Politique relative à la conservation et à la destruction des dossiers, et aux incidents de confidentialité

Politique d'entreprise

TERMONT

Table des matières

1 – OBJECTIFS

La présente Politique relative à la conservation et à la destruction des dossiers, et aux incidents de confidentialité (la « Politique ») vise plusieurs objectifs. Le premier de ces objectifs est de veiller à ce que les dossiers et les documents de TERMONT Montréal inc. (« TERMONT ») qui le nécessitent soient adéquatement protégés et conservés, et à ce que les dossiers qui ne sont plus requis par TERMONT ou qui n'ont plus de valeur soient détruits en temps utile. La présente Politique a également pour but d'aider le personnel à comprendre leurs obligations en ce qui concerne la conservation des documents papier et électroniques, notamment les courriels, les fichiers Web, les fichiers texte, les fichiers audio et vidéo, les documents en format PDF, l'ensemble des fichiers de la suite Microsoft Office et les autres fichiers formatés.

Le deuxième objectif de la présente Politique est de mettre en place un registre pour y consigner des renseignements sur les incidents de confidentialité visant TERMONT.

Le troisième objectif de la présente Politique est d'adopter un plan d'intervention en cas d'incident de confidentialité, intégré au plan d'intervention en cas d'incident informatique actuel de TERMONT, devant s'appliquer en cas d'incident de confidentialité touchant des renseignements personnels.

La présente Politique est adoptée conformément à certaines dispositions, qui entreront en vigueur le 22 septembre 2023, de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021 c. 25 (le « Projet de loi nº 64 » ou la « Loi 25 »), sanctionnée au Québec le 22 septembre 2021, qui modifie la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1. (la « LPRPSP »). La présente Politique assure également la conformité aux dispositions applicables de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (la « LPRPDE ») qui s'applique aux entités sous réglementation fédérale.

2 – AUTRES POLITIQUES ET LIGNES DIRECTRICES APPLICABLES

TERMONT a adopté une Politique sur la protection des renseignements personnels (la « Politique sur la protection des renseignements personnels ») le 21 novembre 2018, laquelle a été modifiée par la suite. La Politique sur la protection des renseignements personnels résume les pratiques de TERMONT en ce qui concerne les renseignements personnels recueillis et décrit les mesures que TERMONT prend quant à la collecte, l'utilisation, la divulgation, la protection et le traitement des renseignements personnels en conformité avec ses obligations contenues dans les lois sur la protection des renseignements personnels.

Afin de s'assurer de bien la comprendre, la présente Politique relative à la conservation et à la destruction des dossiers, et aux incidents de confidentialité doit être lue conjointement avec la Politique sur la protection des renseignements personnels, de sorte que ces deux documents puissent être harmonisés sans contradiction.

3 – CALENDRIER DE CONSERVATION DES DOSSIERS

Vous trouverez en Annexe A un Calendrier de conservation des dossiers qui est approuvé à titre de calendrier initial de la tenue, de la conservation et de la destruction des dossiers physiques de TERMONT et de la conservation et de la destruction des documents papier et électroniques.

Le Responsable de la protection des renseignements personnels de TERMONT supervise l'administration de la présente Politique et la mise en œuvre des processus et des procédures visant à s'assurer du respect du calendrier de conservation des dossiers. Le Responsable de la protection des renseignements personnels de TERMONT est également autorisé à faire ce qui suit :

- apporter des modifications au Calendrier de conservation des dossiers de temps à autre afin de s'assurer qu'il est conforme aux lois locales, provinciales et fédérales et qu'il comprend les catégories de documents et de dossiers pertinents pour TERMONT;
- surveiller les lois locales, provinciales et fédérales qui touchent la conservation des dossiers;
- passer annuellement en revue le programme de conservation et de destruction des dossiers;
- surveiller la conformité avec la présente Politique.

