

POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Centre de pièces et services experts inc ou Electro-Experts

Conformément à la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25, 2021, c. 25) et à la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP, chapitre P-39.1)

TABLE DES MATIÈRES

- 1. Préambule et introduction**
- 2. Définitions**
- 3. Nomination et rôle du responsable de la protection des renseignements personnels (RPRP)**
- 4. Renseignements personnels collectés**
- 5. Règles de consentement**
- 6. Utilisation et communication des renseignements personnels**
- 7. Contrôles d'accès et sécurité**
- 8. Conservation et destruction des données**
- 9. Gestion des incidents de confidentialité**
- 10. Droits des personnes concernées**
- 11. Formation du personnel**
- 12. Obligations de transparence et publication**
- 13. Transferts et communication à des tiers**
- 14. Évaluation des facteurs relatifs à la vie privée (EFVP)**
- 15. Sanctions et responsabilités**
- 16. Entrée en vigueur et révision**

ANNEXES

- Annexe A – Formulaire de demande d'accès ou de rectification
- Annexe B – Formulaire de consentement au traitement des données
- Annexe C – Formulaire de déclaration d'incident de confidentialité (interne)
- Annexe D – Registre des incidents de confidentialité (modèle)
- Annexe E – Registre des formations du personnel (modèle)

1. PRÉAMBULE ET INTRODUCTION

1.1 Présentation de l'entreprise

Centre de pièces et services experts inc. ou Electro-Experts (ci-après « l'Entreprise ») est une entreprise familiale fondée en 2005. Aujourd'hui devenue la plus grande entreprise de service d'électroménagers et d'appareils électroniques au Québec, la compagnie compte plus de 175 employés. Une équipe d'environ 120 techniciens professionnels, certifiés et formés par les manufacturiers, œuvrent dans 8 succursales partout au Québec et en Ontario, afin de mieux vous servir. L'Entreprise offre ses services à domicile et le siège social est établi au 8260 boulevard Pie IX, H1Z 3T6, Montréal dans la province de Québec.

Pour ce faire, nous offrons un service complet de réparation d'électroménagers et autres appareils à domiciles ou en atelier, ainsi qu'un réseau de distribution de pièces pour une clientèle avertie, dotée de connaissances techniques. Nous offrons aussi une vaste gamme de produits en magasins, pouvant compter des aspirateurs et des grilles au gaz, selon les succursales.

1.2 Engagement envers la protection des renseignements personnels

L'Entreprise s'engage à protéger la vie privée de toutes les personnes avec lesquelles elle interagit, conformément aux lois applicables. Elle s'engage à ne collecter que les renseignements personnels nécessaires à l'accomplissement de ses activités, à les utiliser uniquement aux fins pour lesquelles ils ont été collectés, et à les protéger par des mesures de sécurité appropriées.

La présente politique reflète les valeurs fondamentales de l'Entreprise en matière de respect de la vie privée et de transparence envers toutes les personnes concernées.

1.3 Références légales

La présente politique est élaborée en conformité avec les textes législatifs suivants :

- **Loi sur la protection des renseignements personnels dans le secteur privé** (LPRPSP), chapitre P-39.1, telle que modifiée par la Loi 25 ;
- **Loi modernisant des dispositions législatives en matière de protection des renseignements personnels** (communément appelée « Loi 25 »), 2021, c. 25, dont les dispositions ont été progressivement mises en vigueur de 2022 à 2023 ;
- **Code civil du Québec**, articles 35 à 40, relatifs au droit à la vie privée ;
- Les règlements et lignes directrices émis par la **Commission d'accès à l'information du Québec (CAI)**.

1.4 Champ d'application

La présente politique s'applique à :

- **Les clients** de l'Entreprise (particuliers et entreprises qui font appel aux services de réparation) ;
- **Les employés et techniciens** de l'Entreprise, qu'ils soient permanents, à temps partiel ou saisonniers ;

- **Les fournisseurs et partenaires commerciaux** de l'Entreprise ;
- **Les sous-traitants** auxquels l'Entreprise peut avoir recours pour certains services ;
- **Toute autre personne** dont les renseignements personnels sont détenus par l'Entreprise.

Elle s'applique à tous les renseignements personnels détenus par l'Entreprise, quelle que soit la nature de leur support (papier, numérique, audiovisuel) et quelle que soit la forme sous laquelle ils sont accessibles. (Réf. : art. 1 LPRPSP)

2. DÉFINITIONS

Aux fins de la présente politique, les expressions suivantes ont le sens qui leur est donné ci-dessous :

Terme	Définition
Renseignement personnel	Tout renseignement qui concerne une personne physique et permet de l'identifier, directement ou indirectement. Exemples : nom, adresse, numéro de téléphone, adresse courriel, données de paiement, historique de services. (Réf. : art. 2 LPRPSP)
Renseignement personnel sensible	Tout renseignement personnel qui, de par sa nature (état de santé, données biométriques, informations financières détaillées, opinions politiques ou religieuses), commande une protection plus élevée en raison du préjudice particulier que sa divulgation pourrait causer à la personne concernée. (Réf. : art. 12 al. 2 LPRPSP)
Responsable de la protection des renseignements personnels (RPRP)	La personne qui, au sein de l'Entreprise, est chargée d'assurer la protection des renseignements personnels et le respect des obligations prévues par la LPRPSP. Par défaut, il s'agit de la personne ayant la plus haute autorité au sein de l'Entreprise, à moins qu'une délégation écrite ne soit faite. (Réf. : art. 3.1 LPRPSP)
Incident de confidentialité	Tout accès, utilisation ou communication non autorisé d'un renseignement personnel, ou toute perte d'un renseignement personnel ou toute autre atteinte à la protection de ce renseignement. (Réf. : art. 3.6 LPRPSP)
Consentement manifeste	Consentement donné de manière claire, libre, éclairée et spécifique par la personne concernée, exprimé de façon active et non équivoque. Un consentement tacite ou présumé n'est pas considéré comme manifeste pour les fins sensibles. (Réf. : art. 14 LPRPSP)
Traitement des données	Toute opération effectuée sur des renseignements personnels, que ce soit leur collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, consultation, utilisation, communication, diffusion ou destruction.
Anonymisation	Processus irréversible par lequel les renseignements personnels sont dépouillés de tout élément permettant d'identifier directement ou indirectement la personne concernée, selon les meilleures pratiques généralement reconnues. (Réf. : art. 23 LPRPSP)

Terme	Définition
Dépersonnalisation	Processus qui consiste à retirer les identificateurs directs d'un renseignement personnel, mais dont le résultat ne constitue pas une anonymisation complète (la réidentification reste techniquement possible). Utilisée notamment pour les fins de recherche ou d'analyse interne.
Commission d'accès à l'information (CAI)	L'organisme québécois chargé de surveiller l'application de la LPRPSP, de traiter les plaintes des personnes concernées, et d'émettre des lignes directrices en matière de protection des renseignements personnels. Site web : www.cai.gouv.qc.ca .
EFVP	Évaluation des facteurs relatifs à la vie privée. Analyse structurée visant à identifier et à réduire les risques pour la vie privée liés à un projet impliquant des renseignements personnels. (Réf. : art. 3.3 LPRPSP)
Personne concernée	Toute personne physique dont des renseignements personnels sont détenus par l'Entreprise.

