ORDRE DES COMPTABLES PROFESSIONNELS AGRÉÉS DU QUÉBEC

5, Place Ville Marie, bureau 800, Montréal (Québec) H3B 2G2
T. 514 288-3256 1 800 363-4688 Téléc. 514 843-8375
www.cpaquebec.ca

Politique de sécurité de l'information

Politique de sécurité de l'information			**Nos. Résolution : 302/717**
Adoption par le Conseil d'administration	2014/05/29	Entrée en vigueur	2014/05/29
Dates de révision	2018/06/15 2022/05/25 2023/11/30		
Responsables de la mise à jour de la politique	Directeur, Sécurité de l'information Première vice-présidente et chef des finances et des opérations		
Politiques et lignes directrices liées	Ligne directrice relative aux rôles et responsabilités découlant de la Politique de sécurité de l'information Ligne directrice relative à la gestion des incidents et des problèmes Ligne directrice relative à l'utilisation de services infonuagiques Ligne directrice relative à la gestion des accès Politique d'approvisionnement		
Procédure en découlant	Guide relatif à la politique d'approvisionnement		

Table des matières

Politique de sécurité de l'information

Contexte

01. L'Ordre des comptables professionnels agréés du Québec (Ordre) utilise des informations de toute nature afin d'assurer la protection du public qui est au cœur de ses opérations. De plus, il a pour but d'être reconnu par ses membres pour la qualité de sa gestion et l'efficacité de son fonctionnement, en lien avec la portion de sa mission visant à accroître la fiabilité de l'information.

Objectifs

02. C'est dans cette perspective que l'organisation s'est dotée d'une politique de sécurité de l'information (Politique) qui exprime la prise de position de l'Ordre concernant les mesures de sécurité considérées comme essentielles afin d'assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité de ses actifs informationnels.

03. La Politique regroupe les énoncés de principes généraux et les rôles et responsabilités des intervenants en sécurité de l'organisation[1]. Des lignes directrices sont toutefois requises afin de soutenir, développer et préciser cette Politique. Ces dernières visent à présenter de façon concrète les mesures de sécurité de l'information que les employés doivent comprendre et respecter dans leurs activités professionnelles.

Champ d'application

04. La Politique s'applique à tous les utilisateurs des actifs informationnels de l'Ordre, qu'ils soient employés, dirigeants, administrateurs, consultants, fournisseurs, clients, partenaires d'affaires, ou membres des comités, à toute entité associée à l'Ordre ou qui en est le mandataire.

05. Fondation des comptables professionnels agréés du Québec (la Fondation)

Bien que la Fondation soit une entité juridique à part entière, cette politique s'applique néanmoins à cette dernière du fait qu'elle utilise quotidiennement les locaux, de même que les ressources humaines et matérielles de l'Ordre, notamment les employés attitrés à la gestion et à l'administration de la Fondation, ainsi que le parc et les réseaux informatiques de l'Ordre.

06. Les actifs visés sont ceux appartenant à l'Ordre et exploités par lui, ceux lui appartenant et exploités ou détenus par un fournisseur ou un tiers, et ceux appartenant à un fournisseur de services ou un tiers et exploités par l'Ordre au profit du fournisseur.

---

[1] Le masculin est utilisé sans discrimination dans le seul but d'alléger le texte.

07. Toutes les activités impliquant la manipulation ou l'utilisation des actifs informationnels sont touchées par cette Politique.

Lois et règlements

08. La présente Politique doit être appliquée et interprétée en fonction des lois, règlements et normes énumérés en annexe B.

Principes généraux

Norme

09. Les principes de base de la présente Politique s'inspirent des référentiels de CIS et NIST. Ces normes internationales offrent une vue d'ensemble des systèmes de gestion de la sécurité de l'information (SGSI) et édictent des pratiques reconnues afin notamment d'établir ce SGSI.

Protection des actifs informationnels

10. Les actifs informationnels sont assignés à un propriétaire, catégorisés et inventoriés. Cet inventaire doit être automatisé lorsque cela est techniquement possible.

11. Ces actifs sont classifiés et protégés selon leur degré de sensibilité et leur cycle de vie, afin d'assurer leur disponibilité, intégrité, confidentialité et traçabilité.

12. Des processus doivent être mis en œuvre pour identifier le matériel et/ou les logiciels non autorisés et avertir le personnel approprié lorsqu'ils sont découverts.

13. Le choix des mesures de protection des actifs informationnels s'appuie sur une évaluation périodique des risques et a pour objet d'atténuer et maintenir le niveau de risque acceptable pour l'Ordre.

14. Tous les actifs informationnels (matériels et logiciels) doivent être correctement configurés et renforcés par les mesures de sécurité et les protections requises.