4 – INTERRUPTION DE LA DESTRUCTION DES DOSSIERS EN CAS DE LITIGE OU DE RÉCLAMATION

Si TERMONT se voit signifier une citation à comparaître ou une demande de documents, ou si une personne a connaissance d'une enquête ou d'une vérification gouvernementale concernant TERMONT ou de l'introduction d'un litige contre TERMONT ou la concernant, une telle personne doit en informer le Responsable de la protection des renseignements personnels de TERMONT, et toute destruction de documents doit être interrompue jusqu'à ce que le Responsable de la protection des renseignements personnels de TERMONT, suivant les recommandations d'un conseiller juridique, n'en décide autrement. Le Responsable de la protection des renseignements personnels de TERMONT doit prendre les mesures nécessaires pour aviser sans délai tous les membres du personnel de l'interruption de la destruction des documents.

5 – REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Vous trouverez en Annexe B un Registre des incidents de confidentialité qui est approuvé pour l'inscription de tous les incidents de confidentialité concernant TERMONT.

Les incidents de confidentialité comprennent tout accès non autorisé à des renseignements personnels, toute utilisation ou communication non autorisée de renseignements personnels, toute perte de renseignements personnels ou toute autre atteinte à la protection de ces renseignements.

Lorsqu'un incident de confidentialité concernant TERMONT survient, le Responsable de la protection des renseignements personnels de TERMONT doit veiller à ce que le Registre des incidents de confidentialité soit rempli et à ce que tous les renseignements requis y soient inscrits, et doit le mettre à la disposition des organismes de réglementation (si nécessaire).

-

6 – PLAN D'INTERVENTION EN CAS D'INCIDENT DE CONFIDENTIALITÉ

Vous trouverez en Annexe C le Plan d'intervention en cas d'incident de confidentialité de TERMONT, qui est approuvé en tant que module ajouté au Plan d'intervention en cas d'incident informatique existant de TERMONT et qui vise les incidents de confidentialité.

Il convient de mentionner que les incidents de confidentialité ne résultent pas tous d'un incident informatique et ne sont pas tous de nature criminelle. Par conséquent, certaines polices d'assurance pourraient ne pas s'appliquer. Le Plan d'intervention en cas d'incident de confidentialité contient des renseignements relatifs à la police d'assurance contre les cyber risques de TERMONT qui s'appliquent dans les cas où un incident de confidentialité découle d'un incident informatique. D'autres polices d'assurance (comme une assurance de la responsabilité civile des entreprises ou une assurance de la responsabilité civile des administrateurs et des dirigeants) peuvent s'appliquer dans le cas d'un incident de confidentialité.

7 – APPLICABILITÉ

La présente Politique s'applique à tous les dossiers physiques générés par TERMONT, y compris les documents originaux et les copies. Elle s'applique également aux documents papier et électroniques mentionnés ci-dessus.

La présente Politique s'applique à tous les incidents de confidentialité concernant TERMONT.

8 – ANNEXE A – CALENDRIER DE CONSERVATION DES DOSSIERS

Le Calendrier de conservation des dossiers est organisé de la façon suivante :

- Dossiers d'emploi

Le Calendrier de conservation des dossiers sera complété sur une base continue en fonction des exigences réglementaires et/ou juridiques et des bonnes pratiques.