3. NOMINATION ET RÔLE DU RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (RPRP)

3.1 Obligation légale

Conformément à l'article 3.1 de la LPRPSP, toute entreprise doit s'assurer que la protection des renseignements personnels soit sous la responsabilité d'une personne désignée. Par défaut, c'est la personne ayant la plus haute autorité au sein de l'Entreprise qui assume ce rôle. Cette personne peut toutefois déléguer, par écrit, l'exercice de cette fonction à un membre de son personnel. (Réf. : art. 3.1 LPRPSP)

3.2 Identité du RPRP

L'Entreprise désigne la personne suivante à titre de Responsable de la protection des renseignements personnels :

Information	Détail
Nom complet	Karl Brasseur
Titre / Fonction	Propriétaire
Adresse courriel	k.brasseur@electro-experts.com
Numéro de téléphone	1-888-915-8888 option 7
Adresse postale	8260 boulevard Pie IX, H1Z 3T6, Montréal, Québec
Date de nomination	29 décembre 2023

3.3 Publication des coordonnées

Les coordonnées du RPRP doivent être rendues accessibles sur le site Internet de l'Entreprise à l'adresse www.electro-experts.com, ou, si l'Entreprise ne dispose pas d'un site web, par tout autre moyen approprié permettant aux personnes concernées d'en prendre connaissance facilement. (Réf. : art. 3.2 LPRPSP)

3.4 Délégation de la fonction

Le RPRP peut déléguer, en tout ou en partie, l'exercice de ses fonctions à un ou plusieurs membres du personnel de l'Entreprise. Cette délégation doit :

- Être faite par écrit et signée par le RPRP ;
- Préciser la nature et l'étendue des fonctions déléguées ;
- Être conservée dans le registre de gouvernance de l'Entreprise ;
- Être revue lors de tout changement de personnel concerné.

La délégation ne dégage pas le RPRP de sa responsabilité ultime à l'égard de la protection des renseignements personnels au sein de l'Entreprise.

3.5 Rôles et responsabilités du RPRP

Le RPRP est responsable, notamment, des fonctions suivantes :

- Élaborer, mettre à jour et faire respecter la présente politique de confidentialité ;
- S'assurer que l'Entreprise respecte toutes les obligations découlant de la LPRPSP ;
- Recevoir et traiter les demandes d'accès, de rectification et de portabilité des personnes concernées ;
- Gérer les incidents de confidentialité, incluant l'évaluation du risque, la notification à la CAI et aux personnes concernées ;
- Tenir à jour le registre des incidents de confidentialité ;
- Superviser la formation du personnel en matière de protection des renseignements personnels ;
- Procéder ou superviser les évaluations des facteurs relatifs à la vie privée (EFVP) ;
- Approuver les ententes avec les fournisseurs de services tiers qui traitent des renseignements personnels au nom de l'Entreprise ;
- Agir comme point de contact avec la Commission d'accès à l'information (CAI) ;
- Approuver les politiques et pratiques de protection des renseignements personnels.

(Réf. : art. 3.2 LPRPSP)

3.6 Mécanisme de plaintes et de recours

Toute personne qui estime que ses renseignements personnels ne sont pas traités en conformité avec la présente politique ou avec la LPRPSP peut soumettre une plainte au RPRP par :

- **Courriel** : audit@electro-experts.com

- **Courrier postal** : 8260 boulevard Pie IX, H1Z 3T6, Montréal, Québec à l'attention du Responsable de la protection des renseignements personnels

Le RPRP s'engage à accuser réception de toute plainte dans un délai de cinq (5) jours ouvrables et à fournir une réponse dans un délai de trente (30) jours suivant la réception. Si la personne n'est pas satisfaite de la réponse obtenue, elle peut porter plainte à la Commission d'accès à l'information du Québec (CAI). (Réf. : art. 42 LPRPSP)

4. RENSEIGNEMENTS PERSONNELS COLLECTÉS

4.1 Types de renseignements collectés

4.1.1 Clients

Dans le cadre de la prestation de ses services de réparation d'électroménagers, l'Entreprise peut recueillir les renseignements personnels suivants :

Type de renseignement	Exemples / Précisions
Identité	Nom, prénom, titre de civilité
Coordonnées	Adresse domiciliaire, numéro de téléphone (domicile, bureau, cellulaire), adresse courriel
Informations de service	Numéro de bon de travail, appareil(s) concerné(s) (marque, modèle, numéro de série), description du problème, date(s) de service, historique des réparations effectuées
Informations de paiement	Mode de paiement, numéro de transaction, informations de facturation. Les numéros de carte de crédit complets ne sont pas conservés par l'Entreprise et sont traités directement par le prestataire de paiement certifié PCI-DSS.
Informations domiciliaires	Accès au domicile, instructions particulières pour la visite du technicien (codes d'entrée le cas échéant – conservés temporairement et détruits après la visite)
Communications	Notes ou commentaires fournis par le client lors d'appels téléphoniques, de courriels ou de formulaires en ligne
Préférences de communication	Langue de service, canal de communication préféré, consentement aux communications marketing

4.1.2 Fournisseurs et sous-traitants

L'Entreprise peut collecter les renseignements professionnels suivants auprès de ses fournisseurs et sous-traitants :

- Nom de l'entreprise, numéro d'enregistrement, NEQ ;
- Noms et coordonnées des représentants autorisés ;
- Informations bancaires et de facturation (entreprise) ;
- Informations relatives aux permis, licences et certifications professionnelles.

4.1.3 Employés et techniciens

Dans le cadre de la gestion des ressources humaines, l'Entreprise collecte les renseignements personnels suivants concernant ses employés et techniciens :

- Nom complet, date de naissance, adresse domiciliaire ;
- Numéro d'assurance sociale (NAS), informations fiscales ;
- Coordonnées en cas d'urgence ;
- Certifications professionnelles, permis de conduire ;
- Informations salariales et avantages sociaux ;
- Évaluations de rendement ;
- Informations relatives aux absences et congés.

Les renseignements personnels des employés sont régis par les lois du travail applicables et font l'objet d'une protection accrue.

