US Employee Privacy Statement

Current Issue:	April 2025
Availability:	https://cibc.sharepoint.com/sites/sbu/en/us/policies/Pages/desc/us-employee-privacy-statement.aspx
Owner:	SVP and Chief Human Resources Officer, US Region; delegated to AVP Human Resources, US Region
Approved:	AVP Human Resources, US Region
Approval Date:	April 16, 2025
Next Review:	April 2026

Table of Contents

1.0 Summary and Intent

The Employee Privacy Statement - US Region ("Statement") describes how CIBC ("CIBC" or "we") collects, uses, discloses, and retains ("processes") personal information[1] about you before, during and after your working relationship with us in accordance with federal and state privacy laws.

This Statement applies to job applicants, current and former employees, and current and former contingent workers (collectively "employees" unless otherwise specified) whose primary place of employment is in the United States.

This Statement does not form part of any contract of employment or other contract to provide services. We may update this Statement at any time but if we do so, we will provide you with an updated copy of this Statement as soon as reasonably practical.

In circumstances where you are also a client of CIBC, information that we process that arises from that relationship is generally covered by CIBC's respective client privacy policy or policies, where applicable. However, where it is necessary for compliance with a legal obligation, such information may also be processed for the purposes of this Statement (e.g., monitoring trading activity or where we have reason to believe that there may be a breach of CIBC policies or procedures, any relevant contract, and/or applicable laws, or to otherwise comply with relevant laws or regulations).

2.0 Privacy Statement

2.1. Types of personal information CIBC processes

"Personal information" means any information about a person from which that person can be identified or that reveals something about a person, including information that is linked or can be linked to an individual.

We collect, store and use the following categories of personal information about you:

- Name, date of birth, gender, marital status, beneficiaries, identification numbers (including Social Security Number), and other identifying information;
- Contact information, such as home/mailing address, telephone number, cellular phone number, email address and emergency contact information;
- Demographic information such as age, marital status, gender;
- Background information, including education, training, work history and reference information, professional or other designations, eligibility to work in the US, and results from credit information and criminal record checks;
- Health and medical information, including emergency contact and health information of employees and their spouses and dependents;
- CIBC work history, experience, training, compensation information, and employment performance;
- Biometric information, such as a voiceprint or fingerprint, to enable identification and authentication based on behavioral and/or physical characteristics to allow access

[1] "Personal information" has the meaning provided in Section 2.1. of this Statement, unless referenced in accordance with a specific law or regulation, in which case the definition in that law or regulation applies.

to CIBC systems and facilities;

- Photographs and audio or visual recordings, such as workplace conversations (e.g., telephone conversations), business meetings, events, and/or training sessions, may be captured by CIBC for various reasons, such as to facilitate accurate information gathering, provide absent parties with access to meeting content, or respond to workplace accommodation needs;
- Protected characteristics such as race, ethnicity, sex life or sexual orientation as part of inclusion and diversity initiatives or as necessary to comply with applicable laws;
- Preferences such as hobbies and leisure activities, membership in voluntary/charitable/public organizations, and preferences such as those regarding work tools, travel, hours, and food for workplace events;
- Information posted on internal and external social networks, such as Workplace, Facebook, LinkedIn, etc. as described in the CIBC Code of Conduct (Code), Acceptable Use Policy for CIBC Information and Information Systems (AUP), and CIBC Social Media Policy.

2.2. Sources from which CIBC receives personal information

CIBC may obtain the categories of personal information listed, both directly and indirectly:

- Directly from you. For example, from forms you complete, benefit selections you may choose, or posts on work collaboration sites;
- Indirectly from you. For example, from observing your actions on CIBC website or information technology (IT) assets;
- From publicly available sources. Public records or widely available sources, including information from the media, and other records and information that are made available by federal, state, and local government entities. We also may collect personal information that you intentionally choose to make public, including via social media (e.g., we may collect information from public social media profile(s) to the extent individuals choose to make their profile(s) publicly visible and accessible);
- From business partners. For example, we may use third parties to run background checks as a condition of your employment or contract services; we may rely on professional employer organizations or staffing agencies for recruiting purpose; we may gather information about you, such as performance or evaluation information from a People Leader or other member(s) of management. We may combine information that we collect from different sources.

