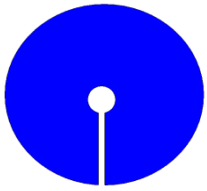

SBI Canada Bank

Privacy Policy

Owner:	Privacy Officer
Version:	2.2
Approving Body:	Board
Date Approved:	August 30, 2016
List of Recipients:	All Staff

Introduction

1. All banks in Canada are subject to *Personal Information Protection and Electronic Documents Act* (PIPEDA), hereinafter referred to as PIPEDA" and the "Act". This Act supports and promotes electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions.

   In this context

   - "*Personal Information*" means information about an identifiable individual.
   - "Electronic Document" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data.

   PIPEDA has two parts. The first part of the Act, *Protection of Personal Information in the Private Sector*, establishes rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. This Part applies to every organization in respect of personal information that

   a) the organization collects, uses or discloses in the course of commercial activities; or

   b) is about an employee[1] of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

   The second part of the Act, *Electronic Documents*, provides for the use of electronic alternatives in the manner provided for in this Part where federal laws contemplate the use of paper to record or communicate information or transactions.

   The Digital Privacy Act, proclaimed on June 18, 2015, has introduced several changes in PIPEDA. All new measures defined under the Digital Privacy Act, except for the data breach

[1] This Part does not apply to an organization in respect of the business contact information of an individual that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession.

notification requirements[2], are in force as of the issuance of this Policy and have been taken into consideration in this Policy.

The *Office of the Privacy Commissioner of Canada (OPC)* has also issued several guidelines and interpretation bulletins that convey OPC's expectations of banks regarding compliance with PIPEDA.

This Privacy Policy (the "Policy") defines the enterprise-wide approach adopted by SBI Canada Bank, hereinafter referred to as "SBIC" and the "Bank", for complying with PIPEDA as well as guidelines and interpretation bulletins issued by OPC.

Scope of this Policy

2. This Policy applies to all directors, senior management, and employees of the Bank.

3. This Policy shall be read in conjunction with the other compliance-related policies and procedures issued by the Bank, especially the *Legislative Compliance Management Policy* and related procedures.

4. The Bank defines compliance with the policies and procedures of the Bank as well as the legal and regulatory requirements applicable to the Bank as a responsibility of every employee of the Bank.

5. A breach of this Policy by an officer or employee of the Bank might result in disciplinary action that could lead to dismissal.

6. This Policy is subject to review and approval by the Board every two years.

Protection of Personal Information

7. PIPEDA applies to the Bank in respect of the following types of personal information:

   a. Personal Information that the Bank collects, uses, or discloses in the course of commercial activities; or

   b. Personal Information about employees of the Bank that the Bank collects, uses or discloses in connection with its operations.

8. The Bank is required to comply with the following ten Privacy Principles as set out in Schedule 1 of PIPEDA.

   Principle 1. Accountability

[2] The Bank may issue revised/additional procedures, as deemed appropriate by the Privacy Officer of the Bank, to implement the Breach Notification requirements, as they come into force. The new requirements pertaining to Breach Notification will be incorporated in this Policy at the time of the next revision.

Principle 2. Identifying Purposes

Principle 3. Consent

Principle 4. Limiting Collection

Principle 5. Limiting Use, Disclosure, and Retention

Principle 6. Accuracy

Principle 7. Safeguard

Principle 8. Openness

Principle 9. Individual Access

Principle 10. Challenging Compliance

9. SBIC shall also take appropriate steps in the event of a privacy breach. This includes taking measures to contain the breach; evaluating the risks associated with the breach; notifying the affected parties, if required; and implementing preventative solutions.

Privacy Management Program at SBIC

Accountability

10. SBIC is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The Bank shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

11. The Privacy Officer is responsible for establishing and managing compliance with the Privacy requirements applicable to the Bank. The contact details of the Privacy Officer are made available on the website of the Bank and provided to clients upon request.

12. The role and responsibilities of the Privacy Officer are defined in the mandate of the Privacy Officer. The mandate is approved by the Audit Committee of the Board.

13. The Bank, with the authorization of Audit Committee of the Board, may delegate other individuals to act on behalf of Privacy Officer.