4.2 Méthodes de collecte

L'Entreprise collecte les renseignements personnels par les moyens suivants :

- **Site web de l'Entreprise** : formulaires de demande de service en ligne, formulaires de contact ;
- **Téléphone** : lors de la prise de rendez-vous ou du suivi des réparations ;
- **Visites à domicile** : renseignements recueillis lors de l'évaluation ou de la réparation ;
- **Courriel et messagerie** : communications initiées par le client ou le fournisseur ;
- **Logiciel de gestion des réparations** : saisie directe par le personnel autorisé.

4.3 Finalités de la collecte

Les renseignements personnels sont collectés aux fins suivantes, déterminées avant ou au moment de leur collecte :

- Fournir les services de réparation d'électroménagers demandés ;
- Planifier et confirmer les rendez-vous de service ;
- Établir et émettre les factures et reçus ;
- Gérer les garanties sur les réparations effectuées ;
- Assurer le suivi des réparations et le service après-vente ;
- Communiquer avec les clients au sujet de leur dossier de service ;
- Respecter les obligations légales et réglementaires (tenue de livres, fiscalité) ;
- Envoyer des communications marketing et promotionnelles (uniquement avec consentement explicite) ;
- Améliorer la qualité des services offerts (analyse interne anonymisée).

4.4 Principe de minimisation

Conformément à l'article 5 de la LPRPSP, l'Entreprise s'engage à ne collecter que les renseignements personnels strictement nécessaires aux fins déterminées au moment de la

collecte. Aucun renseignement personnel superflu ne sera demandé. Le personnel est formé et tenu de respecter ce principe. (Réf. : art. 5 LPRPSP)

5. RÈGLES DE CONSENTEMENT

5.1 Types de consentement

La LPRPSP prévoit deux types de consentement selon la nature et la sensibilité des renseignements personnels collectés :

Type	Description et application
Consentement explicite (manifeste)	Requis pour les renseignements sensibles, les utilisations à des fins autres que celles pour lesquelles ils ont été collectés, les transferts hors Québec, et les communications à des tiers non impliqués dans la prestation du service. Le consentement manifeste doit être donné de manière active et non équivoque. (Réf. : art. 14 LPRPSP)
Consentement implicite	Applicable lorsqu'un client fait appel aux services de l'Entreprise, signifiant ainsi son consentement à la collecte des renseignements nécessaires à la prestation du service demandé. Applicable uniquement aux renseignements non sensibles directement liés au service.

5.2 Caractéristiques du consentement valide

Pour être valide, le consentement doit être :

- **Libre** : donné sans pression, contrainte ou condition à l'obtention du service (sauf si le renseignement est essentiel au service) ;
- **Éclairé** : la personne doit être informée des fins de la collecte, de l'utilisation et de la communication prévues ;
- **Donné à des fins spécifiques** : le consentement doit être lié à des finalités précises et non à des fins générales ou indéfinies ;
- **Manifeste** : clairement exprimé, notamment pour les renseignements sensibles. (Réf. : art. 14 LPRPSP)

5.3 Consentement pour communications marketing

L'envoi de communications à des fins de prospection commerciale, de promotion de services ou d'offres spéciales requiert un consentement **explicite et opt-in** de la personne concernée. Ce consentement doit :

- Être obtenu distinctement du consentement au service ;
- Identifier clairement le type de communications qui sera envoyé ;
- Prévoir un mécanisme simple de désabonnement dans chaque communication.

5.4 Droit de retirer le consentement

Toute personne peut retirer son consentement en tout temps, sans frais et sans justification. L'Entreprise doit alors cesser de collecter, d'utiliser ou de communiquer les renseignements personnels concernés dès que le retrait est signifié, sous réserve des obligations légales en vigueur. Le retrait du consentement peut être effectué par courriel (*Réf. : art. 14 al. 3 LPRPSP*)

5.5 Conservation des preuves de consentement

L'Entreprise conserve une trace du consentement obtenu pour chaque personne concernée, incluant :

- La date et le mode d'obtention du consentement ;
- Les fins pour lesquelles le consentement a été donné ;
- Le formulaire ou la preuve électronique de consentement.

Ces preuves sont conservées pour la durée de la relation avec la personne concernée et pour une période minimale de deux (2) ans après la fin de la relation.

5.6 Cas d'exception au consentement

Dans les situations suivantes, le consentement peut ne pas être requis :

- Lorsque la loi autorise ou exige expressément la collecte, l'utilisation ou la communication du renseignement ;
- Lorsqu'il y a urgence mettant en danger la sécurité d'une personne ;
- Lorsque la collecte est nécessaire pour la prévention ou la détection d'une fraude ou d'un crime ;
- Lorsque la communication est nécessaire à une transaction commerciale (sous conditions strictes). (*Réf. : art. 18 LPRPSP*)

6. UTILISATION ET COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

6.1 Utilisations autorisées

Les renseignements personnels collectés par l'Entreprise ne peuvent être utilisés qu'aux fins pour lesquelles ils ont été collectés, soit :

- La prestation des services de réparation d'électroménagers ;
- La facturation, la gestion des paiements et la tenue des livres comptables ;
- La gestion des garanties sur les travaux effectués ;
- Le suivi des réparations et le service après-vente ;
- Les communications relatives au dossier de service du client ;
- Le respect des obligations légales et fiscales ;
- Les communications marketing, avec le consentement explicite de la personne.

Toute utilisation à d'autres fins requiert un nouveau consentement explicite de la personne concernée. (*Réf. : art. 13 LPRPSP*)

6.2 Communication à des tiers

L'Entreprise peut communiquer des renseignements personnels aux catégories de tiers suivantes, dans les limites nécessaires à la prestation des services :

Catégorie de tiers	Fins de la communication
Sous-traitants en réparation	Lorsqu'une réparation spécialisée est confiée à un technicien externe autorisé
Fournisseurs de pièces de rechange	Pour la commande de pièces nécessaires à la réparation (nom, appareil, numéro de série)
Prestataires de paiement	Pour le traitement sécurisé des transactions financières
Transporteurs et livreurs	Pour la livraison d'appareils ou de pièces (nom, adresse de livraison)
Comptable / Firme comptable	Pour la tenue de livres, la fiscalité et les états financiers
Assureur de l'Entreprise	En cas de réclamation liée à un service fourni
Autorités légales	Lorsque requis par une ordonnance judiciaire, une obligation légale ou réglementaire

6.3 Exigences contractuelles pour les tiers

Avant de communiquer des renseignements personnels à un tiers, l'Entreprise doit s'assurer qu'un contrat écrit est conclu, stipulant notamment que le tiers :

- N'utilisera les renseignements qu'aux seules fins prévues au contrat ;
- Ne communiquera pas les renseignements à d'autres parties sans le consentement de l'Entreprise ;
- Prendra les mesures nécessaires pour assurer la protection du caractère confidentiel des renseignements ;
- Détruira les renseignements lorsqu'ils ne seront plus nécessaires aux fins prévues ;
- Notifiera l'Entreprise de tout incident de confidentialité le concernant. (Réf. : art. 18.3 LPRPSP)

6.4 Interdiction d'utilisation non autorisée

Il est strictement interdit à l'Entreprise et à tout membre de son personnel de :

- Vendre des renseignements personnels à des tiers ;
- Utiliser des renseignements personnels à des fins commerciales non consenties ;
- Communiquer des renseignements personnels à des fins non prévues sans consentement ;
- Utiliser les renseignements personnels d'un client à des fins personnelles.

