



## **Politique sur la sécurité d'Assurance LAWPRO<sup>MD</sup>**

La politique sur la sécurité expose les mesures prises par Assurance LAWPRO pour assurer la protection et la confidentialité des renseignements personnels concernant ses clients et ses employés en conformité et en complémentarité avec le Code de la protection des renseignements personnels disponible à l'adresse [www.lawpro.ca/privacy](http://www.lawpro.ca/privacy).

Dans la présente politique, les mots « nous » et « nôtre » désignent Assurance LAWPRO<sup>MD</sup> qui inclut TitrePLUS<sup>MD</sup> et practicePRO<sup>MD</sup>. Les mots « vous » et « votre » désignent la personne cliente ou cliente éventuelle d'Assurance LAWPRO. Nos sites Internet peuvent avoir des liens avec d'autres sites conçus et tenus exclusivement par des tiers, non assujettis à la présente politique sur la sécurité. Veuillez prendre connaissance des politiques de sécurité adoptées par ces sites afin de déterminer leurs pratiques.

### ***Dispositifs de sécurité internes***

Seuls certains membres du personnel d'Assurance LAWPRO, tenus d'accéder aux renseignements qui vous concernent en raison de la nature de leurs fonctions, peuvent extraire des renseignements de votre dossier principal. Autrement dit, l'accès à des systèmes, des bases de données ou des applications spécifiques n'est autorisé que s'il est nécessaire et est réglementé en fonction du travail à effectuer. Cet accès est vérifié annuellement.

L'accès à tous les systèmes informatiques d'Assurance LAWPRO exige un code d'identification unique et un mot de passe propre à l'utilisateur. Le personnel concerné est responsable du code d'identification qui lui a été assigné. Les mots de passe ne doivent pas être échangés par les utilisateurs et ils sont modifiés régulièrement.

Lorsqu'un membre du personnel change radicalement de fonctions après une mutation dans un autre service par exemple, ses autorisations d'accès sont revues et modifiées. Si, dans son nouveau service, la personne n'a plus besoin d'accéder à certains renseignements pour accomplir son travail, cet accès est supprimé. Les comptes d'utilisateur sont désactivés à la fin de l'emploi ou du contrat.

Les systèmes informatiques d'Assurance LAWPRO possèdent aussi des fonctions de vérification intégrées qui repèrent l'accès et la modification des données. Ces listes de contrôle peuvent servir à détecter les tentatives non autorisées d'accès à des renseignements. Le stockage de renseignements personnels sur les disques durs des ordinateurs de bureau et des ordinateurs portatifs n'est habituellement pas autorisé. Tous les fichiers informatiques contenant des renseignements personnels sont centralisés dans nos serveurs sécurisés et des copies de sauvegarde sont effectuées pendant la nuit. L'accès direct aux bases de données centrales n'est pas permis. Des applications logicielles spéciales sont utilisées pour contrôler l'accès et maintenir la sécurité et l'exactitude des données enregistrées dans les systèmes.

Notre personnel sait que les renseignements personnels (les données enregistrées dans les documents imprimés, ou dans les médias numériques tels que cassettes, CD/DVD ou USB) ne doivent pas être laissés à la vue ou accessibles aux personnes non autorisées pouvant venir de l'extérieur. Les employés doivent sortir de toutes les applications et fermer leur ordinateur de bureau à la fin de la journée. Chaque fois qu'ils s'absentent de leur bureau

pendant une période assez longue, ils doivent aussi fermer les applications qui contiennent des renseignements personnels.

L'accès aux dossiers sur papier est réglementé par un système de signature de registre. Un service d'élimination et de déchiquetage sécuritaire est par ailleurs utilisé pour garantir la sécurité des documents imprimés et des dossiers jetés au rebut.

### ***Dispositifs extérieurs de contrôle de l'accès***

Afin de protéger vos renseignements personnels contre toute consultation extérieure non autorisée, l'accès aux locaux d'Assurance LAWPRO est réglementé par le personnel de la réception et par l'inspection de cartes de sécurité. L'accès à distance aux systèmes informatiques d'Assurance LAWPRO par le personnel est limité par l'emploi de codes d'identification et de mots de passe et n'est autorisé qu'en cas de nécessité. Les procédures de sécurité d'Assurance LAWPRO sont vérifiées par deux firmes externes pour s'assurer d'être conforme aux normes de sécurité applicable et pour adhérer aux meilleures pratiques. L'entrée dans les sites Internet d'Assurance LAWPRO est protégée par un coupe-feu et par un logiciel de routage, ainsi que par des contrôles d'accès installés dans les serveurs des différents sites. Les serveurs les plus importants sont surveillés par un logiciel de détection d'intrusion qui signale l'accès non autorisé ou les modifications apportées au système.

