseignement, à la demande du propriétaire du renseignement personnel visé.

5.3 Consentement

Avant de procéder à la collecte, l'utilisation, la communication ou à la divulgation volontaire de renseignements personnels, l'Entreprise doit obtenir le consentement du propriétaire des renseignements personnels visés.

5.3.1 Caractéristiques du consentement

a. L'Entreprise a l'obligation d'obtenir un consentement manifeste: de sorte que la personne potentiellement consentante puisse comprendre de manière évidente l'objet du consentement.

b. L'Entreprise a l'obligation d'obtenir un consentement libre: de sorte que la personne potentiellement consentante ne subisse aucune coercition ou contrainte et agisse de sa propre volonté.

c. L'Entreprise a l'obligation d'obtenir un consentement éclairé: de sorte que la personne potentiellement consentante puisse effectuer un choix en connaissance des implications et des conséquences évidentes de son choix.

d. L'Entreprise a l'obligation d'obtenir un consentement spécifique: de sorte que la personne potentiellement consentante puisse consentir à un objectif précis et clairement circonscrit.

e. L'Entreprise a l'obligation d'obtenir un consentement granulaire: de sorte que la personne potentiellement consentante puisse consentir à chaque fin particulière.

f. L'Entreprise a l'obligation d'obtenir un consentement compréhensible: de sorte que la personne potentiellement consentante puisse consentir à des termes simples et clairs.

g. L'Entreprise a l'obligation d'obtenir un consentement distinct: de sorte que la personne potentiellement consentante puisse consentir distinctement de toute autre information, lorsque la demande est faite par écrit.

h. L'Entreprise a l'obligation d'obtenir un consentement temporaire: de sorte que la personne potentiellement consentante puisse consentir pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.

i. L'Entreprise a l'obligation de fournir un mécanisme simple permettant à l'individu de retirer son consentement à tout moment et pour toutes fins et de l'informer des conséquences d'un retrait. Ce mécanisme doit être accessible à tous et publicisé.

5.3.2 Consentement des mineurs

Au Québec, est considéré mineur toute personne de **moins de 18 ans**.

a. Si le mineur a moins de 14 ans, le consentement à l'utilisation ou à la communication de ses renseignements personnels devra être donné par le parent ou le titulaire de l'autorité parentale.

b. Si le mineur a 14 ans ou plus, le consentement pourra être donné par le mineur lui-même ou par le parent ou le titulaire de l'autorité parentale.

c. Si cette collecte est manifestement au bénéfice du mineur, l'Entreprise pourra toutefois procéder à cette collecte sans consentement parental.

5.3.3 Exceptions au consentement

Quand la santé ou la sécurité d'une personne est menacée par une situation urgente et dangereuse:

a. L'Entreprise peut communiquer les renseignements personnels de cette personne sans son consentement à toute personne à qui cette communication doit être faite.

b. L'Entreprise doit établir le caractère urgent et dangereux de la situation pour qu'elle puisse communiquer les renseignements sans consentement.

Dans le but de prévenir un acte de violence, dont un suicide, l'Entreprise peut:

c. Communiquer des renseignements personnels sans le consentement des personnes concernées. Cette communication doit cependant se limiter aux personnes exposées à ce danger, à leur représentant et à toute personne susceptible de leur porter secours, par exemple un policier, un centre de

prévention du suicide, l'intervenant d'un CLSC, la DPJ, un professionnel de la santé, etc.

5.4 Autres considérations

Afin de se conformer aux exigences légales de la LPRPSP, d'autres éléments sont à considérer.

a. L'Entreprise a l'obligation de mettre en place, utiliser et maintenir un processus de gestion des incidents des actifs informationnels.

b. L'Entreprise a l'obligation de mettre en place, utiliser et maintenir une politique sur la classification des données générales; incluant la classification des renseignements personnels.

c. L'Entreprise a l'obligation de mettre en place, utiliser et maintenir une politique sur la gestion des demandes et des plaintes visant la gestion des renseignements personnels.

d. L'Entreprise a l'obligation de mettre en place, utiliser et maintenir une politique sur la formation et la sensibilisation des risques visant les renseignements personnels.

6. CONFORMITÉ

6.1 Mesures de conformité

L'Entreprise établit cette politique et s'assure qu'on y adhère et s'y conforme en utilisant:

a. Des outils de contrôle

b. Des audits internes et externes

c. De la rétroaction au responsable de la politique

6.2 Exceptions

Toute exception à ces lignes directrices doit préalablement faire l'objet d'une demande par écrit et approuvée par l'Entreprise en utilisant les documents appropriés.

Toute exception sans autorisation préalable sera traitée comme un cas de non-conformité à ces lignes directrices.

6.3 Non-conformité

Quiconque déroge significativement de ces lignes directrices peut faire l'objet de mesures disciplinaires pouvant aller jusqu'à la cessation du lien d'emploi.

7. RÉVISION

La présente politique sera révisée UNE FOIS PAR ANNÉE, ou au besoin suivant des changements contractuels, légaux, ou contextuels.