Annexe A
DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

Je, soussigné·e, déclare avoir lu la Politique de confidentialité de Pro-Def Estrie et m’engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité survit à la fin de mon emploi, stage ou bénévolat auprès de Pro-Def Estrie.

Signé à [inscrivez le lieu]

le : [inscrivez la date]

Nom en lettres moulées :

Signature :

Annexe B
INCIDENT DE CONFIDENTIALITÉ : PLAN DE RÉPONSE

Démarches à effectuer

Lorsqu'un·e Employé·e ou Participant·e constate un incident de confidentialité, il ou elle communique avec la directrice générale par le biais d'un formulaire de signalement prévu à cette fin.

La directrice générale identifie les mesures raisonnables pour réduire le risque de préjudice et pour prévenir de nouveaux incidents.

La directrice générale évalue si l'incident présente un risque de préjudice sérieux, selon la définition présentée à l'annexe D.

Dans le cas où l'incident présente un risque de préjudice sérieux, la directrice générale prévient sans délai la Commission d'accès à l'information (CAI) via le formulaire prévu à cette fin et toute personne dont les renseignements personnels sont affectés.

La directrice générale tient un registre de tous les incidents.

La directrice générale répond à la demande de la CAI d'avoir une copie du registre, le cas échéant.

Annexe C
INCIDENT DE CONFIDENTIALITÉ : CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES

Quand

Tel qu'indiqué à l'article 5.5 de la présente politique, un organisme doit aviser « avec diligence » toutes les personnes dont les renseignements personnels ont été touchés par un incident de confidentialité. Cet avis doit être envoyé directement aux personnes concernées. Toutefois, le Règlement sur les incidents de confidentialité prévoit des situations où la communication peut se faire exceptionnellement par le biais d'un avis public, dont lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisme ou d'accroître le préjudice causé aux personnes concernées..

Contenu

Comme c'est le cas pour l'avis écrit à la CAI, l'avis écrit aux personnes concernées doit contenir les éléments suivants :

☐Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description ;

☐Une brève description des circonstances de l'incident ;

☐La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;

☐Une brève description des mesures que l'organisme a prises ou entend prendre suivant l'incident dans le but de réduire les risques de préjudice ;

☐Les mesures que l'organisme suggère à la personne concernée de prendre dans le but de réduire/atténuer les risques de préjudice ;

☐Les coordonnées de la personne auprès de laquelle la personne concernée peut obtenir de plus amples renseignements à propos de l'incident.

Annexe D
INCIDENT DE CONFIDENTIALITÉ : QUESTIONNAIRE D'ÉVALUATION DU « RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »

Évaluer si l'incident présente un risque de préjudice sérieux[1]

Pour tout incident de confidentialité, l'organisation doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, notamment :

1. Quelle est la **sensibilité** des renseignements concernés ?
2. Quelles sont les **conséquences appréhendées** de leur utilisation ?
3. Quelle est la probabilité qu'ils soient utilisés à des **fins préjudiciables ?**

1. Renseignements sensibles

- Documents financiers ;
- Dossiers médicaux ;
- Les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles (nom, adresse) ;
    - Sauf si le contexte en fait des renseignements sensibles : nom, adresses associé·es à des périodiques spécialisés ou à des activités qui les identifient.

2. Préjudice grave

- Humiliation ;
- Dommage à la réputation ou aux relations ;
- Perte de possibilité d'emploi ou d'occasion d'affaires ou d'activités professionnelles ;
- Perte financière ;
- Vol d'identité ;
- Effet négatif sur le dossier de crédit ;
- Dommage aux biens ou leur perte ;

3. Pour déterminer la probabilité d'un mauvais usage

- Qu'est-il arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'atteinte ?
- Qui a eu accès aux renseignements personnels ou aurait pu y avoir accès ?
- Combien de temps les renseignements personnels ont-ils été exposés ?
- A-t-on constaté un mauvais usage des renseignements ?
- L'intention malveillante a-t-elle été démontrée (vol, piratage) ?
- Les renseignements ont-ils été exposés à des entités ou à des personnes susceptibles de les utiliser pour causer un préjudice ou qui représentent un risque pour la réputation de la ou des personnes touchées ?

Si l'analyse fait ressortir un risque de préjudice sérieux, l'organisation doit aviser la Commission et les personnes concernées de l'incident. Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau.