7. Data protection and cybersecurity

Data collection

7.1 Subject to privacy and data protection laws, including the Personal Information Protection and Electronic Documents Act and the common law governing the transmission of confidential information in Canada, the GTAA reserves the right to collect, use, and disclose personal data and confidential information from the public and Airport Users, directly or via a third party, including but not limited to when the GTAA considers that such data and information are necessary for the following purposes:

7.1.1 Ensuring the safety and security of Airport operations.

7.1.2 Planning, operational, and other Airport performance management initiatives.

7.1.3 Improving the Passenger experience and customer service at the Airport.

7.1.4 Complying with national and international laws and regulations related but not limited to Airport safety and security, environmental protection, money laundering, sanctions, and export controls.

7.2 The GTAA is committed to taking all reasonable legal safeguards and deploying the necessary technical resources to protect and keep confidential any non-public data or information received from the public or Airport Users, unless expressly required by law or requested by a government authority, court, or law enforcement agency.

7.3 The GTAA Privacy Policy governs how personal data and confidential information is collected, processed, stored, used, managed, disclosed, transferred, and destroyed.

Data privacy protection and cybersecurity

7.4 Airport Users must comply with applicable laws relating to data and privacy protection and must immediately notify the GTAA of any data breach, system breach or unauthorized access to data relating to the Airport upon detection, provide additional details about any such incident upon request by the GTAA, and, upon request, deliver an independent forensics report in a timely manner.

7.5 Airport Users who have been granted access to Airport systems and data must:

7.5.1 Implement and maintain information privacy protection and security programs and practices to safeguard information from unauthorized access, including technical, administrative, operational, organizational, and physical safeguards.

7.5.2 Comply and abide by the rules, protocols, and requirements of access and use of the Airport systems and data as established, and amended from time to time, by the GTAA.

7.5.3 Ensure that access credentials remain secure and are only used by those individuals to whom the credentials have been provided.

7.5.4 Monitor unauthorized access to technology systems, respond to access validation and audits of access accounts in a timely manner, and take responsibility for the removal of user accounts for employees who are terminated or change job functions, including temporary sub-contractors.

7.5.5 Comply with industry best practices, applicable terms of use, and contractual provisions related to cybersecurity.

7.5.6 Protect and retain system audit records to the extent needed to enable adequate monitoring, analysis, and investigation.

7.5.7 Report any unlawful, unauthorized, or inappropriate system activity or malicious codes such as viruses, worms, and Trojan horses.

7.5.8 Monitor for and patch security vulnerabilities on a regular basis by competent and fully trained personnel.

7.5.9 Plan for contingencies and inform the GTAA regarding their cybersecurity policies and protection initiatives.

7.5.10 Establish incident handling capabilities for technology systems that must include preparation, detection, analysis, containment, recovery, and user response activities.

7.5.11 Notify the GTAA of any critical vulnerabilities present in any technology systems used to support Airport operations or store Airport data and provide assurances that remediation will be performed against the identified critical vulnerabilities in a timely manner.

7.5.12 Notify the GTAA about any potential or actual cybersecurity breaches or unauthorized access to GTAA information or Airport data and take all reasonable measures to minimize damages to the GTAA.

7.5.13 Report privacy breaches of data protection safeguards intended to protect privacy to Canada's Privacy Commissioner and affected individuals in accordance with applicable laws including the Personal Information Protection and Electronic Documents Act.

7.6 Airport Users who through their acts or omissions or who otherwise cause any cybersecurity incident, breach of applicable data protection safeguards, unauthorized access to GTAA information, or non-compliance with provisions of cybersecurity and data protection laws shall indemnify the GTAA for any costs incurred as a result of such failures.