15. Des tests d'intrusion ou des balayages de vulnérabilité sur tout actif informationnel doivent avoir lieu périodiquement ou selon les exigences des lois et règlements applicables, et être coordonnés par la direction de sécurité de l'information afin de déterminer les risques et/ou les vulnérabilités potentiels.

Gestion des comptes et contrôle des accès

16. Toute information considérée confidentielle ou sensible doit être protégée contre tout accès ou utilisation non autorisés ou illicites. L'accès aux actifs doit se faire en fonction de ce qui est requis pour l'exécution d'une tâche et selon les rôles et responsabilités d'un utilisateur.

17. Tous les utilisateurs doivent avoir une identité unique vérifiée à l'aide d'un identifiant et d'un mot de passe secret, ou par d'autres moyens offrant une sécurité égale ou supérieure, avant d'être autorisés à utiliser les actifs informationnels de l'Ordre.

18. Les accès aux actifs informationnels doivent être revus à intervalles réguliers. L'examen doit inclure la suppression dans les plus brefs délais des accès qui ne sont plus nécessaires.

19. Des mécanismes d'authentification forte (par exemple, une authentification à deux facteurs) doivent être mis en place pour l'accès à distance aux actifs informationnels.

Normes associées : Norme gestion mots de passe, Norme sur la gestion des accès à distance

Gestion des changements

20. Tous les changements impliquant des actifs informationnels doivent suivre le processus de gestion des changements, à savoir la planification, l'évaluation, la révision, l'approbation et la documentation, afin de minimiser l'impact négatif sur les services informatiques, les utilisateurs et nos membres.

Gestion des vulnérabilités

21. Tous les actifs informationnels doivent être à jour avec les derniers correctifs et mises à jour de sécurité selon les normes définies à l'Ordre. Les correctifs et/ou les mises à jour de sécurité doivent être évalués en fonction de leur criticité et appliqués à intervalles réguliers, mais les mises à jour critiques doivent être appliquées dès que possible.
22. La mise en œuvre des correctifs et des mises à jour de sécurité doit suivre le processus établi de gestion des changements et l'approbation requise.

Gestion des fournisseurs de services

23. L'Ordre doit établir et maintenir un inventaire des fournisseurs de services connus qui conservent des données sensibles ou qui sont responsables des plateformes ou des processus informatiques critiques. Cet inventaire doit être mis à jour annuellement.
24. Les fournisseurs doivent être classifiés en tenant compte de la nature des services fournis, du niveau d'accès aux données sensibles et de leur impact sur la sécurité de l'information.

Journalisation et surveillance de la sécurité

25. Pour s'assurer que des mesures de protection appropriées sont en place et efficaces, l'Ordre se réserve le droit d'enregistrer et de surveiller l'accès et les événements afin de détecter, de signaler et de se protéger contre:
26. La violation des politiques et des normes de sécurité de l'information ;
27. L'utilisation abusive des services, des systèmes ou des informations, comme l'accès non autorisé ;
28. La perte d'informations confidentielles ;
29. La perte de disponibilité des services due à une violation de la sécurité ;
30. Les journaux d'événements et d'audits liés à la sécurité doivent être examinés et analysés en temps raisonnable afin d'identifier toute activité suspecte, inappropriée, inhabituelle ou malveillante.

Sensibilisation et formation

31. Une formation sur la sensibilisation à la sécurité informationnelle doit être fournie à tous les employés et consultants. Ainsi, il importe que le personnel soit sensibilisé aux menaces et aux conséquences d'une atteinte à la sécurité, qu'il comprenne son rôle et ses obligations ainsi que les procédures de sécurité existantes afin que chacun puisse développer ses réflexes et reconnaître les incidents ou les risques potentiels et ainsi travailler dans un environnement sécuritaire.
32. Tous les employés et les consultants doivent suivre la formation de sensibilisation à la cybersécurité afin de comprendre leurs responsabilités en matière de sécurité de l'information.

Responsabilité des intervenants

33. La protection de l'information détenue par l'Ordre s'appuie sur l'engagement continu de l'ensemble des intervenants. Chacun a l'obligation de protéger l'information et le matériel mis à sa disposition. Les intervenants ont des responsabilités spécifiques en matière de sécurité et sont redevables de leurs actions. Ainsi, les rôles et responsabilités des intervenants sont clairement définis à tous les niveaux de l'organisation et dans tous les processus d'affaires de l'Ordre.

Traitement et signalement des incidents

34. Tout utilisateur a l'obligation de signaler sans tarder aux autorités compétentes qui se doivent d'être définies dans un processus de gestion des incidents, tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité tel que le vol, l'intrusion dans un réseau ou système, les dommages délibérés, l'utilisation abusive, la fraude, etc.

