CANADIAN PARTNERSHIP AGAINST CANCER | PARTENARIAT CANADIEN CONTRE LE CANCER

Aperçu du cadre de sécurité et de protection des renseignements personnels

Le Partenariat canadien contre le cancer (le Partenariat) remplit un vaste mandat visant à mettre en œuvre la stratégie de lutte contre le cancer du Canada en unissant les efforts de partenaires de partout au pays et en collaborant avec les cancérologues, les organismes caritatifs et les organismes nationaux en matière de santé, les gouvernements, les organismes de lutte contre le cancer, les survivants, etc. Dans le cadre de l'exécution de son mandat, le Partenariat collecte, emmagasine et partage une grande quantité de renseignements possédant différentes sensibilités, c'est pourquoi il a aménagé un programme de sécurité des renseignements tout aussi robuste.

Cadre de sécurité et de protection des renseignements personnels du Partenariat

Le cadre de sécurité et de protection des renseignements personnels forme la base du programme robuste de sécurité des renseignements du Partenariat qui inclut une vaste gamme de normes et de politiques relatives aux technologies de l'information. L'ensemble des normes et des politiques relatives aux technologies de l'information et à la gestion de l'information du Partenariat sont élaborées en fonction des normes de l'industrie et sont conçues pour étayer et pour guider une vaste gamme d'activités des TI en lien avec la sécurité dans le cadre des différents travaux du Partenariat. Le programme de sécurité de l'information, fondé sur le cadre de cybersécurité du NIST, a des retombées positives sur l'ensemble de l'organisation grâce à la mise en œuvre de normes de sécurité des systèmes et de directives opérationnelles qui soutiennent les opérations quotidiennes et stratégiques.

Le programme de protection des renseignements personnels du Partenariat a été mis en œuvre pour garantir que les personnes avec lesquelles il collabore dans le cadre de ses activités opérationnelles connaissent leurs droits quant à la protection de leurs renseignements personnels. Le Partenariat a adopté plusieurs politiques qui assurent une plus grande transparence envers les personnes quant aux types de renseignements personnels qu'il recueille et aux fins pour lesquelles il les recueille. Le programme de protection des renseignements personnels est fondé sur l'obtention du consentement de l'individu, et à chaque occasion possible, sauf si la loi en dispose autrement, le Partenariat obtiendra le consentement quant à la façon dont il recueille et utilise les renseignements personnels.

Le Partenariat accorde également un droit raisonnable d'accès et de modification des renseignements personnels qu'il détient concernant une personne, et s'efforcera de fournir lesdits renseignements dans un délai raisonnable et dans un format lisible à la personne qui en fait la demande.

Le programme de sécurité et de protection des renseignements personnels est géré et exécuté sous l'autorité et l'administration de l'agent en chef de la sécurité et de la protection des renseignements personnels et des services généraux du Partenariat. Des rapports de surveillance et de conformité du cadre de sécurité et de protection des renseignements personnels sont présentés chaque année au comité du conseil des finances et de la vérification du Partenariat.

Dix éléments essentiels du cadre de sécurité et de protection des renseignements personnels

1. *Groupe complet et en expansion de politiques de sécurité et de protection des renseignements personnels au sein des systèmes*, qui fournit des conseils sur une vaste gamme d'enjeux relatifs à la sécurité et à la protection des renseignements personnels.
2. *Examen annuel des normes en matière de sécurité pour garantir la conformité aux pratiques exemplaires de l'industrie, et examen biennal de toutes les politiques en matière de sécurité et de protection des renseignements personnels*, afin de veiller à leur pertinence et à leur efficacité.
3. *Programme de formation personnalisé portant sur les systèmes de sécurité*, offert sous la forme d'une formation en ligne assistée par ordinateur, qui comprend des séances de formation annuelles pour tout le personnel ainsi que des séances d'orientation pour les nouveaux employés.
4. *Évaluations des menaces et des risques* et *évaluations des facteurs relatifs à la vie privée* de tous les nouveaux systèmes d'information du Partenariat et de tous ceux ayant été modifiés de manière significative ainsi que la gestion des mesures correctives découlant de ces évaluations à l'aide de plans de mise en œuvre de mesures de protection.
5. *Programme de gestion active des risques* retraçant et surveillant la mise en œuvre des contrôles de sécurité et des risques à la sécurité au sein des systèmes d'information de l'organisation.
6. *Examens périodiques approfondis de l'accès utilisateur* aux banques de données les plus sensibles du Partenariat.
7. *Conseil consultatif relatif aux modifications apportées aux TI* formé de membres clés du service des TI du Partenariat, d'un fournisseur externe expert en TI, d'un membre externe de la sécurité des TI et de gestionnaires de programme, au besoin, pour veiller à ce que les modifications à apporter aux systèmes soient vérifiées et évaluées minutieusement, d'un point de vue à la fois technique et opérationnel, afin de minimiser les risques.
8. *Examens de la protection des renseignements personnels et de la sécurité* des processus d'examen des systèmes du Partenariat pour veiller à la détection précoce des problèmes potentiels liés à la sécurité ou à la protection des renseignements personnels, à la détermination du niveau de risque associé à ces problèmes et à l'atténuation ou à l'acceptation des risques.
9. *Maintenance et amélioration continues des systèmes d'information organisationnels du Partenariat*, y compris la sécurité de réseau, la gestion de la segmentation et de l'accès afin de minimiser et d'atténuer les risques pour la sécurité.
10. *Introduction de nouvelles technologies centralisées de gestion de l'identité et de l'accès* afin de garantir un niveau d'assurance élevé relativement à l'accès utilisateur à l'ensemble des services de l'organisation et à ceux axés sur le public.

Le service de soutien des technologies de l'information au Partenariat

Le directeur des technologies de l'information a la responsabilité de la gestion de la sécurité de l'information au Partenariat et de la direction de la stratégie en matière de sécurité de l'information. Sous la responsabilité

de l’agent en chef de la sécurité et de la protection des renseignements personnels, le directeur des technologies de l’information recommande des politiques en matière de protection des renseignements personnels et de sécurité de l’information en lien avec les initiatives stratégiques, l’architecture technologique et les questions liées à la sécurité des systèmes.

L’équipe des technologies de l’information, sous la supervision du directeur des technologies de l’information, est dotée d’un gestionnaire en TI à temps plein et d’une équipe de technologues chargée d’assurer la gestion des sites Web du Partenariat, et de l’ensemble des technologies et systèmes connexes.

Le Partenariat compte également sur une équipe dévouée d’experts externes en sécurité de l’industrie, disponibles sur demande, pour effectuer une évaluation indépendante et plus détaillée de la sécurité et pour fournir des conseils portant sur la politique, l’architecture des systèmes, les pratiques opérationnelles et la sécurité de l’information. Le Partenariat se penche sur les très importantes questions de sécurité en lien avec l’infrastructure de l’entreprise, la vérification, l’évaluation des risques associés aux projets nouveaux et existants, en mettant à profit le savoir-faire des fournisseurs et des ressources internes et externes.