La profession de CPA et l'utilisation des technologies à l'ère numérique : vos pratiques sont-elles au point?

Dans l'exercice de leur profession, les comptables professionnels agréés utilisent de plus en plus les nouvelles technologies, les supports technologiques ainsi que les services hébergés et en infonuagique, ce qui soulève de nombreux enjeux de nature déontologique.

Conscient de cette réalité et afin de bien la cerner, l'Ordre a entrepris au cours des derniers mois des travaux qui déboucheront sur une vaste refonte du Règlement sur la tenue des dossiers et des cabinets de consultation et sur la cessation d'exercice d'un membre de l'Ordre des CPA et des modifications au Code de déontologie des CPA, dont l'entrée en vigueur est prévue pour 2018.

Résolu à accompagner ses membres vers la mise en place de pratiques conformes aux plus hauts standards, l'Ordre vous propose, dans un premier temps, le présent outil d'autodiagnostic lié à l'utilisation des technologies de l'information. Que vous exerciez en cabinet, en entreprise, seul ou au sein d'un organisme public, vous pourrez ainsi évaluer dans quelle mesure vos pratiques sont au point.

Dans la foulée de cet outil, un guide des bonnes pratiques est en cours de préparation et sera diffusé en décembre 2016. L'Ordre proposera également un atelier de formation pour vous aider concrètement à adapter vos façons de faire en prévision de l'adoption des nouvelles dispositions réglementaires.

Postes de travail

1. Les accès à votre poste de travail sont-ils protégés par un nom d'usager et un mot de passe?

2. Les mots de passe attribués sont-ils suffisamment sécuritaires?
   - *Saviez-vous que, selon les normes généralement reconnues dans ce secteur, un mot de passe sécuritaire devrait être composé d'un minimum de 8 caractères et comprendre des chiffres, des lettres, des majuscules et des minuscules et des caractères spéciaux ?*
   - *Saviez-vous que, suivant ces mêmes normes, pour être sécuritaire, un mot de passe doit être changé au moins aux 3 mois et ne pas être réutilisé avant 2 ans ?*

3. Votre poste de travail est-il mis en veille automatiquement après un certain laps de temps?

4. Le nom d'usager et le mot de passe donnant accès à votre poste de travail sont-ils partagés ou conservés dans un endroit accessible à un membre de votre cabinet ou à votre employeur en cas de décès ou d'incapacité subite?

5. Votre poste de travail est-il protégé par un antivirus mis à jour de façon automatisée?

6. Les disques durs des ordinateurs portables sont-ils chiffrés?

Employés

7. Offrez-vous à votre personnel ou votre employeur vous offre-t-il un programme de formation et de sensibilisation des employés en lien avec les politiques, lignes directrices et procédures concernant la sécurité?

8. Ces politiques, lignes directrices et procédures sont-elles diffusées auprès des employés?

9. Lors du départ d'un employé, les accès qui lui étaient accordés (serveur, comptes, documents) sont-ils supprimés afin d'assurer la confidentialité des données?

   › *Saviez-vous que, selon une étude menée par Lieberman Software en mai 2014, jusqu'à 13 % des anciens salariés déclarent que leurs identifiants de connexion leur permettent encore d'avoir accès aux systèmes informatiques de leur ex-employeur ? L'étude a été menée auprès de 280 professionnels des TI, dont plus de 55 % travaillaient dans des entreprises de plus de 1 000 employés.*

Sauvegardes

10. Avez-vous mis en place une méthode de gestion des copies de sauvegarde des données enregistrées sur votre réseau?

    › *On entend par données tous les renseignements relatifs à vos clients.*

11. Savez-vous à quelle fréquence sont sauvegardées les données?

12. Savez-vous à quel endroit les copies de sauvegarde sont conservées?

13. Ces copies de sauvegarde sont-elles chiffrées ou protégées par un mot de passe adéquat?

    › *Le chiffrement est une méthode permettant de renforcer la sécurité d'un message ou d'un fichier en brouillant son contenu de sorte que seules les personnes disposant de la clé de chiffrement appropriée pour les déchiffrer peuvent les lire.*

14. Savez-vous si ces données sauvegardées seront récupérables dans un format qui sera lisible lorsque viendra le temps de les consulter, à court terme?

Réseau interne (incluant le réseau vous reliant à l'Internet)

15. Les données sont-elles hébergées dans un environnement hébergé ou infonuagique, ou sur un réseau local?

16. Si vous utilisez un réseau local, ce réseau est-il protégé par un pare-feu mis à jour régulièrement?

17. La sécurité physique de ce serveur est-elle assurée?

18. Si l'accès à un réseau est offert à des visiteurs, ce réseau est-il distinct de celui donnant accès aux données?

Consultants externes ou internes

19. Lorsque vous faites affaire avec un consultant externe ou interne qui peut avoir accès aux données relatives à vos clients contenues dans votre système informatique (réseau interne, poste de travail, ordinateur mobile, téléphone intelligent, environnement hébergé et infonuagique, ou autre), lui faites-vous signer un engagement de confidentialité?