35. Tous les incidents de cybersécurité seront gérés conformément au plan de réponse aux incidents de sécurité informatique de l'Ordre.

Continuité des affaires

36. L'Ordre doit disposer de mesures d'urgence issues de son plan de continuité des affaires, consignées par écrit, éprouvées et mises à jour en vue d'assurer la remise (dans un délai raisonnable) des opérations jugées essentielles en cas de sinistre majeur.

37. Les procédures de sauvegarde et de restauration doivent être maintenues et testées pour vérifier l'intégrité de la sauvegarde et valider les étapes de restauration.

38. Des tests de restauration doivent être effectués avec les données de sauvegarde de production au moins une fois par an pour vérifier que les données sauvegardées peuvent être récupérées.

39. Les sauvegardes contenant des données sensibles doivent être chiffrées de manière appropriée.

Droit de propriété intellectuelle

40. Les utilisateurs doivent se conformer aux exigences légales portant sur l'utilisation de produits à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle.

Droit de regard

41. L'Ordre a un droit de regard et d'intervention, exercé conformément aux lois et règlements énumérés en annexe B, sur l'utilisation de ses actifs informationnels et des moyens et des lieux qui permettent d'y accéder. Ainsi, l'usage permis doit être clairement défini et diffusé auprès des utilisateurs.

Mesures d'exception

42. Sans l'autorisation écrite du président et chef de la direction, aucune dérogation à la présente Politique et à ses documents afférents n'est permise.

Rôles et responsabilités

43. Les responsabilités sont définies pour les rôles stratégiques ou d'importance.

Conseil d'administration (Conseil)

44. Le Conseil approuve la Politique ainsi que ses mises à jour. De plus, il approuve le profil global de risque lié à la sécurité de l'information.

Comité d'audit

45. Le comité d'audit est mandaté par le Conseil afin de surveiller l'application de cette politique.

Présidente ou président et chef de la direction

46. Le président et chef de la direction est le premier responsable de la sécurité de l'information.

Première vice-présidente ou premier vice-président et chef des finances et des opérations

47. Le premier vice-président assure la prise en compte de la sécurité de l'information au sein des opérations de l'Ordre permettant l'application de la Politique.

Secrétaire et vice-présidente ou vice-président, Affaires juridiques et gouvernementales

48. Le secrétaire et vice-président, Affaires juridiques s'assure que l'Ordre répond aux exigences légales, réglementaires et contractuelles applicables à cette Politique.

Vice-présidente ou vice-président, Technologies et systèmes d'information

49. Le vice-président, Technologies et systèmes d'information est responsable fournir les ressources nécessaires pour maintenir un niveau de contrôle de la sécurité des informations conforme à la présente politique. Il rend compte au comité de direction et au comité d'audit.

Directeur ou directrice, Sécurité de l'information

50. Le directeur, Sécurité de l'information est responsable de l'élaboration de la politique, des lignes directrices et des processus permettant la mise en place du système de gestion de la sécurité de l'information. Il rend compte au comité de direction et au comité d'audit.

Propriétaire d'actifs informationnels (détenteur)

51. Le détenteur assure la gestion de la sécurité de son actif informationnel, en veillant à ce que les mesures de sécurité appropriées soient élaborées, mises en place et appliquées.

Utilisatrice ou utilisateur

52. Les utilisateurs des actifs informationnels prennent connaissance et adhèrent à la Politique, ainsi qu'à toutes les directives, lignes directrices, autres politiques, normes ou procédures édictées par l'organisation. De plus, ils utilisent les actifs informationnels en se limitant aux fins pour lesquels ils sont destinés et à l'intérieur des accès qui lui sont accordés.

Dispositions finales

Sanctions

53. Lorsqu'un utilisateur contrevient à la présente Politique et aux directives, lignes directrices, autres politiques, normes ou procédures édictées par l'organisation, il s'expose à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges d'accès, la réprimande, la suspension, le congédiement ou autre.