2.3. Purposes for which CIBC collects, uses, and discloses personal information

We process personal information about employees during various stages of CIBC's relationship with the employee in order to do any of the following:

- Conduct pre-employment screening (e.g., criminal record checks, credit checks, reference checks) and annual security screening for designated employees necessary for keeping CIBC systems and information secure and to meet regulatory requirements of the Office of the Superintendent of Financial Institutions (OSFI). Annual security screening includes a review of records relating to sanctions and politically exposed persons, court cases,

internal CIBC records, a financial check, and a criminal record check. Refer to the CIBC Security Screening Policy for further details;

- conduct internal investigations into suspected unlawful or inappropriate activity, including but not limited to theft, fraud, criminal activity, breach of an agreement, or allegation-based investigations of an employee's adherence to CIBC policies and applicable laws;
- Comply with applicable laws;
- Receive and process applications for employment;
- Establish, manage or terminate an employment relationship;
- Manage and promote CIBC's business and brand and community programs;
- Protect employees, CIBC, clients and other third parties from theft, fraud and similar risks;
- Conduct pre-employment screening (e.g., criminal record checks, credit checks, reference checks);
- Verify academic credentials and accreditations relevant to an employee's employment;
- Administer payroll and incentive compensation;
- Collect employment equity information in accordance with CIBC policies or procedures and applicable law;
- Relocate employees either domestically or internationally;
- Conduct exit interviews;
- Enroll in, administer and maintain CIBC benefit and pension plans and employee banking offers;
- Determine eligibility for benefits or support under various CIBC programs and policies;
- Adhere to various reporting requirements (e.g., income tax reporting);
- Monitor and disclose employee performance and results against business targets (e.g., sales results, call handling results);
- Monitor, document, and address adherence to regulatory compliance requirements, including, but limited to employee screening, vetting, and disclosures;
- Share letters of commendation or complaint;
- Manage attendance;
- Contact employees for business continuity purposes;
- Enable CIBC to instruct legal counsel;
- Safeguard the health, safety and welfare of employees;
- Monitor, document, and address adherence to CIBC's policies or procedures, any relevant contract(s) and/or applicable law;
- Develop, improve, deliver, and maintain employee learning and development programs;
- As described to you when collecting your personal information or as otherwise permitted by law;
- Any other reasonable purpose related to employment at CIBC or a contractual relationship to provide services to CIBC.

In addition, where we are considering selling or divesting all or part of the business in which an employee is employed, we may disclose information about employees to the potential purchaser

solely for purposes related to the transaction. CIBC and the potential purchaser will protect the information using security safeguards appropriate to the sensitivity of the information. If the transaction does not proceed, where permitted by law, CIBC will ensure that the information is returned or destroyed by the potential purchaser within a reasonable timeframe. If the transaction is completed, the purchaser may collect, use or disclose the information for the purposes for which the information was collected, permitted to be used or disclosed by CIBC before the transaction. Where required by law, CIBC or the purchaser will, within a reasonable time, notify the employee concerned that a transaction was completed and that their personal information had been disclosed to the purchaser.

2.4. What personal information is disclosed and to whom

We may disclose several categories of personal information to service providers for business purposes, such as IT administration, pre-employment screening, payroll, auditing, and consulting and other professional advising. These categories include:

- Identifiers;
- Demographic information;
- Professional or employment-related information;
- Health information;
- Internet or other similar network activity;
- Geolocation;
- Financial information;
- Characteristics of Protected Classifications under California or Federal Law for employees.

Personal information may also be shared with other third parties if we believe we must do so in order to comply with the law or to protect ourselves from legal liability or other risks. For example, we may share information in response to a court order or subpoena, or to a request made by a government agency or investigatory body, including U.S. and non-U.S. law enforcement or regulatory authorities. In addition to information we may provide about you in response to such legal orders or requirements, we may also freeze or turn over payroll funds to which you would otherwise be entitled, such as pursuant to a child support or wage garnishment order.

CIBC, its third-party service providers and other third parties to whom CIBC discloses information may perform activities outside of the United States. Any information that is used, stored or accessed in countries outside of the United States may be subject to the law of those countries (e.g., where a third-party service provider operates internationally). As a result, it is possible that information may be disclosed in response to valid demands or requests from law enforcement or other government authorities, courts, law enforcement, or other parties in countries outside of the United States.

2.5. How personal information is secured, retained and destroyed

We may store personal information in different ways such as on paper, electronic media, film and/or tape.

Personal information will be retained in accordance with the CIBC Records Management Policy and the applicable records retention schedule, and secured in accordance with Information/Cyber Security Risk Policy.

Certain types of personal information (e.g., tax records) will be retained for the requisite period as may be specified by applicable laws.

2.6. How to access personal information

In the absence of a legal requirement, we seek to promote access to your personal information. For employees other than contingent workers, much of this information is available directly through CIBC's Workday platform. Such employees should enter any changes to their personal information or personal circumstances in Workday (or the applicable HR system) as changes occur, to ensure that their HR records are current. We will not be responsible for any failure by you to keep your personal information current. Depending on your state of residence, CIBC may provide additional rights. CIBC does not maintain personnel files on contingent workers.

