



## **Politique de protection des renseignements personnels et de confidentialité**

L'union des travailleuses et travailleurs accidentés ou malades (**uttam**) respecte le droit à la vie privée de chaque individu et s'engage à protéger la confidentialité des renseignements personnels recueillis auprès de son personnel et des travailleuses et travailleurs accidentés ou malades. En règle générale, les renseignements personnels sont disponibles seulement aux personnes qui doivent y avoir accès dans l'exercice de leurs fonctions au sein de l'**uttam**.

## Table des matières

Définitions.....	3
1. Contexte.....	4
2. Application.....	4
3. Collecte, utilisation et communication.....	5
a. Consentement.....	6
b. Collecte des renseignements auprès de la personne elle-même.....	6
c. Collecte auprès de tiers.....	6
d. Détention et utilisation des renseignements.....	7
e. Communication.....	7
f. Autres moyens technologiques utilisés.....	8
4. Conservation et destruction des renseignements personnels.....	8
a. Information en format papier.....	8
b. Information en format électronique.....	9
5. Responsabilité de l' <b>uttam</b> .....	9
6. Sécurité des données.....	9
7. Droits d'accès, de rectification et de retrait du consentement.....	10
8. Processus de traitement des plaintes.....	10
a. Incident de confidentialité.....	10
b. Traitement des plaintes liées à la confidentialité.....	11
9. Approbation.....	12
a. Responsable de la protection des renseignements personnels.....	12
10. Publication et modifications.....	13
11. Évaluation sommaire des facteurs relatifs à la vie privée.....	13
Annexe A	
Politique de confidentialité et de respect de la vie privée.....	14
Annexe B	
Liste non exhaustive sur les types de renseignements.....	17
Annexe C	
Déclaration relative à la confidentialité.....	18
Annexe D	
Incident de confidentialité : Plan de réponse.....	19
Annexe E	
Incident de confidentialité : contenu de la communication aux personnes concernées.....	20
Annexe F	
Incident de confidentialité : questionnaire d'évaluation du « risque sérieux de préjudice grave » .....	21
Annexe G	
Formulaire de signalement.....	22
Annexe H	
Rapport d'incident de confidentialité et/ou de sécurité.....	24

## DÉFINITIONS

### « Incident de confidentialité »

Tout accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

### « Membre/non-membre »

Travailleuses et travailleurs victimes de lésions professionnelles qui consultent l'**uttam** et qui fournissent des renseignements personnels à l'organisme en lien avec la réalisation de sa mission, notamment, de les soutenir dans l'exercice de leurs droits à la suite d'une lésion professionnelle et, à ce titre, de les représenter lors de contestations faites à la révision administrative de la Commission des normes, de l'équité, de la santé et de la sécurité du travail.

### « Personnel de l'uttam »

Conseil d'administration, équipe de la permanence, militantes et militants.

### « Rapport d'incident de confidentialité et/ou de sécurité »

Le formulaire mis à la disposition de toute personne (Conseil d'administration, permanence de l'**uttam**, militantes et militants ainsi que les travailleuses et travailleurs accidentés ou malades), afin d'informer la personne responsable des renseignements personnels.

### « Registre des incidents de confidentialité »

L'ensemble des renseignements consignés sur des incidents déclarés et concernant les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises en réaction à l'incident. Les dates pertinentes y figurent aussi : survenance de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.

### « Risque sérieux de préjudice »

Le risque évalué à la suite d'un incident de confidentialité qui pourrait porter préjudice aux personnes concernées. Ce risque est analysé par la personne responsable des renseignements personnels. Pour tout incident de confidentialité, la personne responsable évalue la gravité du risque de préjudice pour les personnes concernées en estimant « la sensibilité des renseignements concernés », « les conséquences appréhendées de leur utilisation » et « la probabilité qu'ils soient utilisés à des fins préjudiciables ».

### « Renseignements personnels »

Tout renseignement fourni ou communiqué à l'**uttam** sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre) qui concerne le personnel de l'**uttam**, ainsi que les travailleuses et travailleurs qui consultent l'organisme, et qui peut être utilisé pour l'identifier, y compris : son nom, son numéro de téléphone, son adresse, son courriel, son genre, son orientation sexuelle et toute information concernant sa santé.

## 1. Contexte

L'union des travailleuses et travailleurs accidentés ou malades (**uttam**) est un organisme à but non lucratif qui traite des renseignements personnels dans le cadre de ses activités.

La présente politique vise à assurer la protection des renseignements personnels et à encadrer la manière dont l'**uttam** collecte, utilise, communique, conserve et détruit ces renseignements personnels ou dont, autrement, elle les gère.