6.5 Communication hors Québec

Toute communication de renseignements personnels à une personne ou organisation située hors du Québec est soumise aux exigences suivantes :

- Réalisation préalable d'une EFVP ;
- Obtention du consentement manifeste et éclairé de la personne concernée, après l'avoir informée des risques ;
- Conclusion d'une entente écrite avec le destinataire étranger assurant une protection équivalente à celle requise par la LPRPSP. (Réf. : art. 17 LPRPSP)

7. CONTRÔLES D'ACCÈS ET SÉCURITÉ

7.1 Principe du moindre privilège

L'accès aux renseignements personnels détenus par l'Entreprise est accordé selon le principe du moindre privilège : seuls les membres du personnel qui ont besoin d'un accès dans le cadre de leurs fonctions peuvent y accéder, et uniquement dans la mesure nécessaire à l'exercice de leurs responsabilités. (Réf. : art. 10 LPRPSP)

7.2 Catégories d'accès par rôle

Rôle	Données accessibles
Technicien terrain	Informations du bon de travail du jour (nom client, adresse, appareil, problème signalé). Pas d'accès aux informations de paiement ni à l'historique complet.
Service à la clientèle	Dossier client complet, historique des réparations, bons de travail, coordonnées. Accès restreint aux informations de paiement.
Administrateur / Comptabilité	Informations de facturation, données de paiement, informations fiscales. Accès restreint aux dossiers de service détaillés.
Direction / RPRP	Accès complet à tous les dossiers et systèmes, sous réserve des obligations légales.
Responsable TI	Accès aux systèmes et à l'infrastructure, sans accès aux données personnelles au-delà de ce qui est nécessaire à la maintenance.

7.3 Mesures de sécurité physiques

- Classeurs et tiroirs verrouillés pour les dossiers papier contenant des renseignements personnels ;
- Accès aux locaux de l'Entreprise limité au personnel autorisé (système de clés ou code d'accès) ;
- Bureau et documents protégés pendant les absences (politique du bureau propre) ;
- Destruction sécurisée des documents papier (déchiqueteur) ;
- Accès des visiteurs supervisé en tout temps dans les zones contenant des dossiers clients.

7.4 Mesures de sécurité informatiques

- **Mots de passe** : complexité minimale requise (8 caractères, majuscules, chiffres, caractères spéciaux), changement périodique (au moins tous les 90 jours), unicité par employé ;
- **Chiffrement** : les données stockées et transmises par voie électronique doivent être chiffrées (protocoles TLS/SSL pour les transmissions, chiffrement au repos pour les données sensibles) ;
- **Antivirus et protection contre les logiciels malveillants** : installation et mise à jour régulière sur tous les appareils ;
- **Pare-feu** : protection du réseau de l'Entreprise ;
- **Sauvegardes** : sauvegardes automatiques régulières (au moins quotidiennes) des données, stockées dans un emplacement sécurisé distinct du système principal ;
- **Mises à jour** : application régulière des correctifs de sécurité sur tous les systèmes et logiciels ;
- **Authentification** : authentification multifacteur recommandée pour les accès à distance ou aux systèmes critiques.

7.5 Accès aux systèmes de gestion des réparations

L'accès au logiciel de gestion des réparations et à la base de données clients est accordé nominativement à chaque utilisateur. Les identifiants d'accès sont strictement personnels et ne doivent pas être partagés. Toute connexion est journalisée et peut faire l'objet de vérifications périodiques.

7.6 Révision périodique des droits d'accès

Le RPRP procède à une révision des droits d'accès au moins une fois par année et lors de tout changement de poste ou de responsabilités d'un employé. Les accès non justifiés par les fonctions actuelles de l'employé sont révoqués sans délai.

7.7 Procédure lors du départ d'un employé

Lors du départ d'un employé (démission, congédiement, fin de contrat), les mesures suivantes sont prises le jour du départ ou avant :

- Révocation immédiate de tous les accès informatiques et physiques ;
- Récupération de tout équipement appartenant à l'Entreprise (ordinateur, téléphone, badge) ;
- Changement des codes d'accès physiques si nécessaire ;
- Rappel à l'employé de son obligation de confidentialité post-emploi ;
- Suppression ou transfert des courriels et données professionnelles de l'employé.

7.8 Journalisation des accès

L'Entreprise maintient des journaux d'accès aux systèmes informatiques contenant des renseignements personnels. Ces journaux consignent au minimum l'identifiant de l'utilisateur, la date et l'heure d'accès, et les actions effectuées. Ils sont conservés pour une

durée minimale de douze (12) mois et peuvent être consultés en cas d'incident de confidentialité.

8. CONSERVATION ET DESTRUCTION DES DONNÉES

8.1 Durées de conservation

Les renseignements personnels ne doivent pas être conservés au-delà de la durée nécessaire aux fins pour lesquelles ils ont été collectés, sous réserve des obligations légales applicables.

(Réf. : art. 23 LPRPSP)

Type de données	Durée de conservation	Fondement
Dossiers clients et bons de travail	5 ans après la fin de la relation commerciale ou la dernière transaction	Prescription civile (art. 2925 C.c.Q.), obligations légales
Informations de facturation et paiement	6 à 7 ans (conformément aux exigences fiscales de Revenu Québec et CRA)	Loi sur la fiscalité, Loi de l'impôt sur le revenu
Données de ressources humaines (employés actifs)	Durée de l'emploi + 5 ans après la fin de l'emploi	Loi sur les normes du travail, obligations fiscales
Données de fournisseurs et sous-traitants	5 ans après la fin de la relation d'affaires	Prescription civile
Preuves de consentement	2 ans minimum après la fin de la relation	LPRPSP, gestion du risque légal
Registre des incidents de confidentialité	5 ans à compter de la date de l'incident	Art. 3.7 LPRPSP
Journaux d'accès informatiques	12 mois minimum	Bonnes pratiques de sécurité
Communications marketing (historique de consentement)	Durée du consentement + 2 ans	Loi canadienne anti-pourriel (LCAP)

8.2 Méthodes de destruction sécurisée

Support	Méthode de destruction
Documents papier	Déchetage par déchiqueteur à coupe croisée (niveau P-4 minimum) ou recours à un service certifié de destruction de documents
Données numériques (serveurs, PC)	Effacement sécurisé selon la norme NIST SP 800-88, ou destruction physique du support si nécessaire
Appareils mobiles (téléphones, tablettes)	Réinitialisation aux paramètres d'usine avec chiffrement préalable, ou destruction physique

Support	Méthode de destruction
Supports amovibles (clés USB, disques)	Effacement sécurisé ou destruction physique

8.3 Calendrier et révision annuelle

L'Entreprise procède à une révision annuelle de ses dossiers afin d'identifier les renseignements personnels dont la période de conservation est expirée. Cette révision est effectuée au cours du premier trimestre de chaque année civile et est consignée au registre des destructions.