### ***Sécurité du réseau et des serveurs***

Le réseau et les serveurs d'Assurance LAWPRO sont placés en sécurité dans une salle de serveurs climatisée à accès limité. L'accès au matériel d'Assurance LAWPRO est réservé aux membres désignés du service des systèmes d'information d'Assurance LAWPRO et aux techniciens des fournisseurs expressément autorisés par Assurance LAWPRO. Ces techniciens sont supervisés par le personnel d'Assurance LAWPRO et/ou sont liés par les conditions d'un accord de confidentialité.

La stabilité des systèmes est assurée par un réseau redondant d'alimentation sans coupure et par les caractéristiques de « reprise » redondantes des composants intégrés aux serveurs. Les critères du coupe-feu sont mises à jour régulièrement, les définitions des virus sont mis à jour plusieurs fois par jour, et un logiciel de détection des virus et de filtrage du web sont installés sur le réseau et dans tous les ordinateurs de bureau.

Les données transmises sur le réseau interne (ou Intranet) d'Assurance LAWPRO, de même que les communications courantes envoyées par courrier électronique à l'extérieur du réseau ne sont pas chiffrées<sup>1</sup>. Le personnel est toutefois invité à tenir compte de la confidentialité des documents avant de les transmettre par courrier électronique à l'extérieur du réseau. Des sauvegardes sont exécutées la nuit sur tous les systèmes et les bandes de sauvegarde sont entreposées en sécurité dans une installation extérieure en prévision d'une reprise après sinistre. Seuls, le personnel autorisé des systèmes d'information d'Assurance LAWPRO et les employés de l'installation extérieure ont accès aux données sauvegardées. Des essais de reprise après sinistre sont exécutés à intervalles réguliers.

### ***Sécurité sur Internet***

#### **1. Ce que nous savons de nos visiteurs**

Quand vous consultez les pages d'information non sécurisées de nos sites Internet, seuls les renseignements suivants sont repérés :

- le nom de domaine par lequel vous accédez à Internet (« sympatico.ca » ou « aol.com » par exemple);
- la date et l'heure d'accès au site;

- les pages et les fichiers que vous avez consultés sur le site; et
- l'adresse du site par lequel vous avez rejoint le site d'Assurance LAWPRO (page « Liens » d'un autre site par exemple).

Sauf dans les cas mentionnés plus loin, cette information est seulement stockée ou examinée de façon globale pour surveiller la structure du trafic et le volume d'utilisation. Nous n'examinons pas l'utilisation que les personnes font de nos sites Internet.

Assurance LAWPRO utilise cependant des méthodes conformes aux normes de l'industrie pour déceler les tentatives non autorisées d'accéder aux sites Web et de modifier ou de perturber leurs données. L'accès non autorisé est strictement interdit et peut être signalé aux autorités compétentes et aux fournisseurs de services Internet.

## 2. Protocole SSL et cryptage

Afin de mieux protéger votre sécurité quand vous communiquez avec Assurance LAWPRO par l'entremise de ses divers sites Internet, nous vous recommandons d'utiliser un navigateur qui permet un cryptage de 128 bits, une forme de cryptage sécurisé qui procure une protection adéquate lors de la transmission de données confidentielles par Internet.

Pour vérifier que vous avez bien établi une connexion SSL (Secure Socket Layer), assurez-vous que l'adresse du site Internet commence par « https:// », et non par la norme « http:// ». Pour en savoir plus au sujet de votre navigateur préféré et comment il soutient les connexions SSL et l'encryption, consultez l'internet. Pour Internet Explorer, visitez [www.microsoft.com/ie](http://www.microsoft.com/ie); pour Firefox, [mozilla.com/firefox](http://mozilla.com/firefox); pour Chrome [google.com/chrome](http://google.com/chrome); et pour Safari, visitez [apple.com/safari](http://apple.com/safari). Si vous ne disposez pas d'un navigateur permettant le cryptage, demandez des conseils à l'administrateur de votre système informatique.