De plus, elle vise à informer toute personne intéressée sur la manière dont elle traite leurs renseignements personnels.

Cette politique s'ajoute à la *Politique de confidentialité et de respect de la vie privée* qui traite des renseignements personnels recueillis par l'**uttam** par un moyen électronique que vous retrouvez à l'**Annexe A**.

Le personnel de l'**uttam** est tenu de signer la présente entente de confidentialité (**Annexe C**) avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès de l'**uttam**.

L'obligation de confidentialité s'applique à la durée de la relation du personnel avec l'**uttam** et survit à la fin de cette relation.

## 2. Application

Cette politique s'applique à l'**uttam**, ce qui inclut les membres de son Conseil d'administration et de la permanence ainsi que les militantes et militants qui s'impliquent auprès de l'organisme. Elle s'applique également à l'égard du site Internet contrôlé et maintenu par l'**uttam**.

Elle vise tous les types de renseignements personnels gérés par l'**uttam**, que ce soient les renseignements de son personnel (Conseil d'administration, équipe de la permanence, militantes et militants), des membres et non membres de l'**uttam** (travailleuses et travailleurs victimes de lésions professionnelles qui consultent l'organisme), de ses consultants (notamment, avocats et médecins) et de toute personne appelée à soumettre des renseignements personnels à l'organisme.

En application de la présente politique, un renseignement personnel est un renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier. À titre d'exemple, il pourrait s'agir du nom, de l'adresse, de l'adresse courriel, du numéro de téléphone, du genre ou de renseignements bancaires d'une personne, de renseignements sur sa santé, son origine ethnique, sa langue, etc.

Un renseignement personnel sensible est un renseignement envers lequel il y a un haut risque d'atteinte raisonnable en matière de vie privée comme les renseignements de santé, bancaires, ceux relatifs à l'orientation sexuelle, l'origine ethnique, les croyances religieuses ou philosophiques, etc.

De manière générale, les coordonnées professionnelles d'une personne ne constituent pas des renseignements personnels, par exemple, le nom, le titre, l'adresse, l'adresse courriel ou le numéro de téléphone du lieu de travail d'une personne. Plus particulièrement, et par souci de précision, au sens de la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec, et à compter du 22 septembre 2023, les sections 3 (collecte, utilisation, communication), 4 (conservation et destruction) et 6 (sécurité des données) ne s'appliquent pas aux renseignements d'une personne relatifs à l'exercice d'une fonction au sein d'un organisme, tels que son nom, son titre, sa fonction ainsi que l'adresse, l'adresse courriel et le numéro de téléphone de son lieu de travail.

Ces mêmes paragraphes ne s'appliquent pas non plus à un renseignement personnel qui a un caractère public en vertu de la loi, et ce, dès l'entrée en vigueur de la présente politique.

### **3. Collecte, utilisation et communication**

Dans le cadre de ses activités, l'**uttam** peut collecter différents types de renseignements, et ce, à différentes fins. Les types de renseignements que l'**uttam** pourrait collecter, leur utilisation (ou l'objectif visé) ainsi que les moyens par lesquels les renseignements sont recueillis sont indiqués à l'**Annexe B** de la présente politique.

L'**uttam** informe également les personnes concernées, au moment de la collecte des renseignements personnels et de tout autre renseignement recueilli, des fins pour lesquelles ils sont collectés et les moyens de la collecte, en plus des autres informations à fournir tel que requis par la loi.

En application de la présente politique, l'**uttam** peut, au besoin, constituer un ou des dossiers contenant des renseignements personnels concernant son personnel. La constitution de tels dossiers a pour objet de :

- Maintenir les coordonnées à jour;
- Permettre, dans le cas de son personnel rémunéré, la réalisation de tâches administratives requises ou permises par la loi (impôts sur le revenu, assurances collectives, etc.).

L'**uttam** peut également, au besoin, constituer des dossiers contenant des renseignements personnels concernant les travailleuses et travailleurs qui consultent l'organisme. La constitution de tels dossiers a pour objet de permettre à l'**uttam** de réaliser sa mission de les soutenir dans l'exercice de leurs droits à la suite d'une lésion

professionnelle et, à ce titre, de les représenter lors de contestations faites à la révision administrative de la Commission des normes, de l'équité, de la santé et de la sécurité du travail.

L'**uttam** applique les principes généraux qui suivent relativement à la collecte, l'utilisation et la communication des renseignements personnels.