8.4 Registre des destructions

L'Entreprise tient un registre de toutes les destructions de renseignements personnels, incluant :

- La description des renseignements détruits ;
- La date de destruction ;
- La méthode utilisée ;
- Le nom de la personne responsable de la destruction ;
- Le cas échéant, la confirmation du prestataire de service mandaté.

8.5 Anonymisation comme alternative à la destruction

Lorsque l'Entreprise souhaite conserver des données à des fins statistiques, analytiques ou de recherche interne, elle peut procéder à l'anonymisation des renseignements personnels plutôt qu'à leur destruction, à condition que le résultat de l'anonymisation soit irréversible et conforme aux meilleures pratiques reconnues. Les données ainsi anonymisées ne sont plus soumises aux obligations de la LPRPSP. (Réf. : art. 23 LPRPSP)

9. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

9.1 Définition d'un incident de confidentialité

Un incident de confidentialité désigne tout accès, utilisation ou communication non autorisé d'un renseignement personnel, ou toute perte d'un renseignement personnel ou autre atteinte à la protection de ce renseignement. Il peut s'agir, sans s'y limiter, de :

- La perte ou le vol d'un appareil contenant des renseignements personnels (ordinateur portable, téléphone, clé USB) ;
- L'envoi d'un courriel contenant des renseignements personnels à la mauvaise personne ;
- Une intrusion dans les systèmes informatiques (cyberattaque, rançongiciel) ;
- L'accès non autorisé à un dossier client par un employé non habilité ;
- La divulgation accidentelle de renseignements personnels lors d'une conversation ou d'une communication.

9.2 Évaluation du risque de préjudice sérieux

Tout incident de confidentialité doit faire l'objet d'une évaluation par le RPRP afin de déterminer s'il présente un risque qu'un préjudice sérieux soit causé à la personne concernée. Parmi les facteurs à considérer :

- La sensibilité des renseignements en cause ;
- L'anticipation raisonnable qu'une utilisation de ces renseignements cause un préjudice (vol d'identité, discrimination, perte financière, atteinte à la réputation) ;
- Le nombre de personnes concernées ;
- Si les renseignements ont été réellement consultés ou transmis à un tiers non autorisé. (Réf. : art. 3.6 LPRPSP)

9.3 Obligations de déclaration à la CAI

Lorsque l'évaluation conclut à un risque de préjudice sérieux, l'Entreprise doit :

- Déclarer l'incident à la Commission d'accès à l'information (CAI) **dans les délais les plus brefs** (idéalement dans les 72 heures suivant la prise de connaissance de l'incident) ;
- Utiliser le formulaire de déclaration officiel de la CAI (disponible sur le site www.cai.gouv.qc.ca) ;
- Fournir toutes les informations requises, incluant la nature de l'incident, les renseignements en cause, le nombre de personnes affectées et les mesures prises. (Réf. : art. 3.7 LPRPSP)

9.4 Avis aux personnes concernées

Lorsque l'incident présente un risque de préjudice sérieux, l'Entreprise doit aviser les personnes concernées avec diligence, afin de leur permettre de prendre les mesures appropriées pour se protéger. L'avis doit contenir :

- Une description de l'incident ;
- La nature des renseignements personnels en cause ;
- Les mesures prises par l'Entreprise pour remédier à l'incident ;
- Les mesures que la personne peut prendre pour se protéger ;
- Les coordonnées du RPRP. (Réf. : art. 3.7 al. 2 LPRPSP)

Si les personnes concernées ne peuvent être rejointes directement, un avis public doit être publié par un moyen permettant de les rejoindre (site web, médias, etc.).

9.5 Registre des incidents de confidentialité

L'Entreprise doit tenir un registre de tous les incidents de confidentialité, qu'ils aient ou non donné lieu à une déclaration à la CAI. Ce registre est conservé pour une durée minimale de cinq (5) ans. Son modèle est présenté à l'Annexe D de la présente politique. (Réf. : art. 3.7 al. 3 LPRPSP)

9.6 Procédure interne de réponse aux incidents

En cas d'incident de confidentialité confirmé ou suspecté, les étapes suivantes doivent être suivies :

Étape	Phase	Actions requises
1	Détection et signalement	Tout employé ayant connaissance d'un incident doit le signaler immédiatement au RPRP via le formulaire de l'Annexe C ou par contact direct.
2	Confinement (Containment)	Prendre les mesures immédiates pour limiter l'incident : déconnecter les systèmes compromis, bloquer les accès non autorisés, récupérer les documents perdus si possible.
3	Évaluation du risque	Le RPRP évalue la gravité de l'incident, la sensibilité des renseignements en cause et le risque de préjudice sérieux pour les personnes concernées.
4	Notification	Si un risque de préjudice sérieux est identifié : déclarer à la CAI, aviser les personnes concernées. Documenter toutes les communications.
5	Correction	Mettre en place les mesures correctives pour remédier à la cause de l'incident et prévenir sa récurrence.
6	Documentation	Consigner l'incident au registre des incidents (Annexe D), documenter toutes les décisions et actions prises.
7	Révision post-incident	Procéder à une analyse post-incident pour identifier les lacunes et mettre à jour les politiques, procédures ou mesures de sécurité selon les besoins.

9.7 Révision post-incident et mesures correctives

À la suite de tout incident de confidentialité, le RPRP procède à une révision approfondie dans les 30 jours suivant la résolution de l'incident, incluant une analyse des causes profondes et la mise en place de mesures correctives documentées. Les résultats de cette révision sont consignés dans le registre des incidents et servent à améliorer les politiques et procédures de l'Entreprise.