## 3. Ouverture de session

Par mesure de protection, nous vous demandons d'inscrire votre numéro de membre du Barreau (ou le numéro du cabinet) et votre mot de passe afin d'accéder aux secteurs sécurisés de nos sites Internet. Nous vous recommandons d'utiliser une combinaison de lettres et de chiffres pour composer ce mot de passe. Évitez d'employer des mots qui peuvent facilement vous être associés et modifiez régulièrement le mot de passe.

Ne dévoilez jamais votre mot de passe, car il aide à vérifier votre identité avant d'autoriser l'accès à certains renseignements confidentiels comme votre police d'assurance ou votre adresse. Si vous n'êtes pas en mesure de fournir le mot de passe exact, l'accès au système ne vous est pas accordé. Les tentatives d'accès avec un mot de passe incorrect sont dépistées par le système; pour des raisons de sécurité, l'accès sera barré dans l'éventualité où plusieurs tentatives successives d'accès au système seront essayées avec un mot de passe incorrect. Cela dit, si un ordinateur est commun à plusieurs personnes, nous recommandons de régler le navigateur de façon qu'il **ne puisse pas** sauvegarder les mots de passe aux fins d'utilisation ultérieure. Cette option est disponible avec tous navigateurs modernes.. Au besoin, nous offrons plusieurs options commodes en cas d'oubli du mot de passe, notamment un dispositif d'aide-mémoire et de validation en ligne ou un service de rappel par notre Service à la clientèle.

Quand vous réussissez à ouvrir une session, votre navigateur web établit une connexion SSL sécurisée entre l'ordinateur et notre site Internet. Lorsque vous sortez de la partie sécurisée du site, le navigateur web vous en avise et vous informe que vous retournez à une section accessible à tous.

#### **4. Fermeture automatique**

Pour mieux empêcher l'accès non autorisé aux dossiers, nos systèmes se ferment automatiquement si une session sécurisée en ligne reste inactive pendant plus d'une heure. Si la session se termine, vous devez à nouveau fournir le numéro de membre ou de cabinet et le mot de passe avant de pouvoir reprendre vos activités en ligne. Comme la plupart des opérations effectuées sur les sites Internet d'Assurance LAWPRO ne prennent que quelques minutes, cette situation se produit rarement.

#### **5. Mémoire cache**

Dans un navigateur web, la mémoire « cache » contient les copies des pages visionnées et l'information enregistrée pendant la session de navigation. Elle sert aussi à restituer les pages consultées antérieurement quand on appuie sur le bouton « Précédente ».

Pour que vos opérations dans les sites web d'Assurance LAWPRO se déroulent bien, la mémoire cache du navigateur Internet **doit** être activée avant l'utilisation du site. Si toutefois vous désirez protéger la confidentialité de vos renseignements personnels, vous pouvez choisir d'effacer la mémoire cache du navigateur après avoir terminé la session de navigation.

Des renseignements additionnels au sujet de l'utilisation de votre navigateur web et comment effacer la mémoire cache sont disponibles en ligne. Pour Internet Explorer, visitez [www.microsoft.com/ie](http://www.microsoft.com/ie); pour Firefox, [mozilla.com/firefox](http://mozilla.com/firefox); pour Chrome [google.com/chrome](http://google.com/chrome); et pour Safari, visitez [apple.com/safari](http://apple.com/safari).

#### **6. Témoins**

Pour permettre à nos sites Internet de confirmer à plusieurs reprises votre identité au cours des opérations exécutées par voie électronique, nous nous servons de « témoins » (cookies) qui sont de petits fichiers-textes envoyés par un site Internet à votre navigateur et stockés dans votre ordinateur. Il existe deux types de témoins : les témoins « temporaires » et les témoins « persistants ». Leur principale différence est que le témoin « temporaire » disparaît quand la session de navigation est terminée (c'est-à-dire quand le navigateur est fermé ou laissé au repos pendant une période prolongée), alors que le témoin « persistant » peut rester dans l'ordinateur même après la fin de la session de navigation.