**a. Consentement :**

De façon générale, l'**uttam** collecte les renseignements personnels directement auprès de la personne concernée et avec son consentement, sauf si une exception est prévue par la loi.

La personne concernée étant le personnel du Conseil d'administration et de l'équipe de la permanence, les militantes et militants, les membres et non membres de l'**uttam** (travailleuses et travailleurs victimes de lésions professionnelles qui consultent l'organisme), ses consultants et toute personne appelée à soumettre des renseignements personnels à l'organisme.

Le consentement peut être obtenu de façon implicite dans certaines situations, par exemple, lorsque la personne décide de fournir ses renseignements personnels après avoir été informée par la présente politique sur l'utilisation et la communication aux fins qui y sont indiquées (**Annexe B**). La présente politique et les informations qu'elle contient pourront être consultées par la personne concernée au moment de la collecte des renseignements personnels.

L'**uttam** doit toutefois obtenir le consentement de la personne concernée avant de collecter ses renseignements personnels auprès de tiers, avant de les communiquer à des tiers ou pour toute utilisation secondaire à ceux-ci.

**b. Collecte des renseignements auprès de la personne elle-même:**

Dans tous les cas, l'**uttam** ne collecte des renseignements que si elle a une raison valable de le faire. La collecte est limitée au renseignement nécessaire dont elle a besoin pour remplir l'objectif visé.

Les services offerts par l'**uttam** visent généralement des personnes majeures. L'équipe de la permanence offre des services d'aide et de soutien nécessaires au règlement des dossiers de travailleuses et travailleurs victimes de lésions professionnelles.

**c. Collecte auprès de tiers :**

L'**uttam** peut collecter des renseignements personnels auprès de tiers. À cet effet, l'**uttam** demande le consentement de la personne concernée avant de collecter des renseignements personnels la concernant auprès d'un tiers visé.

Dans les cas où un tel renseignement n'est pas collecté directement auprès de la personne elle-même, mais auprès d'un établissement ou organisme (clinique/Cnésst), la personne concernée peut demander la source des renseignements collectés à l'**uttam**.

#### **d. Détention et utilisation des renseignements :**

L'**uttam** veille à ce que les renseignements qu'elle détient soient à jour et exacts au moment de leur utilisation pour prendre une décision relative à la personne visée.

Elle ne peut utiliser les renseignements personnels d'une personne que pour les raisons indiquées dans la présente politique ou pour toutes autres raisons fournies lors de la collecte. Dès que l'**uttam** souhaite utiliser ces renseignements pour une autre raison ou une autre fin, un nouveau consentement devra être obtenu de la personne concernée, lequel devra être obtenu de façon expresse, s'il s'agit d'un renseignement personnel sensible.

Accès limité : l'**uttam** met en place des mesures pour limiter l'accès à un renseignement personnel seulement aux membres de son personnel (équipe de la permanence – militantes et militants) qui agit au sein de son organisation, qui ont la qualité pour en prendre connaissance et pour qui ce renseignement est nécessaire dans l'exercice de leurs fonctions.

Les renseignements personnels sensibles ne sont accessibles qu'à l'équipe de la permanence.

#### **e. Communication :**

En règle générale, et à moins d'une exception indiquée dans la présente politique ou autrement prévue par la loi, l'**uttam** obtiendra le consentement de la personne concernée avant de communiquer ses renseignements personnels à un tiers. De plus, lorsque le consentement est nécessaire et lorsqu'il s'agit d'un renseignement personnel sensible, l'**uttam** devra obtenir le consentement explicite de façon verbale de la personne avant de communiquer le renseignement.

Des renseignements personnels de la personne concernée peuvent être communiqués à des tiers dans les cas qui suivent :

- à son représentant/avocat;
- à ses consultants. Par exemple, les consultants peuvent être des médecins spécialisés pour l'exécution de mandats dans la réalisation des activités professionnelles de l'**uttam**.

Ces professionnels sont également soumis au secret professionnel par l'entremise de leur code de déontologie.

#### **f. Autres moyens technologiques utilisés :**

L'**uttam** peut recueillir également des renseignements personnels par l'entremise de moyens technologiques comme des formulaires Web intégrés à un site Internet contrôlé par l'**uttam** (par exemple son formulaire d'adhésion pour faire un don) et des questionnaires accessibles en ligne sur ses plateformes et ses applications (sondages).

Si l'**uttam** recueille des renseignements personnels en offrant un produit ou un service technologique qui dispose de paramètre de confidentialité, l'**uttam** doit s'assurer que ses paramètres offrent un niveau de confidentialité conforme (**Annexe A**).