14. Each employee of the Bank is responsible for complying with this Policy and protecting the personal information under his/her control.

15. The Bank provides training to all staff members and senior management to ensure compliance with the Privacy requirements. The training is provided through in-person training sessions or through the computer-based training system used by the Bank.

Identifying Purposes

16. The Bank identifies the purpose for collecting personal information at or before the time of collection.

17. The purpose of obtaining clients' personal information shall be defined in the respective "Approach Paper" or product program. In this regard, the Bank has issued a Product Development Policy. This policy defines the process used by the Bank for introducing new products and services and making changes to its existing products and services.

18. If it is not feasible to provide written notice in advance, the individual can be notified orally. In such cases, prior approval from the Privacy Officer of the Bank shall be obtained by the respective business function head.

19. The personal information collected by the Bank shall only be used for the identified purposes.

20. If personal information that has been collected is to be used for a purpose not previously identified, the Bank shall identify the new purpose prior to using the information.

Consent

21. As defined in the Act, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use or disclosure of the personal information to which they are consenting. The Bank shall use simple and clear language[3] for the purpose of seeking consent from clients to ensure that the consent provided by the client meets the validity criteria as defined in the Act.

22. The Bank notifies and seeks consent from the individual about whom the personal information is collected at or before the time of collection, except under certain circumstances as exempted under the Act

23. The Bank prefers to notify clients about the purpose of collecting, using, and disclosing personal information and seeking consent from the clients in writing. In this regard, an application form is deemed to provide notice of the purpose.

24. The Bank shall use only standard forms for collecting personal information required for providing products and services to clients. All client forms and applications used by the Bank shall be pre-approved by the Privacy Officer of the Bank.

25. The Bank may seek consent orally when information is collected over the phone, provided that the information is required to provide services or products required by the client or is

[3] The Bank has implemented a *Clear Language Policy* to ensure that public disclosure statements and client directed communications are presented in clear, simple and plain language.

required for keeping the clients' record up to date, in accordance with the legislative and regulatory requirements that apply to the Bank. These requirements are collectively referred to as the "applicable requirements" in this Policy.

26. If the Bank wishes to collect personal information of clients for marketing and research purposes or for any other specific purpose, prior approval from the Privacy Officer of the Bank shall be obtained by the respective business function head.

27. In accordance with Section 7 and Schedule 1 of the Act, the Bank may collect use, or disclose personal information without the knowledge and consent of the individual under certain circumstances as exempted under the Act. This includes circumstances where seeking consent is impossible or impractical due to legal, medical, or security reasons; where information is being collected and or disclosed for the detection and prevention of fraud or for law enforcement; and when the individual is a minor, seriously ill, or mentally incapacitated. In such events, the Bank shall take reasonable measures to ensure that the collection, use, or disclosure is made in accordance with the exceptions provided in the Act. In this context, reasonable measures include but are not limited to conducting and documenting a review of the exceptions provided under the Act, referring the matter to the Privacy Officer of the Bank, or referring the matter to an external law firm.

28. If personal information that has been collected earlier is to be used for a purpose not previously identified, the Bank shall seek consent form the individual prior to using the information for the new purpose. This does not apply if the new purpose is required by law.

29. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. SBIC will not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

30. The Bank will not obtain consent through deception.

31. The Bank will allow its clients and employees to withdraw their consent subject to legal or contractual restrictions and reasonable notice. If a client or an employee withdraws his/her consent, the Bank will inform them about the implication of such withdrawal.

Limited Collection

32. The Bank shall only collect personal information that is essentially required. In this context, essentially required information refers to the set of information that is required by the Bank to provide the product or service required by the clients, perform its functions, and comply with the applicable requirements.

33. The details of personal information that is required to provide any product or service shall be provided in the respective Approach Paper.

34. SBIC will collect personal information by fair and lawful means.

Limiting Use, Disclosure, and Retention

35. The Bank will not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required/permitted by law.

36. The Bank shall retain personal information only as long as necessary for the fulfillment of the identified purposes. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made.

