



中国工商银行 (加拿大)

INDUSTRIAL AND COMMERCIAL BANK OF CHINA (CANADA)

PRIVACY STATEMENT FOR RECRUITMENT AND EMPLOYMENT

(Effective Date: Dec 2025)

Approved by:

Mr. Yuan Lu
Chief Executive Officer

Date:

Contents

0.	CHANGE LOG.....	3
1.	Introduction.....	3
2.	Scope	3
3.	Collection of Personal Information.....	3
4.	Use of Personal Information	5
	4.1 Purposes for Collecting Personal Information.....	5
	4.2 Dependent Information	5
	4.3 Cross-Border Transfer of Personal Information	6
5.	Disclosure of Personal Information.....	6
6.	Consent to Use Personal Information.....	7
7.	Retention and Disposal of Personal Information.....	7
8.	Security of Personal Information.....	8
9.	Transparency and Individual Rights	8
10.	Additional Information.....	9
11.	Compliance with Legislation	9
12.	Contact Information	9
13.	Acknowledgement of Receipt and Consent.....	9

0. CHANGE LOG

Month/ Year	Summary of Changes
May 2025	<ul style="list-style-type: none">▪ New document
Dec 2025	<ul style="list-style-type: none">▪ Incorporated the changes related to the collection of biometric data due to operational changes

1. Introduction

The Privacy Statement for Recruitment and Employment (the “Statement”) explains how Industrial and Commercial Bank of China (Canada) (the “Bank”, “ICBK”, “we”, “our”, or “us”) collects, uses, discloses, and protects personal information (the “Personal Information”) of prospective job applicants, employees, interns, and contractors during the recruitment process and throughout their employment or engagement with us.

The Bank is committed to protecting your Personal Information, ensuring it is managed securely and in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and other applicable privacy laws. Our practices reflect our commitment to collecting only the information necessary to support recruitment and ongoing employment-related purposes, safeguarding it against misuse, and maintaining transparency by clearly communicating how we collect, use, share, and protect such information.

2. Scope

The Statement applies to all prospective job applicants (both internal and external), current employees, interns, and contractors engaged with ICBK. It governs the collection, use, disclosure, retention, and protection of Personal Information related to recruitment, hiring, employment and internships activities. Personal information refers to any information that can identify an individual.

3. Collection of Personal Information

Personal Information will be collected in the course of recruitment, hiring and employment and internship activities. The word “Information” means personal, financial and other confidential information and details about an individual, which is provided voluntarily to ICBK through the individual (e.g. job applicant), or that has been shared with the Bank by a third party you have previously agreed can share the information with ICBK (e.g. online job board, social media sites, recruitment agencies/staffing companies), and/or received by us from outside sources (e.g. background check providers, your previous employers, publicly available information on social media or through an internet search). The types of Personal Information collected by the Bank may include, but is not limited to:

- Demographic and contact information, such as name, address, contact number, date of birth, email, etc.
- Government-issued Identification, such as social insurance number (SIN) upon acceptance of employment, and government-issued photo identification for verification purposes
- Education background and qualifications
- Employment history and professional references
- Skills and experience relevant to the role
- Employment records, such as attendance records, work schedules, time tracking data, compensation details, benefits information, payroll data, and records of leaves or absence
- Performance data, such as feedback, evaluation, performance reviews, including punctuality assessments derived from attendance records
- Information required for legal or regulatory compliance (e.g. tax, immigration, and employment law compliance)
- Background checks, including reference checks and verification of academic and professional qualifications, credit record checks, criminal record checks, etc., as permitted by law and with your consent
- Dependent information (e.g. name, address, date of birth, relationship to the employee) for benefits, insurance, emergency contact, and other applicable purposes
- Health or accommodation information, to the extent legally permitted or required, in relation to support accessibility that may be requested during the recruitment process and throughout the employment
- Biometric information (e.g. fingerprints) may be collected in certain circumstances for secure system access with your consent. Participation is voluntary and is solely collected for the purpose disclosed (e.g. system access). Biometric data is encrypted and stored in secure data centres, which could include locations outside Canada. Employees may opt out or withdraw consent at any time, subject to operational feasibility.
- Biometric data will be retained only for the purposes disclosed in this document for as long as required. The information will be deleted when no longer required for the stated purpose, for example, upon employee withdrawal from the biometric program or upon departure from the role that requires this biometric information to execute the responsibilities of said role.
- Any other information required for the purpose of recruitment and employment.