### **4. Conservation et destruction des renseignements personnels**

Sauf si une durée minimale de conservation est requise par la loi ou la réglementation applicable, l'**uttam** conservera les renseignements personnels collectés selon les paramètres suivants :

#### **a. Information en format papier :**

Pour les non-membres de l'organisation, les renseignements personnels utilisés par l'**uttam** quant à la gestion des dossiers des travailleuses et travailleurs victimes de lésions professionnelles sont conservés pour une durée de 3 ans après que le dossier soit devenu passif. L'objectif de cette conservation étant de permettre la réactivation du dossier à la demande de la personne concernée. Cependant, la personne peut demander de récupérer son dossier complet ou demander de le détruire.

À la fin de la durée de conservation ou lorsque les renseignements personnels ne sont plus nécessaires, l'**uttam** s'assurera :

1. de les détruire elle-même ; ou
2. de mandater une entreprise pour les détruire.

La destruction des renseignements par l'**uttam** doit être faite de façon sécuritaire, afin d'assurer la protection de ces renseignements.

Les dossiers format papier des membres sont conservés en permanence tant que la personne demeure membre de l'organisme. Le dossier étant, par la suite, traité de manière identique que pour le dossier des personnes non-membres.

Toute personne dont des renseignements personnels auront été collectés par l'**uttam** peut demander d'obtenir son dossier et/ou de supprimer toute information personnelle la concernant, lorsque le renseignement est périmé, parce que sa conservation n'est plus justifiée au regard de la finalité pour laquelle il a été recueilli ou parce qu'il a été recueilli de manière non conforme à la loi.



## **b. Information en format électronique :**

Toute l'information personnelle enregistrée dans la banque de données informatique de l'**uttam** est conservée indéfiniment, sauf si la personne demande la destruction complète de toute l'information la concernant.

## **5. Responsabilité de l'uttam**

De façon générale, l'**uttam** est responsable de la protection des renseignements personnels qu'elle détient.

Le responsable de la protection des renseignements personnels de l'**uttam** est un membre de la permanence de l'organisme. Il doit, de façon générale, veiller à assurer le respect de la législation applicable concernant la protection des renseignements personnels. Le responsable doit approuver les politiques et pratiques encadrant la gouvernance des renseignements personnels. Plus particulièrement, cette personne est chargée de mettre en œuvre la présente politique et de veiller à ce qu'elle soit connue, comprise et appliquée. En cas d'absence ou d'impossibilité d'agir de ce responsable, le responsable adjoint, membre du conseil d'administration, assurera les fonctions du responsable de la protection des renseignements personnels.

Les membres du personnel de l'**uttam** ayant accès à des renseignements personnels ou étant autrement impliqués dans la gestion de ceux-ci doivent en assurer leur protection et respecter la présente politique.

Les rôles et les responsabilités du personnel de l'**uttam** tout au long du cycle de vie des renseignements personnels peuvent être précisés par tout autre politique de l'**uttam** à cet égard, le cas échéant.

## **6. Sécurité des données**

L'**uttam** s'engage à mettre en place des mesures de sécurité raisonnables pour assurer la protection des renseignements personnels qu'elle gère. Les mesures de sécurité en place correspondent, entre autres, à la finalité, à la quantité, à la répartition, au support et à la sensibilité des renseignements. Cela signifie qu'un renseignement pouvant être qualifié de sensible (voir la définition prévue à la section 2) devra faire l'objet de mesures de sécurité plus importantes et devra être mieux protégé.

Notamment, et conformément à ce qui a été mentionné précédemment concernant l'accès limité aux renseignements personnels, l'**uttam** doit mettre en place des mesures nécessaires pour imposer des contraintes aux droits d'utilisation de ses systèmes d'information de manière que seuls les membres de son personnel qui doivent y avoir accès soient autorisés à y accéder. Les membres de l'équipe de la permanence ayant accès aux documents électroniques s'obligent à s'assurer que tous ces documents

comportant des renseignements personnels, incluant ceux copiés sur un appareil de stockage portatif, soient protégés par des mots de passe individuels.

## **7. Droits d'accès, de rectification et de retrait du consentement**

Pour faire valoir ses droits d'accès, de rectification ou de retrait du consentement, la personne concernée doit soumettre une demande écrite à cet effet au responsable de la protection des renseignements personnels de l'**uttam**, à l'adresse électronique indiquée à la section 9 ou par la poste.