Nouveau numéro	Ancien numéro pouvant figurer sur les boîtes	Type de document	Nombre d'années de conservation recommandé	Commentaires
HR-1	2220/2250/2260	Documents liés aux candidatures, que les candidats soient embauchés ou non (curriculum vitae, vérification de casier judiciaire, examen médical ou évaluation des compétences, etc.)	4	Ces documents sont conservés jusqu'à la fin du processus d'embauche, plus 4 ans. Selon le délai de prescription de 3 ans + délai supplémentaire de 1 an
FIN -2	3520 à 3536	Documents de paie, feuilles de temps, congés	7	Au Québec, ces documents sont conservés tout au long de l'emploi jusqu'à sa cessation, + le délai de prescription, + un délai supplémentaire de 1 an Au Québec, le délai de prescription est de 3 ans.
HR-2	2320/2405/2430/ 2470/2610	Documents relatifs à l'emploi : contrats d'emploi, lettres de congédiement, preuves de mesures disciplinaires, etc., hormis les dossiers médicaux	4	Ces documents sont conservés tout au long de l'emploi jusqu'à la fin du dernier de ces 3 événements à survenir : a) la cessation d'emploi; b) le versement des prestations, notamment les prestations de retraite, s'il y a lieu; + le délai de prescription (3 ans), + un délai supplémentaire de 1 an
HR-3	2220/2415	Renseignements utilisés pour la réalisation d'un plan d'équité salariale	6	Les renseignements sont conservés pendant la période qui précède la publication des résultats d'un audit relatif à l'équité salariale ou de tout renseignement utilisé dans le cadre d'un tel audit, plus un délai de 6 ans.
HR-4	2435/2445/2450/ 2455	Documents relatifs à l'assurance-emploi, y compris les dossiers d'emploi	7	Ces documents sont conservés jusqu'à la fin de l'année pour laquelle ils étaient gardés, plus un délai de 7 ans.
HR-5	2620	Ententes et programmes de formation, factures et contrats relatifs à la formation	7	Ces documents sont conservés jusqu'à la fin du dernier exercice auquel les dépenses de formation se rapportent, plus un délai de 7 ans.

HR-6		Dossiers médicaux des employés	41	La *Loi sur la santé et la sécurité du travail* prévoit que le directeur de santé publique doit conserver le dossier médical d'un travailleur pendant une période d'au moins 20 ans après la fin de son emploi ou de 40 ans après le début de son emploi, selon la plus longue durée.

9 – ANNEXE B – REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Le Registre des incidents de confidentialité exige la collecte des renseignements suivants :

- Identification (numéro d'identification de l'incident; numéro de dossier de l'organisme de réglementation, s'il y a lieu)
- Description (description sommaire de l'incident; catégories de renseignements personnels; date de l'incident; date de prise de connaissance par l'entité pertinente; nombre de personnes touchées; mesures correctives)
- Évaluation (risque de préjudice sérieux pour les personnes touchées; motifs pour lesquels un avis n'est pas remis aux organismes de réglementation ou aux personnes touchées)
- Avis (s'il y a lieu) (date de l'avis à l'organisme de réglementation; date de l'avis aux personnes touchées; type d'avis et motifs)
- Gouvernance (nom de la personne qui remplit le registre; durée de conservation minimale du dossier)