Révision

54. La présente Politique doit être révisée annuellement ou lors de changements significatifs qui pourraient l'affecter.

Date d'entrée en vigueur

55. La présente Politique entre en vigueur à sa date d'approbation par le Conseil d'administration.

Annexe A

Glossaire

56. **Actif informationnel** : Pour les fins de cette Politique, est incluse l'information elle-même, peu importe son support (papier ou technologique) ainsi que les systèmes utilisés pour son traitement, son utilisation, son stockage, sa conservation et sa communication interne et externe.
57. **Cycle de vie de l'information** : Ensemble des étapes que franchit une information et qui va de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation de l'Ordre.
58. **Confidentialité :** Propriété d'une information de n'être accessible qu'aux personnes désignées et autorisées.
59. **Degré de sensibilité de l'information :** Varie selon les informations, sera jugée sensible tout renseignement considéré comme confidentiel, stratégique, essentiel, critique, indispensable ou vital pour les opérations de l'Ordre, et dont la divulgation, l'altération, la perte ou la destruction est susceptible de porter préjudice à l'organisation, à son personnel ou à sa clientèle, ses partenaires et ses fournisseurs.
60. **Disponibilité :** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
61. **Intégrité :** Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.
62. **Traçabilité :** Propriété d'un document associé à la conservation de tout ce qui le compose, soit sa provenance, de tout changement de support (informatique, papier, audio, visuel, numérique) et la piste des étapes du ou des processus qui ont créé ce document.
63. **Risques liés à la sécurité de l'information :** Tout événement lors du traitement, l'utilisation ou l'entreposage comportant un degré d'incertitude, qui pourrait porter atteinte à la confidentialité, l'intégrité, la disponibilité ou la traçabilité de l'information et causer un préjudice à l'Ordre.
64. **Système d'information** : Service au sein de l'organisation auquel on attribue en général la responsabilité première de gérer le matériel informatique, les logiciels et les données.

Annexe B

Lois et règlements

65. La présente politique doit être appliquée et interprétée en fonction des lois, des règlements, des directives et des normes applicables, notamment :

66. Le *Code civil du Québec* (L.Q., 1991, c. 64), notamment les articles 36 et 37, qui portent respectivement sur le respect de la vie privée de même que la cueillette, l'utilisation et la communication de renseignements personnels;

67. Le *Code des professions* (L.R.Q., c. C-26), notamment l'article 60.4 portant sur le secret professionnel et les articles 108.1 à 108.11 inclusivement portant sur l'accès aux documents et la protection des renseignements personnels;

68. La *Loi sur les comptables professionnels agréés* (L.R.Q., c. C-48.1) incluant tous les règlements s'y rapportant dont le *Code de déontologie des comptables professionnels agréés* (L.R.Q., C-48.1, r. 6) et ses articles 48, 48.1 et 49 portant sur le secret professionnel et le *Règlement sur l'assurance de la responsabilité professionnelle des membres de l'Ordre des comptables professionnels agréés du Québec* prévoyant de l'échange d'information avec « l'ACPAI », gestionnaire du régime d'assurance collectif d'assurance responsabilité professionnelle;

69. La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) à l'exception des articles 8, 28, 29, 32, 37 à 39, 57, 76 et 86.1 de cette loi qui s'applique aux documents détenus par un ordre professionnel dans le cadre du contrôle de l'exercice de la profession comme à ceux détenus par un organisme public;

70. La *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) qui s'applique aux renseignements personnels détenus par un ordre professionnel, autres que ceux détenus dans le cadre du contrôle de l'exercice de la profession, comme à ceux détenus par une personne qui exploite une entreprise;

71. La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ 2021, c 25);

72. La Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, c. 5);

73. La Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);

74. Le *Code criminel du Canada* (L.R.C., 1985, c. C-46), notamment les articles 342.1, 366 et 430, qui portent respectivement sur l'interception frauduleuse d'informations, la falsification des documents et les méfaits;

75. La *Loi sur le droit d'auteur* (L.R.C., 1985, c. C-42);

76. La Loi sur les marques de commerce (L.R.C., 1985, c. T-13);

77. La *Charte des droits et libertés de la personne du Québec* (L.R.Q., c. C-12) et plus spécifiquement, ses articles 5 et 9 portant sur le respect de la vie privée et le secret professionnel et la *Charte canadienne des droits et libertés* (Annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R-U));

78. La Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications (L.C. 2010, ch. 23);

79. Entente conclue entre l'Ordre des comptables professionnels agréés du Québec et l'Autorité des marchés financiers à l'égard des membres de l'Ordre qui détiennent le titre de planificateur financier;

80. Entente de collaboration entre l'Ordre des comptables professionnels agréés du Québec et le Conseil canadien sur la reddition de comptes (L.R.Q., c. C-48.1, r. 15.1) conformément à l'article 9 de la *Loi sur les comptables professionnels agréés*;

81. Entente entre l'Ordre des comptables professionnels agréés du Québec et l'ACPAI Assurance (« ACPAI ») Règlement sur l'assurance de la responsabilité professionnelle des membres de l'Ordre des comptables professionnels agréés du Québec;

82. Normes de sécurité PCI-DSS (Payment Card Industry DATA Security Standard);

83. Guide de l'Ordre sur l'accès aux documents et sur la protection des renseignements personnels concernant le contrôle de l'exercice de la profession de comptable professionnel agréé;

84. Politique relative au Code d'éthique à l'intention du personnel de l'Ordre.