Sous réserve de certaines restrictions légales, les personnes concernées peuvent demander l'accès à leurs renseignements personnels détenus par l'**uttam** et en demander leur correction dans le cas où ils sont inexacts, incomplets ou équivoques.

Le responsable de la protection des renseignements personnels de l'**uttam**, doit répondre par écrit à ces demandes dans les 30 jours de la date de réception de la demande. Tout refus doit être motivé et accompagné de la disposition légale justifiant le refus. Dans ce cas, la réponse doit indiquer les recours en vertu de la loi et le délai pour les exercer. Le responsable doit aider le requérant à comprendre le refus au besoin.

Sous réserve des restrictions légales applicables, les personnes concernées peuvent retirer leur consentement à la communication ou à l'utilisation des renseignements recueillis.

Elles peuvent également demander à l'**uttam** quels sont les renseignements recueillis auprès d'elle, les catégories de personnes à l'**uttam** qui y ont accès et leur durée de conservation.

## **8. Processus de traitement des plaintes**

### **a. Incident de confidentialité**

La personne responsable d'assurer la protection des renseignements personnels, dont les coordonnées apparaissent au point 9, s'assure de la tenue d'un Registre des incidents de confidentialité.

En application de la présente politique, un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisé par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

Lorsqu'un membre du personnel de l'**uttam** ou qu'une travailleuse ou un travailleur accidenté ou malade constate un incident de confidentialité, il ou elle doit informer

avec diligence la personne responsable de la protection des renseignements personnels afin qu'il soit inscrit au registre. Le membre du personnel, la travailleuse ou le travailleur doit, pour ce faire, compléter un formulaire de signalement (**Annexe G**) et l'acheminer ensuite à la personne responsable de la protection des renseignements personnels.

Le Registre doit conserver les informations sur un incident de confidentialité pour une période de cinq ans.

Doit être colligé dans le formulaire de signalement :

- 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);
- La date ou la période à laquelle l'organisme s'est aperçu de l'incident;
- Le nombre de personnes concernées par l'incident (une approximation si cette information n'est pas connue).

La personne responsable juge si l'incident présente un « risque sérieux de préjudice » (**Annexe F**). Les renseignements ainsi que les mesures à prendre afin de diminuer le risque qu'un préjudice sérieux soit causé aux personnes concernées sont versés au Registre.

Si l'incident présente un risque sérieux de préjudice, la personne responsable avise la Commission d'accès à l'information et les personnes concernées de tout incident présentant un risque sérieux de préjudice à l'aide du formulaire approprié (**Annexes E et G**).

## **b. Traitement des plaintes liées à la confidentialité**

Toute personne qui souhaite formuler une plainte relative à l'application de la présente politique ou, plus généralement, à la protection de ses renseignements personnels par l'**uttam**, doit le faire par écrit en s'adressant au responsable de la protection des renseignements personnels de l'**uttam**, à l'adresse courriel indiquée à la section suivante ou par la poste.

La personne devra indiquer son nom, ses coordonnées pour le joindre, incluant un numéro de téléphone, ainsi que l'objet et les motifs de sa plainte, en donnant suffisamment de détails pour que celle-ci puisse être évaluée par l'**uttam**. Si la plainte formulée n'est pas suffisamment précise, le responsable de la protection des renseignements personnels peut requérir toute information additionnelle qu'il juge nécessaire pour pouvoir évaluer la plainte.

L'**uttam** s'engage à traiter toute plainte reçue de façon confidentielle.

Dans les 30 jours suivant la réception de la plainte ou suivant la réception de tous les renseignements additionnels jugés nécessaires et requis par le responsable de la protection des renseignements personnels de l'**uttam** pour pouvoir la traiter, ce dernier doit l'évaluer et formuler une réponse motivée écrite par courriel ou par la poste, au plaignant. Cette évaluation visera à déterminer si le traitement des renseignements personnels par l'**uttam** est conforme à la présente politique, à toute autre politique et pratique en place au sein de l'organisation et à la législation ou réglementation applicable.

Dans le cas où la plainte ne peut être traitée dans ce délai, le plaignant doit être informé des motifs justifiant l'extension de délai, de l'état d'avancement du traitement de sa plainte et du délai raisonnable nécessaire pour pouvoir lui fournir une réponse définitive.

L'**uttam** doit constituer un dossier distinct pour chacune des plaintes qui lui sont adressées. Chaque dossier contient la plainte, l'analyse et la documentation à l'appui de son évaluation, ainsi que la réponse envoyée à la personne à l'origine de la plainte.