   - *Saviez-vous que selon un mondial en sécurité de l'information tenu en 2016 par le cabinet PwC, 41% des vols de données sont liés à des fournisseurs de services/consultants actuels ou antérieurs[1]?*

Fournisseurs de services d'hébergement de données et de services infonuagiques

20. Si les données sont hébergées à l'externe, un contrat a-t-il été conclu avec le fournisseur infonuagique?

21. Ce contrat prévoit-il:

   - des mesures assurant la confidentialité des données hébergées?
   - des mesures assurant l'intégrité des données hébergées?
   - des mesures encadrant l'accessibilité des données hébergées, vous permettant d'y avoir accès en tout temps?
   - un processus de destruction des données et des mesures quant à leur conservation?
   - un processus lié à la récupération des données hébergées et qui en garantit la valeur et l'intégrité?
     - *Saviez-vous qu'il est possible d'exiger un plan de réversibilité prévoyant notamment les conditions, les coûts et les facteurs déclencheurs (manquements contractuels du fournisseur, libre choix du client, simple écoulement du temps) qui vous permettront de récupérer vos données?*
   - un calendrier de sauvegardes et leur conservation?

22. Ce contrat comporte-t-il une clause :

   - assurant que vous ou votre employeur demeurez propriétaire des données hébergées et que celles-ci seront détruites à la fin du contrat?
   - obligeant le fournisseur à vous aviser en cas de vol de données ou de brèche?
   - permettant d'effectuer des audits ou de recevoir les résultats des audits effectués?
   - de couverture d'assurance en cas de perte de données?

23. Les clients sont-ils informés que des données les concernant sont sauvegardées sur un serveur externe?

24. Le fournisseur et les données hébergées sont-ils en territoire canadien et de propriété canadienne?

   - *Saviez-vous que le Patriot Act s'applique à tous les contrats conclus avec un fournisseur américain, de sorte que les données hébergées peuvent être accessibles par la justice et les forces de l'ordre américaines?*

[1] Institut Fasken Martineau – Maîtriser les risques en cybersécurité : mieux prévenir et agir – 16 mars 2016

Communications

25. Si vous avez recours à une plateforme de services (portail ou échange de fichiers) qui est accessible à vos clients, avez-vous mis en place des mesures pour en assurer la sécurité?

26. Si vous communiquez avec vos clients ou votre employeur par courriel, savez-vous si le serveur que vous utilisez garantit la confidentialité et utilise un système de chiffrement?

27. Chiffrez-vous les messages et les documents transmis par courriel?

28. Obtenez-vous l'autorisation de vos clients avant d'échanger des informations confidentielles par courriel avec eux?

29. Si vous transmettez des informations confidentielles par texto, comment vous assurez-vous qu'elles demeurent confidentielles?

Technologies mobiles

30. Votre téléphone intelligent contient-il des données relatives à vos clients ou des données de votre employeur?
    - *Saviez-vous que vous pouvez configurer le chiffrement des données confidentielles contenues sur votre téléphone intelligent?*

31. Les données contenues sur des plateformes mobiles (ordinateur portable, tablette, clé USB, disque dur externe, etc.) sont-elles suffisamment protégées et même chiffrées?

32. Vous arrive-t-il d'utiliser des réseaux publics non sécurisés avec une plateforme mobile contenant des données relatives à vos clients ou à votre employeur?

33. Permettez-vous à vos employés, ou votre employeur vous permet-il d'utiliser des appareils personnels et si oui, ces appareils doivent-ils respecter des exigences de sécurité (antivirus à jour, chiffrement des données et mots de passe robustes et changés fréquemment)?

34. Une politique sur l'utilisation de ces technologies et qui prévoit les mesures de sécurité requises a-t-elle été mise en place?

35. Disposez-vous de moyens de sécurité suffisants pour les employés qui se connectent à distance (p. ex. accès VPN)?

36. Lorsqu'un accès à distance est utilisé, à domicile par exemple, comment s'assure-t-on que le réseau Internet du domicile est sécurisé et que des données professionnelles ne puissent s'y retrouver?

N. B. Ce questionnaire d'autodiagnostic a simplement pour but de vous permettre d'évaluer vos pratiques et de vous aider à vous préparer à la nouvelle réglementation qui viendra encadrer l'utilisation des technologies de l'information en 2018. **Il ne doit pas être retourné à l'Ordre.**