Personal Information Protection and Electronic Documents Act (PIPEDA) Compliance Policy

Intent

Thunder Bay International Airports Authority Inc. (TBIAAI) is committed to protecting personal information in compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This policy sets out standards and guidelines to ensure that the company complies with PIPEDA.

Definitions

Breach of security safeguards: The loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards, or from a failure to establish those safeguards.

Commissioner: The privacy commissioner appointed under the *Privacy Act.*

Personal information: Information about an identifiable individual.

Significant harm: Includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business, or professional opportunities, financial loss, identity theft, negative effects on a credit record and damage to or loss of property.

Guidelines

TBIAAI collects, uses, and discloses personal information for legitimate business purposes in accordance with PIPEDA. The company only collects, uses, and discloses personal information that a reasonable person would consider appropriate in the circumstances.

PIPEDA Representative

TBIAAI has designated the HR Advisor as the representative responsible for the organization's compliance with PIPEDA. The representative is responsible for the management and implementation of the company's personal information policies and procedures. The Security Manager and other relevant individuals may be designated to assist with these measures.

The PIPEDA representative is responsible for developing and implementing policies and practices related to PIPEDA, including:

- Procedures that address the collection, use, retention, management of personal information;
- Procedures for protecting personal information in all formats;
- Procedures for receiving and responding to complaints and inquiries;
- Staff training and communicating information about the company's privacy policies and practices;
- Developing information and materials to explain the company's policies and procedures; and

- Reviewing privacy policies, practices, and procedures regularly and making appropriate revisions.

Any questions or concerns regarding privacy and personal information should be directed to the HR Advisor at 807-473-2608. This includes requests for access to personal information and requests to amend personal information from clients.

Consent

TBIAAI obtains consent from individuals to collect, use, and disclose personal information where required by law. Consent may be express or implied depending on the circumstances and the type of personal information collected. All reasonable efforts must be made to obtain express consent before collecting, using, or disclosing personal information.

Express consent is required whenever personal information is collected for new employees or clients, when collected electronically or for use of a background check through a third party. Express consent will be obtained by signatory acknowledgment, whether physical or electronic.

Personal information must only be used and disclosed solely for the purpose for which it was collected by the company. Express consent must be obtained from the individual to use or disclose the information for a reason other than which it was originally collected. Anytime personal information is used for a new purpose, the HR Advisor must be notified so it can be documented.

Individuals have the right to withdraw their consent at any time. The company informs individuals of the implication of their withdrawal. Where an individual withdraws their consent, the company discontinues the collection, use, and disclosure of their information except in situations where consent is not required by law.

Exceptions

PIPEDA allows for the collection, use, and disclosure of personal information without knowledge or consent in certain circumstances. The company collects personal information without consent in the following circumstances:

- when legally required
- in cases of immediate medical necessity

Collection and Use

Personal information is only collected when it serves a legitimate, reasonable business purpose. Information is collected and stored by the HR Advisor or other authorized management members.

Disclosure

TBIAAI does not share this personal information with third parties.

If sharing personal information for the purposes of a person applying for a Transportation Security Clearance / Restricted Area Identification Card (RAIC): Personal information is shared with the *Canadian Air Transport Security Authority (CATSA)*, *Transport Canada (TC)*, and their partners. More information may be found here:

https://tc.canada.ca/en/programs/non-funding-programs/transportation-security-clearance-program/transportation-security-clearance-program-aviation/transportation-security-clearance-program-aviation#partnership

Access to and Amending Personal Information

Individuals have the right to request to access to their personal information held by the company, and request corrections as appropriate to ensure the information is accurate and complete.

Requests for access or correction must be submitted in writing and should be directed to the HR Advisor. The company assists any individual who requires assistance preparing a request for access.