Il est également possible de déposer une plainte auprès de la Commission d'accès à l'information : <https://www.cai.gouv.qc.ca/diffusion-de-l'information/services-et-formulaires/> du Québec ou à tout autre organisme de surveillance en matière de protection des renseignements personnels responsable de l'application de la loi concernée par l'objet de la plainte.

Toutefois, l'**uttam** invite toute personne intéressée à s'adresser d'abord à son responsable de la protection des renseignements personnels et attendre la fin du processus de traitement de la plainte par l'**uttam**.

## 9. Approbation

La présente politique est approuvée par le Conseil d'administration de l'**uttam** et par le responsable de la protection des renseignements personnels de l'**uttam**, dont les coordonnées professionnelles sont les suivantes.

### a. Responsable de la protection des renseignements personnels :

**Isabelle Aubé**

2348 rue Hochelaga  
Montréal, Québec  
H2K 1H8

[Isabelle.aube@uttam.quebec](mailto:Isabelle.aube@uttam.quebec)

Pour toute demande, question ou commentaire dans le cadre de la présente politique, veuillez communiquer avec la responsable par courriel ou par la poste.

## **10. Publication et modifications**

La présente politique est publiée sur le site Internet de l'**uttam**, et ce, relativement aux renseignements personnels qui y sont recueillis. Cette politique est également diffusée par tout moyen propre à atteindre les personnes concernées.

L'**uttam** s'engage également à faire de même pour toutes les modifications à la présente politique, lesquelles devront également faire l'objet d'un avis pour en informer les personnes concernées.

## **11. Évaluation sommaire des facteurs relatifs à la vie privée**

L'**uttam** s'engage à faire une évaluation des facteurs relatifs à la vie privée selon le guide fourni par la Commission d'accès à l'information du Québec dans les situations suivantes :

- Un projet impliquant des renseignements personnels;
- Un projet risquant d'avoir une incidence sur le respect de la vie privée des personnes.

## Annexe A

### Politique de confidentialité et de respect de la vie privée

Le respect de votre vie privée est essentiel. Cette politique vise à vous informer des pratiques adoptées l'**uttam** à l'égard des renseignements personnels.

#### Transmission de renseignements personnels

L'**uttam** s'engage à assurer la protection des renseignements personnels que vous lui confiez. Si vous communiquez volontairement de l'information personnelle ou autrement confidentielle à un membre de son personnel, au moyen d'un formulaire électronique ou d'un courriel par exemple, seule l'information requise pour permettre au personnel de répondre à votre demande est utilisée. Nous traitons la correspondance électronique avec les mêmes mesures de confidentialité que les autres documents écrits. Ainsi, ces renseignements sont communiqués à des tiers seulement avec votre consentement.

#### Données échangées automatiquement lors de l'accès au site

Lorsque vous accédez au site de l'**uttam**, votre ordinateur et notre serveur échangent automatiquement des données, sans que vous interveniez. Tous les serveurs Web échangent des données avec les ordinateurs qui accèdent à Internet. Cet échange avec notre serveur ne permet en aucun cas de vous identifier personnellement. Il permet notamment que le serveur vous transmette un fichier compatible avec l'équipement informatique que vous utilisez. Les données échangées sont les suivantes:

- Identification de votre fournisseur d'accès à Internet (nom de domaine);
- Adresse IP, l'adresse numérique qui permet d'identifier et de localiser votre ordinateur;
- Navigateur (Chrome, Firefox, Explorer, etc.) et système d'exploitation (Windows, Mac OS, Linux, etc.) que vous utilisez;
- Date et heure de votre accès au site;
- Pages Web que vous visitez;
- Adresse du site qui vous a dirigé vers celui de l'**uttam**, s'il y a lieu.

Cette information est utilisée sous forme anonyme à des fins statistiques, notamment pour comptabiliser le nombre de visiteurs et connaître les pages les plus fréquentées.

Ces données sont stockées au Canada.

#### L'utilisation de Google Analytics

L'**uttam** utilise également le service de Google Analytics, un outil d'analyse de site Internet fourni par Google. Vous devez savoir que Google Analytics utilise des témoins (cookies), tels que les témoins Google Analytics ou les témoins de Google Ads, ce qui permet à l'**uttam** de produire des rapports statistiques sur la navigation dans son site ou d'obtenir de

l'information de suivi d'annonces diffusées à l'occasion par l'**uttam** sur le réseau de recherche Google. L'**uttam** ne reçoit pas de ces témoins d'informations personnelles qui permettent de vous identifier.