The Bank may require the aforesaid Personal Information to fulfill its obligations under applicable laws, administer employment benefits, and managing your employment relationship or other types of engagement with us. Failure to provide the requested information may impact the Bank's ability to process benefits, facilitate employment-related opportunities, or maintain your employment status. The Bank is committed to ensuring that any requested information is necessary, reasonable and collected in compliance with applicable privacy laws.

4. Use of Personal Information

4.1 Purposes for Collecting Personal Information

The collected Personal Information will be used for purposes related to recruitment, hiring, employment, and internships, including but not limited to:

- Recruitment and selection processes;
- Conducting background and reference checks;
- Administering and managing employment or contractual relationship, or other types of engagement (e.g. processing compensation payments, providing benefits, payroll, insurance requirements, etc.);
- Ensuring compliance with legal or regulatory requirements related to employment, and internal policy and procedures requirements;
- Preventing or managing any potential conflict of interests or investigations;
- Administering training and professional development ;
- Monitoring and evaluating employee performance, including tracking attendance records to assess punctuality and support performance management initiatives;
- Workforce planning and development, including promotions, transfer, and internal communications and review of employment decisions;
- Improving and managing programs, policies, and employee relations;
- Supporting secure system access through biometric authentication (e.g. fingerprint verification), where required and subject to employee consent;
- Government statistics or returns or any form of governmental data request for any reason

Personal Information may be disclosed to third parties for specific purposes where required or permitted by law, or with the relevant individual's consent. This includes disclosure to government agencies, benefit providers, background check service providers, recruitment agencies, other third-party service providers for recruitment or employment-related services, or regulatory bodies as required by law.

In the course of recruitment and employment processes, automated or AI-assisted tools may be used to support activities such as candidate sourcing, screening or communication. Where such technologies are involved, all decisions in hiring or HR processes will remain subject to human oversight, fairness assessments, and transparency in accordance with the applicable privacy and employment legislation.

4.2 Dependent Information

In some instances, the Bank may need to collect information about your dependents, such as their names, date of birth, and relationship to you. This data is typically required to provide benefits or insurance coverage, as well as for other family-related purposes during your employment. By providing the information of your dependent, you confirm that you have obtained the necessary consent from the data subject (i.e. your dependent)

to share their Personal Information with the Bank for the purposes as outlined in the Statement.

4.3 Cross-Border Transfer of Personal Information

As part of a global organization, Personal Information may be transferred to and processed by our Parent Bank, affiliated entities, or authorized third parties service providers in other jurisdictions, including outside of Canada. These transfers may be necessary for business purposes, such as HR administration, system operations, compliance with applicable regulations, and other legitimate purposes. ICBK's Canadian Privacy Policy and Standards will still apply to this data in terms of protection, privacy and retention.

5. Disclosure of Personal Information

Personal Information may be disclosed to third parties only where necessary to fulfill the purposes outlined in this Privacy Statement, or as required or permitted by law. Personal information will only be shared to the extent necessary for legitimate business, recruitment and employment, tax and compliance purposes. These third parties may include, but not limited to:

a) Government and Regulatory Authorities:

- Canada Revenue Agency (CRA) for tax reporting and payroll compliance.
- Employment and Social Development (ESDC) or the Labour Program for employment standards compliance.
- Any law enforcement, regulatory, or judicial authority as required by applicable laws or lawful requests.

b) Group Benefits, Pension and Insurance Providers:

- Group insurance carriers or third-party benefit administrators for employee health, dental, disability, health spending account, life insurance, other types of group insurance plans and wellness programs.
- Registered pension plan administrator for pension contributions and records management.

c) Payroll and Financial Services Providers

- Payroll service providers to process salary, wages, tax deductions and direct deposits.
- Financial institution to facilitate payroll deposits or other employment-related transactions.

d) Background Check and Verification Services:

- Third-party vendors conducting background checks, employment verification, credit history checks, or credential validations, as permitted by law and with your consent.

e) Professional Advisors or Auditors:

- Legal counsel, accountants, and auditors to ensure regulatory compliance, handle employment-related disputes, or conduct audits of employment practices.

f) Parent Bank or affiliated entities:

- Industrial and Commercial Bank of China, or its affiliated entities for legitimate corporate governance and business purposes, including regulatory compliance, risk management, audits, IT and system support, group-level and internal reporting, workforce management, strategic planning, crisis management, and security within the broader corporate structure.

g) Other Third-party Service Providers:

- Any other third-party service providers subject to contractual safeguards that ensure confidentiality and data protection.