10. DROITS DES PERSONNES CONCERNÉES

10.1 Droit d'accès

Toute personne a le droit de savoir si l'Entreprise détient des renseignements personnels la concernant et, le cas échéant, d'en obtenir communication. La demande d'accès doit être traitée dans un délai de trente (30) jours suivant sa réception (avec possibilité d'extension de 10 jours ouvrables si justifié). (Réf. : art. 27 LPRPSP)

10.2 Droit de rectification

Toute personne peut demander que ses renseignements personnels soient corrigés s'ils sont inexacts, incomplets ou ambigus. L'Entreprise doit effectuer les corrections demandées sans frais et dans les délais prévus. (Réf. : art. 28 LPRPSP)

10.3 Droit à la portabilité

Toute personne a le droit de recevoir les renseignements personnels la concernant dans un format technologique structuré et couramment utilisé, et d'en demander le transfert à un tiers, dans la mesure prévue par la LPRPSP. (Réf. : art. 27 LPRPSP tel que modifié)

10.4 Droit à la désindexation et au retrait

Dans les cas prévus par la loi, toute personne peut demander que des renseignements personnels la concernant soient retirés d'un index accessible au public ou qu'ils cessent d'être diffusés, notamment lorsque la collecte n'était pas conforme à la loi ou que la finalité initiale est caduque. (Réf. : art. 28.1 LPRPSP)

10.5 Droit de s'opposer à l'utilisation à des fins de prospection commerciale

Toute personne peut, en tout temps et sans frais, s'opposer à l'utilisation de ses renseignements personnels à des fins de prospection commerciale ou de sollicitation. L'Entreprise doit cesser toute telle utilisation dès réception de l'opposition. (Réf. : art. 27.1 LPRPSP)

10.6 Droit de ne pas faire l'objet d'une décision automatisée

Toute personne a le droit d'être informée lorsqu'une décision la concernant est prise exclusivement sur la base d'un traitement automatisé de ses renseignements personnels, et de demander qu'un être humain révise cette décision. (Réf. : art. 12.1 LPRPSP)

10.7 Procédure pour exercer ses droits

Les personnes souhaitant exercer l'un des droits mentionnés ci-dessus peuvent soumettre une demande par l'un des moyens suivants :

- **Par courriel** : audit@electro-experts.com (utiliser le formulaire de l'Annexe A) ;

La demande doit permettre d'identifier la personne concernée. L'Entreprise pourra demander une preuve d'identité si des doutes subsistent sur l'identité du requérant.

Élément	Précision
Délai de réponse	30 jours suivant la réception de la demande complète (Réf. : art. 30 LPRPSP)
Extension possible	10 jours ouvrables supplémentaires si la demande est complexe ou volumineuse, avec avis à la personne concernée
Frais applicables	Aucuns frais pour une première demande. Des frais raisonnables peuvent être exigés pour des demandes répétées ou abusives, avec avis préalable à la personne.
Formulaire recommandé	Annexe A de la présente politique

10.8 Droit de porter plainte à la CAI

Si une personne est insatisfaite de la réponse de l'Entreprise à sa demande, ou si elle estime que ses renseignements personnels ne sont pas traités conformément à la loi, elle a le droit de porter plainte à la Commission d'accès à l'information du Québec :

- **Site web** : www.cai.gouv.qc.ca
- **Téléphone** : 1 888 528-7741
- **Adresse** : Commission d'accès à l'information du Québec, 525, boul. René-Lévesque Est, Bureau 2.36, Québec (Québec) G1R 5S9

11. FORMATION DU PERSONNEL

11.1 Obligation de formation

Tout membre du personnel de l'Entreprise ayant accès à des renseignements personnels, de façon régulière ou occasionnelle, est tenu de suivre une formation sur la protection de la vie privée et le respect des obligations découlant de la LPRPSP et de la présente politique. (*Réf. : art. 3.2 LPRPSP*)

11.2 Contenu de la formation

La formation couvre notamment les sujets suivants :

- Les principes fondamentaux de la Loi 25 et de la LPRPSP ;
- Les types de renseignements personnels collectés par l'Entreprise et leur traitement adéquat ;
- Les politiques et procédures internes de l'Entreprise en matière de confidentialité ;
- La gestion des incidents de confidentialité (comment les reconnaître et les signaler) ;
- Les droits des personnes concernées et la procédure de traitement des demandes ;
- La sécurité informatique : gestion des mots de passe, manipulation des données sur appareils mobiles ;
- La sensibilisation aux risques : hameçonnage, ingénierie sociale, manipulation psychologique ;
- Les responsabilités spécifiques des techniciens terrain lors des visites à domicile.

11.3 Formation initiale à l'embauche

Tout nouvel employé doit compléter la formation de base sur la protection des renseignements personnels dans les trente (30) jours suivant le début de son emploi. Cette formation est organisée par le RPRP ou un représentant désigné. La complétion de la formation est consignée au registre des formations (Annexe E).

11.4 Formation continue

Une formation de mise à jour est dispensée au moins une fois par année civile à tous les employés concernés, et lors de tout changement important affectant les politiques internes ou la législation applicable. Des sessions ponctuelles peuvent être organisées en cas d'incident ou de risque identifié.

11.5 Registre des formations

Le RPRP tient à jour un registre des formations dispensées, incluant :

- La date de la formation ;
- Le contenu couvert ;
- Les noms des participants ;
- Les attestations ou signatures de présence.

Le modèle de registre est présenté à l'Annexe E de la présente politique.

11.6 Responsabilités spécifiques des techniciens terrain

Les techniciens qui se rendent au domicile des clients sont soumis à des obligations de confidentialité particulières en raison de leur accès à l'environnement privé des clients. Ils doivent notamment :

- Ne collecter que les renseignements strictement nécessaires à la réparation ;
- Ne pas noter ni mémoriser des informations personnelles non pertinentes observées lors de la visite ;
- Protéger le bon de travail et les données du client en tout temps ;
- Ne jamais laisser sans surveillance un appareil mobile contenant des données clients ;
- Signaler immédiatement tout incident ou situation suspecte au RPRP.

11.7 Sanctions en cas de manquement

Tout manquement aux obligations en matière de protection des renseignements personnels peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement, selon la gravité du manquement et conformément aux politiques RH de l'Entreprise, sans préjudice des sanctions pénales et civiles prévues par la loi.

12. OBLIGATIONS DE TRANSPARENCE ET PUBLICATION

12.1 Publication de la politique

La présente politique est publiée et accessible sur le site Internet de l'Entreprise à l'adresse www.electro-experts.com Si l'Entreprise ne dispose pas de site web, la politique est rendue accessible par tout autre moyen approprié (affichage en magasin, sur demande, etc.). (Réf. : art. 3.2 LPRPSP)

12.2 Langage clair et accessible

Conformément à l'article 8.2 de la LPRPSP, la présente politique est rédigée en termes simples et clairs, compréhensibles pour toute personne non spécialisée en droit. L'Entreprise s'engage à réviser régulièrement la lisibilité du document. (Réf. : art. 8.2 LPRPSP)

12.3 Avis de collecte

Au moment de la collecte de renseignements personnels, l'Entreprise informe la personne concernée :

- Des fins pour lesquelles les renseignements sont collectés ;

- Des moyens par lesquels ils sont collectés ;
- De ses droits en matière d'accès, de rectification et de retrait du consentement ;
- Des coordonnées du RPRP.