Ainsi, lorsque vous visitez le site de l'**uttam**, Google Analytics peut notamment recueillir l'information suivante :

- les pages que vous visitez;
- la date et l'heure de votre visite;
- les liens sur lesquels vous cliquez;
- le système d'exploitation et d'autres données relatives à l'appareil utilisé;
- la langue de votre navigateur;
- le nom de domaine de votre fournisseur de services Internet;
- votre localisation géographique;
- votre adresse IP.

Veillez noter que cette cueillette d'information est inhérente à la navigation sur Internet, en ce qu'elle est déjà réalisée par le serveur de tout site Web visité (voir section précédente). Si vous ne souhaitez pas que cette information soit transmise à Google Analytics, vous pouvez télécharger et installer le module complémentaire pour la désactivation de Google Analytics dans votre navigateur.

Pour connaître les politiques de confidentialité de Google, vous pouvez consulter la page Règles de confidentialité et conditions d'utilisation de Google.

### **Utilisation de témoins**

L'**uttam** utilise les témoins mis en place par les produits Google (voir section précédente). Ces témoins n'accèdent pas aux fichiers ou aux autres données de votre ordinateur. Les témoins ne permettent pas de recueillir des renseignements confidentiels à votre sujet, ni de vous identifier personnellement.

### **Protocole de sécurité**

L'**uttam** utilise le protocole https (chiffrement sur 128 bits) sur son site. Ce protocole permet de chiffrer une communication Internet (TCP/IP) entre votre navigateur et son serveur Web afin d'en garantir la confidentialité. Tous les contenus échangés dans cette communication sont chiffrés à la transmission et déchiffrés à la réception. La communication étant bidirectionnelle, le navigateur et le serveur Web agissent tour à tour comme transmetteur et récepteur.

### **Paiements en ligne**

L'**uttam** ne stocke sur son serveur aucune donnée que vous fournissez pour faire un paiement en ligne sur son site. L'**uttam** utilise PayPal comme fournisseur de paiement en ligne. C'est PayPal qui recueille de façon sécurisée les informations nécessaires pour faire

le paiement, notamment l'information relative à votre carte de crédit et de débit. L'**uttam** n'a pas accès à vos informations financières, tel le numéro de votre carte de crédit. Pour connaître les politiques de confidentialité de PayPal, consultez son [Règlement sur le respect de la vie privée](#).

PayPal partage avec l'**uttam** certaines informations nécessaires au suivi de la transaction, soit votre nom, votre adresse, votre courriel, le montant du paiement et la raison du paiement. Ces données personnelles ne sont conservées par l'**uttam** que pour faire le suivi nécessaire, comme vous faire parvenir votre reçu ou votre carte de membre par exemple.

### **Transmission de vos coordonnées à des tiers**

L'**uttam** s'engage à ne pas divulguer ni commercialiser à des tiers les informations confidentielles que vous nous avez confiées, sauf aux termes d'une obligation légale (notamment par témoignage en justice, assignation à comparaître ou suivant une ordonnance d'un tribunal compétent).

### **Liens vers d'autres sites**

La présente politique de confidentialité ne s'applique pas aux sites tiers auxquels vous accédez à partir des hyperliens publiés sur le site de l'**uttam**, que ces sites aient leur propre politique relative à la confidentialité ou non.

Ces sites externes sont entièrement gérés par des tiers. L'**uttam** ne peut garantir la qualité ou le contenu général de ces sites. Nous n'effectuons aucune vérification quant à la sécurité ou aux règles de confidentialité des sites en question. Les liens proposés pour faciliter vos recherches n'engagent pas la responsabilité de l'**uttam**. Lorsque vous cliquez sur ces hyperliens, la politique de confidentialité ne s'applique plus.



## Annexe B

Liste non exhaustive sur les types de renseignements que l'**uttam** pourrait collecter, leur utilisation ou l'objectif visé, ainsi que les moyens par lesquels les renseignements sont recueillis. Cela comprend, sans s'y limiter, les éléments suivants. Notons que la plupart des renseignements personnels gérés par l'**uttam** sont des renseignements personnels principalement des membres de son personnel et des membres et non membres de l'**uttam** dont les dossiers sont traités par l'organisme, des candidats pour un emploi et de consultants.

