

7. Protection des données et cybersécurité

Collecte de données

- 7.1 Sous réserve des lois sur la protection de la vie privée et des données, y compris la [Loi sur la protection des renseignements personnels et les documents électroniques](#) et la common law régissant la transmission de renseignements confidentiels au Canada, la GTAA se réserve le droit de recueillir, d'utiliser et de divulguer des données personnelles et des renseignements confidentiels du public et des usagers de l'aéroport, directement ou par l'intermédiaire d'un tiers, y compris, sans s'y limiter, lorsque la GTAA estime que ces données et renseignements sont nécessaires aux fins suivantes :
- 7.1.1 Assurer la sûreté et la sécurité des activités de l'aéroport.
 - 7.1.2 Effectuer des activités de planification, d'exploitation et d'autres autres initiatives de gestion du rendement de l'aéroport.
 - 7.1.3 Améliorer l'expérience des passagers et le service à la clientèle à l'aéroport.
 - 7.1.4 Se conformer aux lois et règlements nationaux et internationaux relatifs, sans s'y limiter, à la sûreté et à la sécurité des aéroports, à la protection de l'environnement, au blanchiment d'argent, aux sanctions et aux contrôles à l'exportation.
- 7.2 La GTAA s'engage à prendre toutes les mesures de protection juridiques raisonnables et à déployer les ressources techniques nécessaires pour protéger et garder confidentiels les données ou les renseignements non publics reçus du public ou des usagers de l'aéroport, sauf si la loi l'exige expressément ou si une autorité gouvernementale, un tribunal ou un organisme d'application de la loi le demandent expressément.
- 7.3 La [Politique de confidentialité de la GTAA](#) régit la façon dont les données personnelles et les renseignements confidentiels sont recueillis, traités, stockés, utilisés, gérés, divulgués, transférés et détruits.

Protection de la confidentialité des données et cybersécurité

- 7.4 Les usagers de l'aéroport doivent se conformer aux lois applicables en matière de protection des données et de la vie privée et doivent immédiatement aviser la GTAA de toute atteinte à la sécurité des données, de toute violation du système ou de tout accès non autorisé aux données relatives à l'aéroport dès leur détection, fournir des détails supplémentaires sur tout incident de ce genre à la demande de la GTAA et, au besoin, produire un rapport médico-légal indépendant en temps opportun.
- 7.5 Les usagers de l'aéroport à qui on a accordé l'accès aux systèmes et aux données de l'aéroport doivent :
- 7.5.1 Mettre en œuvre et tenir à jour des programmes et pratiques de protection de la vie privée et de sécurité de l'information pour protéger l'information contre tout accès non autorisé, notamment des mesures de protection techniques, administratives, opérationnelles, organisationnelles et physiques.
 - 7.5.2 Se conformer aux règles, protocoles et exigences d'accès et d'utilisation des systèmes et des données de l'aéroport tels qu'ils sont établis et modifiés de temps à autre par la GTAA.

- 7.5.3 S'assurer que les identifiants d'accès demeurent sécurisés et qu'ils ne sont utilisés que par les personnes à qui ils ont été fournis.
- 7.5.4 Surveiller l'accès non autorisé aux systèmes technologiques, répondre à la validation de l'accès et aux vérifications des comptes d'accès en temps opportun, et assumer la responsabilité du retrait des comptes d'utilisateur pour les employés qui sont congédiés ou qui changent de tâches, y compris les sous-traitants temporaires.
- 7.5.5 Se conformer aux pratiques exemplaires de l'industrie, aux modalités d'utilisation applicables et aux dispositions contractuelles liées à la cybersécurité.
- 7.5.6 Protéger et conserver les dossiers de vérification du système dans la mesure nécessaire pour permettre une surveillance, une analyse et une enquête adéquates.
- 7.5.7 Signaler toute activité illicite, non autorisée ou inappropriée du système ou tout code malveillant comme les virus, les vers et les chevaux de Troie.
- 7.5.8 Surveiller régulièrement les vulnérabilités en matière de sécurité et les faire corriger par un personnel compétent et pleinement formé.
- 7.5.9 Prévoir les urgences et soutenir la GTAA en ce qui concerne ses politiques en matière de cybersécurité et ses initiatives de protection.
- 7.5.10 Établir des capacités de traitement des incidents pour les systèmes technologiques, ce qui doit comprendre la préparation, la détection, l'analyse, le confinement, la récupération et les activités d'intervention des utilisateurs.
- 7.5.11 Aviser la GTAA de toute vulnérabilité critique présente dans tout système technologique utilisé pour appuyer les opérations de l'aéroport ou stocker des données de l'aéroport, et donner l'assurance que des mesures correctives seront prises en temps opportun à l'égard des vulnérabilités critiques identifiées.
- 7.5.12 Aviser la GTAA de toute atteinte potentielle ou réelle à la cybersécurité ou de tout accès non autorisé à l'information de la GTAA ou aux données de l'aéroport, et prendre toutes les mesures raisonnables pour réduire au minimum les préjudices à la GTAA.
- 7.5.13 Signaler au Commissariat à la protection de la vie privée du Canada et aux personnes touchées les violations des mesures de protection des données, conformément aux lois applicables, dont la [Loi sur la protection des renseignements personnels et les documents électroniques](#).

- 7.6 Les usagers de l'aéroport qui, par leurs actes ou omissions, causent un incident de cybersécurité, une violation des mesures de protection des données applicables, un accès non autorisé à l'information de la GTAA, ou le non-respect des dispositions des lois sur la cybersécurité et la protection des données indemniseront la GTAA de tous les coûts engagés à la suite de telles défaillances.