Cet avis est fourni au moment de la collecte, sous forme écrite ou verbale selon le contexte.
(Réf. : art. 8 LPRPSP)

12.4 Paramètres de confidentialité par défaut (Privacy by Default)

L'Entreprise s'engage à appliquer le principe de la vie privée par défaut, c'est-à-dire que les paramètres les plus protecteurs pour la vie privée sont appliqués automatiquement, sans que la personne ait à effectuer de démarche. Les options d'accès élargi ou de communication à des tiers ne peuvent être activées que sur demande explicite de la personne concernée. (Réf. : art. 9.1 LPRPSP)

12.5 Mise à jour et révision de la politique

La présente politique est révisée au moins une fois par année par le RPRP, ou lors de tout changement législatif, organisationnel ou technologique significatif. La version à jour est toujours celle publiée sur le site web ou rendue accessible par l'Entreprise.

12.7 Communication des changements

En cas de modification importante de la politique affectant les droits des personnes concernées ou les modalités de traitement de leurs renseignements, l'Entreprise en informera les personnes concernées par courriel (si disponible), par avis sur son site web, ou par tout autre moyen approprié.

13. TRANSFERTS ET COMMUNICATION À DES TIERS

13.1 Contrats avec fournisseurs et sous-traitants

Avant de confier le traitement de renseignements personnels à un fournisseur de services ou sous-traitant, l'Entreprise doit conclure un contrat écrit contenant les clauses obligatoires suivantes :

- Obligation de confidentialité et d'utilisation des renseignements aux seules fins prévues au contrat ;
- Interdiction de communication à des sous-traitants de rang inférieur sans approbation préalable ;
- Obligation de mettre en place des mesures de sécurité adéquates ;
- Obligation de notifier l'Entreprise de tout incident de confidentialité affectant les renseignements confiés ;
- Obligation de détruire ou de retourner les renseignements à la fin du contrat ;
- Droit d'audit de l'Entreprise sur les pratiques de protection des données du fournisseur. (Réf. : art. 18.3 LPRPSP)

13.2 EFVP avant tout transfert hors Québec

Avant tout transfert de renseignements personnels à une personne ou organisation située hors du Québec, l'Entreprise procède à une EFVP permettant de s'assurer que les renseignements seront adéquatement protégés. Si la protection est jugée insuffisante, le transfert ne peut avoir lieu. (Réf. : art. 17 LPRPSP)

13.3 Interdiction de revente

Il est strictement interdit de vendre, louer, échanger ou autrement transférer des renseignements personnels à des tiers à des fins commerciales sans le consentement explicite et éclairé des personnes concernées. Toute violation de cette interdiction constitue une faute grave et peut entraîner des sanctions disciplinaires, civiles et pénales.

14. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (EFVP)

14.1 Obligation légale

L'Entreprise est tenue de procéder à une EFVP avant tout projet impliquant la collecte, l'utilisation, la communication ou la conservation de renseignements personnels qui présente un risque élevé pour la vie privée des personnes concernées. (Réf. : art. 3.3 LPRPSP)

14.2 Déclencheurs d'une EFVP

Dans le contexte d'une entreprise de réparations d'électroménagers, une EFVP est requise notamment lors :

- De l'implantation d'un nouveau logiciel de gestion des clients ou des réparations ;
- De l'adoption d'un nouveau système de paiement ;
- De la mise en place d'un système de surveillance ou de caméras dans les locaux ;
- De tout transfert de renseignements personnels hors du Québec (ex. : utilisation d'un logiciel hébergé aux États-Unis) ;
- De l'introduction d'un nouveau procédé automatisé de prise de décision ;
- De toute modification substantielle du traitement existant de données.

14.3 Processus d'EFVP simplifié

Étape	Phase	Description
1	Identification du projet	Décrire le projet, ses objectifs et les renseignements personnels en cause.
2	Cartographie des données	Identifier quels renseignements sont collectés, comment, par qui, à quelles fins, et avec qui ils sont partagés.
3	Identification des risques	Évaluer les risques pour la vie privée : probabilité et gravité des impacts potentiels pour les personnes concernées.
4	Mesures d'atténuation	Identifier et implanter les mesures permettant de réduire ou d'éliminer les risques identifiés.

Étape	Phase	Description
5	Documentation et approbation	Documenter les résultats de l'EFVP et soumettre pour approbation au RPRP avant la mise en œuvre du projet.

14.4 Documentation et approbation

Le rapport d'EFVP est rédigé par le responsable du projet, en collaboration avec le RPRP. Il doit être approuvé par le RPRP avant le lancement de tout projet ou activité concerné. Le rapport est conservé par l'Entreprise pendant la durée du projet et pour une période minimale de cinq (5) ans suivant sa conclusion.

15. SANCTIONS ET RESPONSABILITÉS

15.1 Sanctions prévues par la Loi 25

Le non-respect des obligations prévues par la LPRPSP peut entraîner des sanctions administratives et pénales significatives. La CAI dispose de pouvoirs d'enquête et de sanction étendus. *(Réf. : art. 91 et suivants LPRPSP)*

15.2 Responsabilités de chaque employé

Chaque employé de l'Entreprise est personnellement responsable :

- De respecter la présente politique et toutes les procédures internes en matière de protection des renseignements personnels ;
- De signaler immédiatement au RPRP tout incident de confidentialité, toute violation ou tout risque potentiel ;
- De ne pas accéder aux renseignements personnels au-delà de ce qui est nécessaire à l'exercice de ses fonctions ;
- De protéger les identifiants d'accès et de ne jamais les partager ;
- De suivre les formations requises en matière de protection des renseignements personnels.

15.3 Mesures disciplinaires internes

Tout manquement aux obligations prévues par la présente politique peut entraîner des mesures disciplinaires selon la gradation suivante, en fonction de la gravité et du caractère répété du manquement :

Niveau de gravité	Exemples de manquement	Mesures possibles
Mineur	Oubli de verrouiller son ordinateur, utilisation d'un mot de passe non conforme	Avertissement verbal ou écrit, formation complémentaire obligatoire
Modéré	Accès non autorisé à des dossiers sans raison professionnelle, partage d'identifiants d'accès	Suspension temporelle des accès, avertissement écrit au dossier, formation obligatoire
Grave	Divulgaration intentionnelle de renseignements personnels, utilisation à des fins personnelles	Congédiement avec ou sans préavis, poursuite civile ou pénale selon les circonstances

16. ENTRÉE EN VIGUEUR ET RÉVISION

16.1 Date d'entrée en vigueur

La présente politique entre en vigueur le 29 décembre 2023, remplace toute politique antérieure relative à la protection des renseignements personnels adoptée par l'Entreprise.