Responses to requests are provided as soon as reasonably possible, but usually no later than 30 days after receipt. This period may be extended by up to 30 days if the time limit unreasonably interferes with the company's work, or the time to make the necessary consultations to respond the requests is impractical. The time for a response may be extended for longer if it is necessary to convert the personal information into an alternative format. If a request is extended beyond the typical 30-day threshold, a notice of extension is sent to the individual within 30 days of the receipt of their request that advises them of new the timelines, the reason for the extension, and their right to file a complaint with the commissioner regarding the extension.

Where a request for access is received and approved, the company informs the individual whether it holds any personal information about them and the source of the information. The company also informs the individual whether their personal information has been disclosed to any third parties and identifies the third parties if known. If the third parties are not known, a list of organizations the information may have been disclosed to is provided. This information is provided in a manner that is understandable to the individual. If abbreviations or other short forms are used, an explanation is provided along with the information.

Where an individual demonstrates that their personal information held by the company is inaccurate or incomplete, the company updates this information as soon as reasonably possible. This may include correction, deletion, or adding information. If this information has been disclosed to third parties, they must also be informed on the amendment.

The company reserves the right to deny a request for access in accordance with PIPEDA. Where a request for access is denied, the individual is informed of the reason for the refusal in writing and any options for recourse available to them under PIPEDA.

Protecting Personal Information

All personal information in TBIAAI possession or custody, regardless of the format it is held, is protected using appropriate security safeguards. Safeguards implemented are proportional to the sensitivity of the information. These safeguards are intended to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification.

The company is responsible for all personal information in its possession or custody, including information transferred to a third party for processing. Where information is shared with a third party for processing, contracts are in place to protect this information.

The company uses a combination of physical, organizational, and technical measures to safeguard personal information. Access to personal information is limited to authorized personnel who have a legitimate need to access the information. Personal information is

retained only for the period that it is reasonably required. When it is no longer need, personal information is destroyed safely, securely, and effectively.

Breach of Security Safeguards

TBIAAI notifies the required parties in accordance with PIPEDA where there is a breach of security safeguards involving personal information under the company's control and it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The sensitivity of the personal information involved in the breach and the probability that the personal information has been, is being, or will be misused are considered when determining whether a breach of security safeguards creates a real risk of significant harm to an individual.

The Security Manager and HR Advisor, are responsible for coordinating the response to the breach and ensuring that all reasonable action is taken to address the breach.

All notifications are provided as soon as reasonably possible after the breach has occurred.

The company may notify other organizations, government institutions, or parts of government institutions of the breach if the company believes that doing so can reduce or mitigate the harm from the breach.

The company maintains records of every breach of security safeguards. These records are maintained for 24 months after the day the company discovered the breach occurred. Access to or a copy of these records are provided to the privacy commissioner of Canada upon request.

Report to Commissioner

The company provides a written report to the commissioner that contains the following information:

- A description of the circumstances of the breach and, if known, the cause;
- The date or the period during which the breach occurred, or if neither is known, the approximate period;
- A description of the personal information that is the subject of the breach to the extent that the information is known;
- The number of individuals affected by the breach or, if unknown, the approximate number;
- A description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
- A description of the steps that the organization has taken or intends to take to notify affected individuals of the breach; and
- The name and contact information of a person who can answer the commissioner's questions about the breach on behalf of the organization.

The company informs the commissioner of any new information the company becomes aware of after making the initial report.

Notification to Individuals

All individuals who face a real risk of significant harm because of the breach of security safeguards are notified.

The affected individual is directly notified of the breach except where direct notification would likely cause further harm to the individual, cause undue hardship for the company, or where the company does not have their contact information. Direct notification may be provided by phone, mail, or e-mail.

Notifications contain sufficient information to allow the individual to understand the significance of the breach, including:

- A description of the circumstances of the breach;
- The date or period during which the breach occurred or, if neither are known, the approximate period;
- A description of the personal information that is the subject of the breach to the extent that the information is known;
- A description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- A description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- Contact information that the affected individual can use to obtain further information about the breach.