Relation avec l' <b>uttam</b>	Type de renseignement personnel	Fin de la collecte/utilisation	Moyens de recueillir les renseignements
<b>Membres du personnel et candidats à l'emploi</b>	Nom Numéro Tél Adresse Adresse courriel NAS Date de naissance Renseignements bancaires	Gestion des communications avec les membres du personnel ou les candidats  Assurer le fonctionnement du système de paie	Par téléphone  Par courriel, par fax et directement en Format papier
<b>Consultants (avocats, médecins, autres professionnels de la santé et juridiques) et fournisseurs de services (<i>Journal de l'uttam</i>)</b>	Nom Numéro de téléphone cellulaire Courriel Adresse Renseignements bancaires	Gestion de la communication avec le consultant  Gestion des mandats  Paiement des factures	Par téléphone  Par courriel, fax et par l'entremise d'un document joint (Word – PDF)
<b>Travailleuses travailleurs accidentés/malades - Membres ou non</b>  <b>Organisations membres</b>	Nom Numéro Tél Adresse Courriel NAM NAS	Gérer les relations – moyen de communication Fournir le service d'aide et d'accompagnement aux victimes de LP Besoin de recueillir des informations pour constituer le dossier nécessaire à l'accompagnement Inscription comme membre Inscription aux événements organisés par des envois – postal et courriel Fournir des formations Participer à des sondages	Au moyen d'une base de données  Par téléphone, par courriel, par fax et – par l'entremise d'un document  Par envoi postal  Après de tiers – Cnésst/clinique médicale

## Annexe C

### Déclaration relative à la confidentialité

Je, soussigné(e) \_\_\_\_\_, déclare avoir lu la Politique de confidentialité de l'**uttam** et m'engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité survit à la fin de mon emploi ou de mon mandat auprès de l'**uttam**.

Signé à \_\_\_\_\_

le : \_\_\_\_\_

Nom en lettres moulées : \_\_\_\_\_

Signature : \_\_\_\_\_

## **Annexe D**

### **Incident de confidentialité : Plan de réponse**

#### **Démarche à effectuer**

Lorsqu'un membre du personnel de l'**uttam** ou une travailleuse ou travailleur constate un incident de confidentialité, il ou elle communique avec la personne responsable par le biais d'un formulaire de signalement prévu à cette fin (**Annexe G**).

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

La personne responsable évalue si l'incident présente un risque de préjudice sérieux, selon les paramètres présentés à l'**annexe F**.

Dans le cas où l'incident présente un risque de préjudice sérieux, la personne responsable, 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 personne responsable tient un registre de tous les incidents.

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

## **Annexe E**

### **Incident de confidentialité : contenu de la communication aux personnes concernées**

#### **Quand**

Tel qu'indiqué au point 8 a. 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 F

### Incident de confidentialité : questionnaire d'évaluation du « risque sérieux de préjudice grave »

#### Évaluer si l'incident présente un risque de préjudice sérieux

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.

**Annexe G**  
**Formulaire de signalement d'un incident**

Nom : _____
Adresse : _____ _____ _____
Numéro de téléphone : _____
Adresse courriel : _____
<b>1. 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</b>
_____ _____ _____ _____ _____ _____ _____ _____ _____ _____
<b>2. Une brève description des circonstances de l'incident</b>
_____ _____ _____ _____ _____ _____ _____ _____

<b>3. La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue)</b>
<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>
<b>4. La date ou la période à laquelle l'organisme s'est aperçu de l'incident.</b>
<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>
<b>5. Le nombre de personnes concernées par l'incident (une approximation si cette information n'est pas connue).</b>
<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>
<b>6. Autres commentaires</b>
<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>

**Annexe H**  
**Rapport d'incident de confidentialité et/ou de sécurité**

<b>Rapport d'incident de confidentialité et/ou sécurité</b>	#
<b>Date de l'incident</b>	
<b>Date de prise de connaissance de l'incident par l'organisme</b>	
<b>Circonstance de l'incident :</b> <ul style="list-style-type: none"> <li>• Renseignements personnels concernés par l'incident</li> <li>• La/les personne(s) concernée(s) par l'incident</li> </ul>	
<b>Est-ce qu'il y a un risque de préjudice sérieux?</b>  Par exemple : perte d'emploi, fraude bancaire, vol d'identité  <b>Si l'incident représente un préjudice sérieux, veuillez communiquer l'incident à la Commission d'accès à l'information du Québec</b>	<input type="checkbox"/> oui <input type="checkbox"/> non  <a href="https://www.cai.gouv.qc.ca/a-propos/nous-joindre/">https://www.cai.gouv.qc.ca/a-propos/nous-joindre/</a> 514-873-4196
<b>Mesure à prendre</b>	
<b>Date à laquelle la mesure a été appliquée</b>	
<b>Commentaires</b> _____ _____ _____ _____ _____ _____ _____ _____ _____	
<b>Signature de la personne responsable</b> _____ _____	
<b>Date :</b>	