



## POLITIQUE ET PROCÉDURE DE GESTION ET DE DESTRUCTION DES DOCUMENTS CONTENANTS DES RENSEIGNEMENTS PERSONNELS

### 1. OBJECTIF

Assurer une gestion adéquate des documents contenant des renseignements personnels depuis leur création jusqu'à leur destruction, tout en respectant les exigences légales et en garantissant la confidentialité.

### 2. PORTÉE

Cette politique s'applique à tous les employés, sous-traitants et partenaires de l'organisation qui manipulent, conservent ou détruisent des documents contenant des renseignements personnels.

### 3. RESPONSABILITÉS

La Commission d'accès à l'information recommande d'identifier des responsables chargés de veiller à la bonne application de cette procédure. Ces responsables doivent s'assurer que tout le personnel est informé et formé à cette procédure. Au sein de notre organisation, les responsables sont:

Nom des responsables	Information de contact
Cynthia Vallée, Directrice Générale	<a href="mailto:cynthia.vallee@aeclafontaine.ca">cynthia.vallee@aeclafontaine.ca</a>
Cindy Turmel, Directrice des services	<a href="mailto:cindy.turmel@aeclafontaine.ca">cindy.turmel@aeclafontaine.ca</a>

### 4. PROCÉDURE DE GESTION DOCUMENTAIRE

#### 4.1 Inventaire des documents

Inventorier tous les types de documents contenant des renseignements personnels, tels que les fichiers des ressources humaines, fichiers clientèles, etc.

#### 4.2 Classification des documents

Définir les niveaux de confidentialité des documents (protégé, confidentiel, secret) en fonction des critères de sensibilité, finalité, quantité, répartition et support.

## **5. CYCLE DE VIE DES DOCUMENTS**

Les documents contenant des renseignements personnels ont un cycle de vie spécifique. De leur création à leur destruction, ils passent par des phases d'utilisation, de conservation et parfois de communication à des tiers. L'organisation est responsable de la gestion confidentielle de ces renseignements tout au long de ce cycle.

## **6. OBLIGATIONS LÉGALES**

Conformément aux lois applicables, des règles spécifiques en matière de sécurité et de destruction doivent être respectées. L'organisation doit prendre des mesures de sécurité pour protéger les renseignements personnels à chaque étape de leur cycle de vie.

## **7. DESTRUCTION DES DOCUMENTS**

Les documents contenant des renseignements personnels doivent être détruits dès que leur finalité est accomplie, en respectant tout délai légal ou calendrier de conservation.

7.1 Quand le responsable de l'affaire ferme le dossier et si le dossier est prêt pour la destruction (voir article ci-dessous), la date de destruction est déterminée selon la norme de l'Association d'entraide communautaire La Fontaine tel que défini dans l'article 5.2 à moins que le responsable de l'affaire détermine qu'une autre date de destruction conviendrait davantage, par exemple, en respect de la loi LSSSS.

7.2 L'Association d'entraide communautaire La Fontaine conserve les dossiers fermés principalement pour satisfaire aux craintes concernant la gestion du risque. En conséquence, il est prudent de conserver le dossier fermé pendant une période déterminée selon la prescription durant laquelle des réclamations peuvent être déposées à l'égard de L'Association d'entraide communautaire La Fontaine. Dans le doute, le responsable de l'affaire devrait désigner la période applicable la plus longue précédant la date de destruction. La date de destruction pour la plupart des dossiers doit être de dix (10) ans après la date de fermeture fixée par le responsable de l'affaire. Une autre date de destruction des dossiers peut être fixée par le responsable de l'affaire selon les circonstances du dossier.

7.3 La date de destruction doit être suspendue dans les cas suivants se rapportant directement ou indirectement à l'affaire : a) une réclamation réelle ou potentielle déposée contre L'Association d'entraide communautaire La Fontaine, b) une demande de divulgation portant sur les renseignements personnels obtenus par L'Association d'entraide communautaire La Fontaine, c) audits et enquêtes gouvernementales. Cela peut être ordonné par la personne responsable de la protection des renseignements personnels.

7.4 La date de destruction de dossiers peut être reportée à tout moment au besoin.

7.5 Cette politique doit s'appliquer de manière à assurer le maintien de la confidentialité des renseignements personnels contenus aux dossiers et le respect des lois applicables en matière de protection des renseignements privés.

7.6 Toute fermeture ou destruction de dossier ou fichier doit au préalable être autorisée par la personne responsable de la protection des renseignements personnels.

### 7.7 Méthode de destruction :

- Papier (Original et toutes les copies): Utiliser une déchiqueteuse, de préférence à découpe transversale. Pour les documents hautement confidentiels, utiliser une déchiqueteuse suivie d'une incinération.
- Médias numériques réutilisables: Pour des supports tels que cartes de mémoire flash (cartes SD, XD, etc.), clés USB, disques durs d'ordinateur, procéder par formatage, réécriture, ou déchiquetage numérique.
- Médias numériques non réutilisables: Pour certains CD, DVD, cartes de mémoire flash, USB et disques durs qui ne seront plus utilisés, opter pour la destruction physique (déchiquetage, broyage, meulage de surface, désintégration, trouage, incinération). Les déchiqueteuses peuvent souvent détruire CDs et DVDs. Utiliser un démagnétiseur pour les disques durs.
- Machines contenant des disques durs: Pour des appareils tels que photocopieurs, fax, numériseurs, imprimantes, etc., écraser les informations sur le disque dur ou retirer et détruire le disque dur lors du remplacement des machines.

### 7.8 Destruction par un tiers (prestataire). Lorsque la destruction est confiée à un prestataire externe, un contrat écrit doit être établi, précisant:

- Le procédé utilisé pour la destruction.
- La reconnaissance par le prestataire que les renseignements traités sont confidentiels.
- L'obligation pour le prestataire d'informer son client s'il fait appel à un sous-traitant pour la destruction.
- Un engagement à la confidentialité signé par les employés du prestataire.
- L'entreposage sécuritaire des documents à détruire dans des locaux sécurisés avec accès limité.
- La possibilité pour le client d'accéder aux locaux du prestataire pendant la durée du contrat.
- L'obligation pour le prestataire de faire régulièrement rapport de la destruction au client.

## 8. FORMATION ET SENSIBILISATION

Il est essentiel de former et de sensibiliser régulièrement le personnel à cette procédure pour garantir sa bonne application.

## 9. RÉVISION DE LA POLITIQUE

Cette politique et procédure seront révisées annuellement pour s'assurer de leur pertinence et de leur conformité avec les évolutions légales et technologiques.

## 10. SIGNALEMENT

Toute violation potentielle de cette politique doit être signalée immédiatement à la personne responsable de la protection des renseignements personnels.