Il importe de se rappeler les points suivants au sujet des témoins :

- ils ne peuvent être lus que par le site Internet qui les met en place;
- ils ne peuvent pas être utilisés pour repérer les visites à d'autres sites Internet; et
- ils ne peuvent pas apporter de codes ou de virus destructeurs;
- ils ne peuvent pas aller fouiller dans l'ordinateur pour trouver de l'information ou télécharger des données.

Comme la plupart des entreprises en ligne, les sites relevant d'Assurance LAWPRO emploient des témoins pour faciliter et sécuriser les opérations exécutées sur Internet. Les sites d'Assurance LAWPRO n'utilisent pas de témoins persistants, mais seulement des témoins temporaires servant pendant une seule session. Aux fins de sécurité, les témoins temporaires doivent être activés lorsqu'on utilise la section sécurisée des sites.

Des renseignements sur votre navigateur et sur sa méthode de gestion des témoins sont disponibles en ligne. Pour Internet Explorer, visitez [www.microsoft.com/ie](http://www.microsoft.com/ie); pour Firefox, [mozilla.com/firefox](http://mozilla.com/firefox); pour Chrome [google.com/chrome](http://google.com/chrome); et pour Safari, visitez [apple.com/safari](http://apple.com/safari).

Pour **Microsoft Internet Explorer 5.x, 6.x.** ou **7.x**, visitez

Microsoft à l'adresse <http://www.microsoft.com/info/cookies.htm>

Pour **Mozilla version 2.x Firefox**, visitez Mozilla à l'adresse <http://support.mozilla.com/en-US/kb/Cookies>.

Pour Netscape Navigator/Communicator version 6.x, 7.x ou 8.x, visitez Netscape à l'adresse [http://wp.netscape.com/legal\\_notices/cookies.html](http://wp.netscape.com/legal_notices/cookies.html).

### ***Lignes directrices pour la destruction de l'information personnelle***

Assurance LAWPRO reconnaît qu'afin d'empêcher des tiers non autorisés d'accéder à vos renseignements personnels, il est important d'user de précautions lors de l'élimination et de la destruction des renseignements personnels. Pour les besoins de la présente section de la politique, « destruction » (ou « détruire ») signifie la prise de mesures visant à faire en sorte que les renseignements personnels contenus dans les supports de stockage (y compris le papier et les médias audio et vidéo) ne puissent être utilisés ou reconstitués plus tard, une fois que la décision a été prise de ne pas les conserver.

Le chef du service de l'information conservera un dossier de destruction documentant la destruction en vrac des dossiers contenant des renseignements personnels. Toute destruction en vrac de dossiers requiert l'autorisation du Chef de service responsable des dossiers et du Président-directeur général (ou des délégués de l'une ou de l'autre de ces personnes).

**Dossiers sur support papier** : Déchiquetés ou renseignements personnels édités.

**Documents électroniques** : Sous la surveillance du service des systèmes d'information, destruction physique du médium, de l'application ou de l'utilitaire approprié de manière à ce que les données ne puissent être reconstruites.

**Bandes vidéo / sonores** : Destruction physique, à moins de réécriture sur les lieux par le personnel autorisé.

### ***Conclusions***

Tout changement apporté à notre politique sur la sécurité sera reconnu en temps opportun. Assurance LAWPRO peut ajouter, modifier ou retirer des parties de cette politique quand elle le juge pertinent. Pour connaître la date de la dernière mise à jour, il suffit de vérifier la date qui se trouve au bas de la version de la Politique disponible au <http://www.lawpro.ca/security>.

<sup>1</sup> On entend par « cryptage » un processus de brouillage ou de chiffrement de l'information en vue de son passage dans Internet. L'information peut par exemple être brouillée dans votre ordinateur personnel, puis débrouillée (ou « décryptée ») quand elle parvient à Assurance LAWPRO. Cela empêche qu'elle soit lue ou interceptée pendant sa transmission.

<sup>2</sup> Veuillez noter que tous les sites Internet appartenant à des tiers mentionnés dans la présente politique sur la sécurité ne sont pas approuvés par Assurance LAWPRO et que celle-ci ne peut être tenue responsable de leur contenu.

<sup>MC MD</sup> Assurance LAWPRO, TitrePLUS, practicePRO et le logo d'Assurance LAWPRO sont des marques de commerce déposées de Lawyers' Professional Indemnity Company.

*Dernière mise à jour effectuée le 3 juin 2013.*