16.2 Responsable de la mise à jour

Le RPRP, Karl Brasseur est responsable de la mise à jour de la présente politique. Il veille à ce que le document demeure conforme aux exigences légales en vigueur et aux besoins de l'Entreprise.

16.3 Fréquence de révision

La présente politique fait l'objet d'une révision :

- **Au minimum une fois par année civile**, lors d'une révision planifiée ;
- Lors de tout changement significatif dans la législation applicable ;
- Lors de tout changement important dans les activités, les systèmes ou les procédés de l'Entreprise ;
- À la suite d'un incident de confidentialité majeur.

Approuvé et adopté par :

Karl Brasseur / PROPRIÉTAIRE

Responsable de la protection des renseignements personnels

Centre de pièces et services experts inc. ou Electro-Experts

Date : 29 décembre 2023

ANNEXES

ANNEXE A – FORMULAIRE DE DEMANDE D'ACCÈS OU DE RECTIFICATION

N° de formulaire : FA-[] Date de réception : []

Identification de la personne requérante

Champ	Réponse
Nom et prénom	
Adresse	
Numéro de téléphone	
Adresse courriel	
Lien avec l'Entreprise (client / employé / fournisseur / autre)	
Numéro de bon de travail ou de client (si connu)	

Type de demande

Cocher	Type de demande
☐	Accès à mes renseignements personnels
☐	Rectification / Correction de mes renseignements personnels
☐	Portabilité de mes renseignements personnels
☐	Retrait de mon consentement à l'utilisation de mes renseignements personnels
☐	Opposition à l'utilisation à des fins de prospection commerciale
☐	Désindexation / Retrait de renseignements accessibles au public
☐	Autre :

Précisions sur la demande

Veillez décrire les renseignements visés par votre demande et toute information pertinente :

Pièces jointes

☐ Copie d'une pièce d'identité valide (requis pour confirmer l'identité du requérant)

Signature

Signature du requérant	Date

Retourner ce formulaire complété au RPRP par courriel à audit@electro-experts.com. Vous recevrez une confirmation de réception dans les 5 jours ouvrables. Une réponse vous sera fournie dans un délai de 30 jours.

ANNEXE B – FORMULAIRE DE CONSENTEMENT AU TRAITEMENT DES DONNÉES

N° de formulaire : FC- / Date : /

Identification

Champ	Réponse
Nom et prénom	
Adresse	
Téléphone	
Courriel	

Renseignements collectés

Centre de pièces et de services experts inc. ou Electro-Experts collecte les renseignements personnels suivants vous concernant : nom, prénom, adresse, numéro de téléphone, courriel, informations relatives à l'appareil à réparer (marque, modèle, numéro de série), historique des réparations et informations de paiement.

Consentements accordés

Cocher	Objet du consentement
☐	Service de réparation (requis) : Je consens à la collecte et au traitement de mes renseignements personnels aux fins de la prestation des services de réparation d'électroménagers, de la facturation et du suivi de garantie.
☐	Communications marketing (optionnel) : Je consens à recevoir des communications promotionnelles, des offres spéciales et des nouvelles de Centre de pièces et services experts inc. par courriel ou par messagerie texte.
☐	Partage avec sous-traitants (selon le service) : Je consens à ce que mes renseignements soient partagés avec les sous-traitants de Centre de pièces et services experts inc. dans la mesure nécessaire à la réalisation des réparations.

Droits et retrait du consentement

Je comprends que je peux retirer mon consentement en tout temps, sans frais, en communiquant avec le RPRP. Je comprends également que j'ai le droit d'accéder à mes renseignements personnels, de les faire rectifier et de porter plainte à la Commission d'accès à l'information du Québec (CAI) si j'estime que mes droits ne sont pas respectés.

Signature

Signature	Date

Pour les personnes de moins de 14 ans, ce formulaire doit être signé par le titulaire de l'autorité parentale.

ANNEXE C – FORMULAIRE DE DÉCLARATION D'INCIDENT DE CONFIDENTIALITÉ (INTERNE)

N° d'incident : INC-[] Date de déclaration : []

Section 1 – Informations sur la personne déclarante

Champ	Réponse
Nom et prénom	
Poste / Fonction	
Date et heure de la découverte	
Téléphone / Courriel	

Section 2 – Description de l'incident

Champ	Réponse
Type d'incident	☐ Accès non autorisé ☐ Vol/perte de documents ou d'appareil ☐ Cyberattaque ☐ Envoi incorrect ☐ Autre : []
Description détaillée de l'incident	
Renseignements personnels en cause (types)	
Nombre estimé de personnes affectées	
Systèmes ou supports affectés	

Section 3 – Mesures immédiates prises

--

Section 4 – Évaluation du risque (à compléter par le RPRP)

Critère	Évaluation
Sensibilité des renseignements en cause	☐ Élevée ☐ Modérée ☐ Faible
Risque de préjudice sérieux pour les personnes	☐ Oui ☐ Non ☐ À déterminer
Déclaration à la CAI requise	☐ Oui ☐ Non
Avis aux personnes concernées requis	☐ Oui ☐ Non

Section 5 – Signatures

Personne déclarante	RPRP (validation)
Date : <u> </u>	Date : <u> </u>

ANNEXE D – REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ (MODÈLE)

Ce registre doit être conservé pendant une période minimale de 5 ans à compter de la date de chaque incident. Il doit être tenu à jour par le RPRP et être disponible sur demande de la CAI.
(Réf. : art. 3.7 LPRPSP)

N° d'incident	Date de découverte	Type d'incident	Nature des renseignements en cause	Nbre de personnes affectées	Risque de préjudice sérieux	Déclaration à la CAI (date)	Avis aux personnes (date)	Mesures correctives	Dossier clos (date)
INC-001									

ANNEXE E – REGISTRE DES FORMATIONS DU PERSONNEL (MODÈLE)

Ce registre consigne toutes les formations dispensées aux employés en matière de protection des renseignements personnels. Il doit être conservé et disponible sur demande à titre de preuve de conformité.

Section 1 – Détail des sessions de formation

N° session	Date	Contenu / Thèmes couverts	Durée	Formateur / Animateur	Format	Type (initiale / continue / ponctuelle)

Section 2 – Présences et attestations par session

N° session	Nom de l'employé	Poste / Fonction	Date de complétion	Signature de l'employé	Attestation reçue (O/N)

Centre de pièces et services experts inc. ou Electro-Experts |
Politique de protections Loi 25