We may also disclose your Personal Information:

- In accordance with applicable law, to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some of all of the Bank's assets, whether as a going concern or as part of bankruptcy, or similar proceeding, in which case Personal Information held by the Bank about our employees is among the assets transferred.
- To comply with any court order, law, or legal process, including to respond to any government or regulatory request, in accordance with applicable law.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of the Bank, our customers, or others.
- With your consent.

6. Consent to Use Personal Information

By submitting your application and continuing with the recruitment process, or by accepting an offer of employment or engagement with the Bank, you consent to the collection, use, and disclosure of your Personal Information as outlined in this Statement and the Bank's Privacy Policy.

You may withdraw your consent at any time by notifying the Human Resources & Administration Department of the Bank, subject to any legal or contractual restrictions. If consent is withdrawn, certain employment-related processes or benefits may not be available.

7. Retention and Disposal of Personal Information

If your job application is successful, your information will become part of your employee's file and will be retained for the duration of your employment and for as long as necessary to fulfill the purpose for which it was collected, in accordance with internal policies and

legal obligations. This retention is necessary for purposes such as tax reporting, benefits and pension administration, resolving employment-related matters, and ensuring regulatory compliance.

If your job application is unsuccessful, your information will be retained for a period necessary to meet legal and regulatory requirements, or to consider you for potential future employment opportunities, unless you opt out by contacting us. Personal Information will be retained for as long as it is necessary to fulfill the purpose for which it was collected, or as required by the applicable law. Once Personal Information is no longer required, it will be securely disposed or anonymized to prevent unauthorized access, use or disclosure.

8. Security of Personal Information

The Bank takes reasonable steps and appropriate measures include physical, administrative, and technical safeguards to protect Personal Information from loss, theft, unauthorized access, misuse or disclosure.

Security controls are regularly reviewed and updated to reflect evolving regulatory expectations and cyber risks.

Additional safeguards, including encryption, restricted access, and audit controls, are applied to biometric information due to its sensitive nature.

9. Transparency and Individual Rights

The Bank is committed to maintaining transparency in how Personal Information is collected, used and stored. Individuals have the right to:

- Request access of their Personal Information held by the Bank;
- Request to review, update, or correct, their Personal Information, where it is practicable and allowable;
- Withdraw their consent for the use of and delete their Personal Information at any time, subject to any legal or contractual obligations;
- Request information about the collection, storage, or deletion of their biometric information, and opt out of biometric authentication by selecting an alternate access method.

These rights can be exercised by submitting a written request to the Head of Human Resources and Administration, or the Bank's Privacy Officer. The Bank will make reasonable efforts to accommodate such request promptly within 30 calendar days, while adhering to the applicable legal and contractual requirements. By upholding these rights, the Bank reinforces its commitment to safeguarding Personal Information and ensuring transparent practices in all matters related to recruitment and employment.

10. Additional Information

For further details about how personal information is handled, individuals may refer to the Bank's broader Privacy Statement, which provides guiding principles on the collection, use, and disclosure of personal data. The Bank reserves the right to modify or amend the Privacy Statement at our discretion. Please refer to ICBK's corporate website for the latest version of Privacy Statement, which will be updated in accordance with the regulatory requirements from time to time.

11. Compliance with Legislation

The Bank is committed to complying with all applicable privacy laws and regulations, both provincially and federally. If any part of the Statement is inconsistent with the relevant legislation, the legal requirements shall prevail.

12. Contact Information

Inquiries about the Statement or the handling of Personal Information pertaining to recruitment and employment can be directed to the Head of Human Resources & Administration, or the Bank's Privacy Officer by writing to:

Industrial and Commercial Bank of China (Canada)
Bay Adelaide Centre, West Tower, Unit 3710
333 Bay Street, Toronto, ON M5H 2R2

Attention: Head of Human Resources & Administration / Privacy Officer

13. Acknowledgement of Receipt and Consent

By submitting your application, you acknowledge that you have read and understood this Privacy Statement and consent to the collection, use and disclosure of your Personal Information, including any dependent information, as described herein. If you are offered employment, express consent will be obtained through a signed offer letter, which will reference to this Privacy Statement and the Bank's internal policies and procedures regarding the processing, retention and security of your Personal Information.