

Août 2019

Premiers de classe : nouveau programme de cybersécurité visant la certification des entreprises qui ont à cœur la protection de la vie privée

Le 14 août 2019, le gouvernement fédéral a [lancé](#) un nouveau programme de certification en cybersécurité visant à aider les petites et moyennes entreprises à se protéger contre les cybermenaces.

Le lancement de CyberSécuritaire Canada (« **CyberSécuritaire** ») n'est qu'une des mesures qui ont été mises en œuvre par le gouvernement à la suite de [l'annonce de sa Charte numérique](#) un peu plus tôt cette année, et vise à permettre au gouvernement d'atteindre son objectif, soit d'aider les entreprises canadiennes à augmenter la confiance des consommateurs et à demeurer concurrentielles à l'échelle mondiale à l'ère du numérique.

CyberSécuritaire est un programme de certification volontaire dans le cadre duquel les entreprises doivent mettre en œuvre de nombreux [contrôles de cybersécurité de base](#) conçus pour les protéger contre les cyberattaques les plus courantes.

Ces contrôles de cybersécurité de base ont été élaborés de manière à ce qu'il soit relativement facile et peu coûteux pour les entreprises comptant moins de 500 employés et présentant un risque moyen de les mettre en œuvre. Les contrôles de cybersécurité de base comprennent notamment ce qui suit :

- L'élaboration d'un plan d'intervention en cas d'incident qui permet de gérer les incidents de cybersécurité;
- La mise en œuvre d'un système de gestion des informations et des événements de sécurité;
- L'activation de mises à jour automatiques pour les logiciels et le matériel informatique, si une telle option est disponible;
- La configuration et l'activation de logiciels antivirus et d'antimaliciels à jour;
- La mise en œuvre d'une solution d'authentification à deux facteurs;
- L'adoption de politiques concernant les mots de passe;
- L'offre de formation pour sensibiliser les employés afin de diminuer les incidents causés par une erreur humaine;
- La sauvegarde et le chiffrement des données;
- L'établissement d'un périmètre de défense approprié, tel qu'un coupe-feu;
- L'application du principe des « autorisations minimales », c.-à-d. l'octroi d'autorisations aux utilisateurs pour qu'ils aient les fonctionnalités minimalement requises pour l'exécution de leurs fonctions et l'acquittement de leurs responsabilités.

Le Conseil canadien des normes sera responsable de l'accréditation des organismes de certification, qui évalueront la conformité des entreprises au programme CyberSécuritaire et leur accordera la certification. Les entreprises qui sont considérées comme étant conformes au programme CyberSécuritaire pourront afficher une marque ou un logo de certification sur leur site Web ou leur matériel promotionnel.

Le programme CyberSécuritaire sera à l'étape du projet pilote jusqu'à l'élaboration d'une norme de conformité nationale. Les entreprises peuvent s'inscrire dès maintenant à titre d'« utilisateurs

précoces » afin de participer à la mise à l'essai et à l'élaboration du processus de certification. Les entreprises intéressées à s'inscrire à titre d'utilisateurs précoces peuvent communiquer avec l'équipe CyberSécuritaire au 1-800-328-6189 ou par courriel, à l'adresse suivante : ISED-ISDE@canada.ca.

Les entreprises qui ne souhaitent pas s'inscrire à titre d'utilisateurs précoces peuvent quand même prendre de l'avance en commençant à examiner et à mettre en œuvre les contrôles de sécurité de base.

Il est également important de souligner que, bien que l'adhésion au programme de certification CyberSécuritaire soit volontaire, un grand nombre d'organismes sont tenus, en vertu de la législation sur la protection de la vie privée applicable – notamment la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRDE** ») – de mettre en œuvre des mesures de protection appropriées afin de protéger les renseignements personnels contre la perte ou le vol de ceux-ci, ou l'accès à ceux-ci ou la communication, l'utilisation ou la modification de ceux-ci sans autorisation. Par conséquent, il est recommandé aux organismes d'évaluer régulièrement leur programme de protection de la vie privée et des données, compte tenu des menaces de plus en plus grandes pour la cybersécurité et des faits nouveaux dans la législation canadienne et internationale en matière de protection de la vie privée.

par Kristen Pennington

Pour en savoir plus sur le sujet, veuillez communiquer avec les personnes suivantes :

Toronto Kristen Pennington 416.865.7943 kristen.pennington@mcmillan.ca

[mise en garde](#)

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt consulter ses propres conseillers juridiques.

© McMillan S.E.N.C.R.L., s.r.l. 2019