

ÊTRE CONFORME DÈS LE DÉPART ET LE DEMEURER



MISE EN PLACE DE VOTRE PRATIQUE

Les documents ci-dessous ne sont pas destinés aux clients et sont requis afin de maintenir une pratique conforme.

- ✓ Politique et procédures relatives aux incidents de confidentialité
- ✓ Politique et procédures de lutte contre le blanchiment d'argent et le financement des activités terroristes (BA/FT)
- ✓ Dossier de plaintes
- ✓ Unités de formation continue (UFC)
- ✓ Assurance responsabilité professionnelle (erreurs et omissions)
- ✓ Traitement équitable des consommateurs (TEC)
- ✓ Code de conduite de Gryphin Advantage

À CONSIDÉRER

Entente de continuité des affaires

EXIGENCES À L'OUVERTURE D'UN NOUVEAU DOSSIER CLIENT

VENTE D'ASSURANCE VIE / MALADIES GRAVES / INVALIDITÉ

Tous les documents ci-dessous sont destinés au client et doivent être remplis et versés au dossier client chaque fois qu'un NOUVEAU dossier est ouvert.

- ✓ Document de divulgation du conseiller
- ✓ Analyse des besoins financiers
- ✓ Illustration
- ✓ Lettre expliquant les motifs de la recommandation

À CONSIDÉRER

*Fiche de collecte de renseignements
Types d'assurance
Préavis de remplacement d'un contrat
d'assurance de personnes (s'il y a lieu)*

VENTE DE FONDS DISTINCTS / CPG / RENTE

- ✓ Document de divulgation du conseiller
- ✓ Document d'information sur les frais des fonds distincts
- ✓ Notice explicative
- ✓ Aperçu du fonds
- ✓ Copie de la proposition de placement
- ✓ Lettre expliquant les motifs de la recommandation

À CONSIDÉRER

*Fiche de collecte de renseignements
Questionnaire
Documents relatifs au prêt à effet de levier*

DOCUMENTS COMPLÉMENTAIRES AU DOSSIER CLIENT

Tous les documents ci-dessous sont destinés au client et n'ont à être remplis qu'une seule fois par dossier client.

- ✓ Consentement relatif aux renseignements personnels
- ✓ Consentement – Loi canadienne anti-pourriel (LCAP)
- ✓ Lettre d'engagement
- ✓ Personne de confiance (PC)

EXIGENCES EN MATIÈRE DE CYBERSÉCURITÉ

Toutes les mesures de cybersécurité ci-dessous sont obligatoires afin de protéger les renseignements des clients et de maintenir la conformité réglementaire. Ces exigences doivent être mises en œuvre, documentées et revues régulièrement.

AUTHENTIFICATION MULTIFACTEUR (MFA)

- ▶ Activer l'authentification multifacteur pour tous les comptes de courriel professionnels
- ▶ Exiger l'authentification multifacteur pour tous les systèmes de gestion des clients
- ▶ Mettre en œuvre l'authentification multifacteur pour les outils d'accès à distance
- ▶ Documenter l'inscription à l'authentification multifacteur pour tous les membres du personnel
- ▶ Vérifier régulièrement l'état de l'authentification multifacteur

POLITIQUES ET PROCÉDURES

- ▶ Politique de sécurité de l'information
- ▶ Plan d'intervention en cas d'incident
- ▶ Procédure de notification en cas d'incident de confidentialité
- ▶ Directives de sécurité pour le télétravail
- ▶ Politique de gestion des mots de passe
- ▶ Révision et mise à jour annuelles des politiques

FORMATION EN CYBERSÉCURITÉ

- ▶ Formation annuelle de sensibilisation à la cybersécurité pour tout le personnel
- ▶ Simulations d'hameçonnage (trimestrielles)
- ▶ Pratiques exemplaires de traitement des renseignements
- ▶ Sensibilisation à l'ingénierie sociale
- ▶ Documentation de l'achèvement des formations
- ▶ Module de cybersécurité à l'intégration des nouveaux employés

CHIFFREMENT DES DONNÉES

- ▶ *Chiffrer tous les appareils contenant des renseignements sur les clients*
- ▶ *Utiliser le chiffrement des courriels pour les communications contenant des renseignements sensibles*
- ▶ *Utiliser des solutions de sauvegarde chiffrées*
- ▶ *Utiliser des protocoles sécurisés de transfert de fichiers*
- ▶ *Mettre en place des procédures de gestion des clés de chiffrement*
- ▶ *Effectuer régulièrement des vérifications et des audits du chiffrement*

UTILISATION DE L'IA ET POLITIQUE

- ▶ *Politique d'utilisation acceptable des outils d'intelligence artificielle*
- ▶ *Protection des renseignements des clients dans les systèmes d'IA*
- ▶ *Processus d'approbation et d'évaluation des outils d'IA*
- ▶ *Exigences de divulgation relatives à l'utilisation de l'IA*
- ▶ *Révision régulière des résultats produits par l'IA afin d'en vérifier l'exactitude*
- ▶ *Formation du personnel sur l'utilisation responsable de l'IA*