Registre des incidents de confidentialité	
Ce registre est préparé conformément à la législation en matière de protection des renseignements personnels canadienne (LPRPDE) et québécoise (LPRPSP) qui concerne la notification d'incidents. Dans le cas du Québec, il doit être conservé pendant cinq ans après la prise de connaissance de l'incident. Dans les autres cas, il doit être conservé pendant deux ans après une telle prise de connaissance. Vous devez toujours consulter votre conseiller en atteinte à la confidentialité ou votre conseiller juridique avant de finaliser le registre.	
Un incident de confidentialité désigne : ➢ l'accès non autorisé à un renseignement personnel; ➢ l'utilisation ou la communication non autorisée d'un renseignement personnel; ➢ la perte d'un renseignement personnel; ➢ toute autre atteinte à la protection d'un tel renseignement.	
Description sommaire	*Fournir une description sommaire et une catégorisation (p. ex. un accès non autorisé dans le cadre d'une attaque par rançongiciel ayant touché les serveurs de fichiers nord-américains de l'organisation ou la perte d'un téléphone cellulaire d'entreprise non protégé). Éviter de discuter des causes profondes ou du vecteur d'attaque (p. ex. attaque par force brute d'un compte administrateur avec un mot de passe faible exposé sur Internet ou employé ayant cliqué sur un lien contenu dans un courriel d'hameçonnage ou employé en état d'ébriété lors d'une soirée).*
Type de renseignements personnels	*Fournir uniquement des catégories de renseignements personnels, ne pas inclure les renseignements (p. ex. le numéro d'assurance sociale, les numérisations de passeport, les adresses postales, les évaluations de rendement d'un employé, les mots de passe de comptes). Si ces renseignements sont inconnus, expliquer brièvement la raison.*
Date de l'incident	*Indiquer la date de l'incident ou la période pendant laquelle il a eu lieu, ou en donner une approximation.*
Date de connaissance	*Indiquer la date de la prise de connaissance de l'incident ou la période pendant laquelle il y a eu prise de connaissance de l'incident, ou en donner une approximation.*
Nombre de personnes touchées	*Indiquer le nombre exact ou approximatif de personnes touchées.*
Mesures correctives	*Fournir une description sommaire des mesures prises en réponse à l'incident (p. ex. une enquête interne appuyée par des intervenants externes en cybersécurité dès la découverte de l'incident, l'isolement des actifs compromis, le déploiement d'un logiciel de détection et d'intervention aux terminaux pour atteindre une couverture de 98 %, la réinitialisation de tous les mots de passe utilisés avec la suite Microsoft Office 365, la surveillance du Web caché).*
Risque de préjudice sérieux pour les personnes touchées	*Fournir une description sommaire des éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées. À cet égard, la loi identifie les facteurs suivants :* ➢ *la sensibilité des renseignements personnels concernés;* ➢ *les utilisations malveillantes possibles de ces renseignements;* ➢ *les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables.*
Avis à l'organisme de réglementation	*Indiquer la date à laquelle l'avis ou les avis ont été transmis à la Commission d'accès à l'information et/ou au Commissariat à la protection de la vie privée du Canada ou à un autre organisme de réglementation.*
Avis aux personnes touchées	*Indiquer la date à laquelle l'avis a été transmis aux personnes touchées.*
Type d'avis	*Indiquer le type d'avis (p. ex. de façon indirecte au moyen d'un avis sur le site Web, d'un avis envoyé aux médias ou d'un communiqué de presse, ou de façon directe par messager, par courriel, par téléphone ou de vive voix, tout en précisant les mesures correctives prises comme la réinitialisation des comptes, un gel de sécurité ou un service de surveillance du dossier de crédit gratuit).*
Date de conservation	*Si l'incident a visé des renseignements personnels du Québec, vous devez conserver le registre d'incident pendant cinq ans après la date de la prise de connaissance. Dans le cas de renseignements personnels dans le reste du Canada, le registre doit être conservé pendant deux ans après la date de la prise de connaissance.*

Registre des incidents de confidentialité

Identification		Renseignements exigés par la réglementation											Gouvernance	
		Description						Évaluation		Avis (s'il y a lieu)				
Numéro d'identification de l'incident	Numéro de dossier de l'organisme de réglementation (s'il a été avisé de l'incident)	Description sommaire de l'incident	Catégories de renseignements personnels	Date de l'incident	Date de prise de connaissance par l'organisation	Nombre de personnes touchées	Mesures correctives	Risque de préjudice sérieux pour les personnes touchées	Motifs d'absence d'avis aux organismes de réglementation / personnes touchées	Date de l'avis à l'organisme de réglementation	Date de l'avis aux personnes touchées	Type d'avis et motifs d'un avis indirect	Nom de la personne qui a rempli le registre	Durée de conservation minimale du registre
					9/1/2022									9/1/2027

10 – ANNEXE C –PLAN D'INTERVENTION EN CAS D'INCIDENT DE CONFIDENTIALITÉ

Le Plan d'intervention en cas d'incident de confidentialité prévoit les éléments suivants :

- l'équipe d'intervention rapide CORE et le personnel clé de TERMONT
- les ressources (liste de contacts; résumé des garanties de la police d'assurance contre les cyber risques (s'il y a lieu); inventaire des renseignements personnels /mappage des données)
- la procédure d'intervention en cas d'atteinte à la sécurité (évaluation; signalisation progressive; gestion; autopsie; gestion des réclamations)
- le protocole de déclaration des atteintes à la confidentialité
- le processus d'évaluation et de signalisation progressive des incidents (indice de gravité de l'atteinte)

TELLE QU'ADOPTÉE PAR LE CONSEIL D'ADMINISTRATION LE 24 AOÛT 2023, ENTRÉE EN VIGUEUR LE 22 SEPTEMBRE 2023.