2.7. Monitoring

2.7.1. Monitoring Systems and the Workplace

CIBC monitors and records activity on our systems, resources and facilities for our business purposes and in order to assess or address adherence to our policies or procedures, including the AUP, Code, applicable contract(s), and/or applicable laws. This includes monitoring and/or recording activity related to computing devices, email, voicemail, telephone communications, mobile computing and remote access, internet use, including social networking and blogging, as well as all CIBC systems and facilities. To the extent that you associate with or reference CIBC in your personal use of social media, we may collect your personal information as part of monitoring the internet for references to the CIBC brand and employee compliance with the Social Media Policy.

CIBC may also monitor employees in specific job functions as required or permitted by law. For example, CIBC may monitor calls of US broker dealers or swap associated persons for purposes such as identifying client and internal service issues; providing training; and/or confirming discussions. CIBC provides employees notice of such monitoring through this Statement, role-based training, and in the client agreements that disclose how conversations between CIBC regulated employees and clients are recorded. For more information, see Recording Telephone Conversations Standard.

Finally, during the course of daily business, CIBC employees may create recordings in order to facilitate collaboration, such as the recording of Teams meetings or training sessions that can be referenced at a later date. In such cases, the meeting host typically notifies the participants of their intent to record and proceeds to record absent an objection, and tools used typically provide visual cues that a meeting is being recorded. Teams provides notice and a red icon indicates that a meeting is being recorded. Teams recordings are typically retained 45 days and then expired, unless they are being preserved as a business record in accordance with established records retention schedule.

Where abuse, fraud, or breaches of CIBC policy, procedures, any relevant contract(s) and/or applicable laws is suspected, we may investigate and have the right to access any relevant personal information, including data stored within CIBC systems and communication channels.

We may also monitor or access areas within the workplace (including offices, desks and filing cabinets) to:

- facilitate the operation of CIBC's businesses;
- enable security audits;
- protect individuals, third parties, and CIBC's property and interests.

If you contravene the Social Media Policy, Code, or the AUP, or underlying laws and regulations, you may be subject to disciplinary action up to and including termination of employment for cause without notice, or pay in lieu of notice, as well as possible civil, criminal or regulatory action. Such conduct may also affect your individual performance assessments and compensation.

2.7.2. Employee Investigations

In the event that you report potential violations of CIBC policy or law, such as harassment or concerns regarding financial reporting, CIBC takes steps to protect your anonymity and the confidentiality of the concerns you report to CIBC, to the extent possible, including:

- Strictly limiting access to all information reported;
- Ensuring information received is handled and investigated by appropriate employees;
- Securely storing all paper and electronic documents and other materials;
- Limiting the dissemination of personal information as much as possible (for example, redaction);
- Ensuring all employees, including those involved in handling and investigating information received, are bound by CIBC's Code and policies on confidentiality.

In certain cases, CIBC may disclose information including your identity (or information that could reasonably be expected to reveal their identity) as the reporter of a concern to a regulator or law enforcement agency, if such a disclosure is necessary for purposes related to an investigation. In addition, the regulator or law enforcement agency may in turn disclose information disclosed by CIBC to each other.

2.7.3. Monitoring Personal Trading Activity

If you are covered by CIBC's personal trading policies[2], you are subject to monitoring of personal trading activity in respect of securities. The purpose of this monitoring is to ensure compliance with CIBC policies and procedures, relevant contract(s) and/or applicable laws. The trading accounts of your spouse or immediate family members that reside with you may also be monitored for compliance purposes.

2.8. General Questions

If you have questions, please contact your human resources representative or the CIBC HR Contact Centre (HRCC) at 800-668-0918. Job applicants may contact mailbox.careers-carrieres@cibc.com. Contingent workers should contact their employer.

2.9. Additional information

2.9.1. California residents

Employees who are California residents may refer to the CCPA Privacy Notice for prospective and current employees, which may be found at https://us.cibc.com/en/about-us/california-

[2] CIBC governance of personal trading activities is outline in the following policies: CIBC Code of Conduct, US Region Insider Trading Policy, US Capital Markets Personal Trading Policy (US), and CIBC Private Wealth Group, LLC Code of Ethics (US).

consumer-privacy-act-employment.html, for additional information as required under applicable California law.

2.9.2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that CIBC maintain the privacy of your protected health information. HIPAA does not apply to health-related information that is maintained in employment records. However, HIPAA applies to your medical or health plan records if you are a member of a CIBC health plan. Please contact the CIBC HR Contact Center at 1-800-668-0918 with questions regarding your medical or health plan records.

3.0 Questions

Questions regarding medical or health plan records should be addressed to the CIBC HR Contact Center at 1-800-668-0918.

Questions about CIBC privacy practices should be addressed to the US Privacy Office at USPrivacyOffice@cibc.com.