37. The Bank shall retain personal information that is/was the subject of an Access Request as long as necessary for the individual making the request to exhaust any recourse provided by law. Upon receipt of an access request, staff responsible for retention or disposal of relevant records shall ensure that all relevant records are removed from any standard or routine disposal cycles and not destroyed or otherwise disposed of.

38. Personal information that is no longer required to fulfill the identified purposes shall be destroyed, erased, or made anonymous by the Bank. This shall be applied in compliance with the legislative requirements pertaining to record keeping as well as the Record Management Policy and other policies and procedures issued by the Bank.

Disclosure of Information to External Parties

39. From time to time, the Bank might use certain services provided by the Parent Bank and/or external service providers, operating within and outside Canada. Therefore, the Bank might transfer certain personal information of clients as well as employees to the Parent Bank and external service providers. In such cases, the information that is transferred by the Bank is only used for the purpose for which it was originally collected. The outsourcing arrangements made by the Bank shall be in accordance with PIPEDA as well as guidelines issued by the OPC and *Office of the Superintendent of Financial Institutions* (OSFI). The Bank shall use service level agreements (SLA) to ensure that a comparable level of protection is provided when personal information is transferred by the Bank. The Bank might also receive information from the Parent Bank or external service providers as part of the services provided by them. The personal information transferred to another jurisdiction might be accessed by the courts as well as law enforcement and national security authorities of that jurisdiction.

40. The Bank might be served with a production order or receive a request for information from a law enforcement agency, any other government institution such as the Canada Revenue Agency (CRA), or part of a government institution. Before providing the requested information in any such event, the Bank shall ensure that the disclosure is made in accordance with PIPEDA Section 7.(3) and is required for the following purposes:

    a. To comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

b. Made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated the following:

   i. It suspects that the information relates to national security, the defense of Canada or the conduct of international affairs,

   ii. The disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

   iii. The disclosure is requested for the purpose of administering any law of Canada or a province.

41. Before disclosing the requested information, the Bank shall satisfy itself with the genuineness of the production order or the lawful authority of a request for information made by an individual representing a law enforcement agency, any other government institution, or part of a government institution.

42. If the Bank has a reasonable doubt about the genuineness of a production order or lawful authority of a request for information, the matter shall be immediately reported to the Privacy Officer of the Bank. If required, the Privacy Officer might discuss the matter with the RMC and/or recommend the Bank to obtain a legal opinion on whether or not the Bank shall provide the requested information.

43. No information shall be released without obtaining prior approval from the Privacy Officer of the Bank in the following situations:

    a. The Bank has a reasonable doubt about the genuineness or lawful authority of a request for information, or

    b. The request for information was made by an external party such as a law firm.

Accuracy

44. The Bank shall make reasonable efforts to ensure that personal information collected, used, or disclosed by it is accurate, complete, and current. In this context, making reasonable efforts include obtaining the information from the individual.

45. The Bank will not routinely update personal information, unless it is required to update the information to fulfill the purposes for which the information was collected or it is required by law.

46. To ensure accuracy of information, the Bank might also take measures to validate the information provided by client or employees by verifying it with information under its control and information that is publically and /or commercially available.

Safeguards

47. The Bank is responsible for implementing security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

48. The Bank collects and maintains personal information in paper as well as electronic/digital format and has implemented various security safeguards to protect it.

49. The Bank has implemented physical measures to restrict access to its offices and physical records maintained at various locations. In this regards, access cards are required to access various areas of the Bank and physical records are maintained in locked filing cabinets.

50. All staff members are responsible for safeguarding the access cards and key(s) provided to them by the Bank, protecting them from theft or loss, and promptly reporting any lost or stolen key or card to their immediate supervisor as well as to the persons responsible for issuing access cards and keys.

51. The Bank provides certain information or provides access to certain information to all staff members of the Bank to enable them to perform their day-to-day activities. This includes personal information of clients and other staff members as well as information about the processes used by the Bank. The Bank requires all staff members to sign a confidentially agreement at the time of their employment. All staff members shall treat the information provided to them by the Bank as confidential and share it only with other staff members of the Bank on a need-to-know basis.

52. All staff members of the Bank are required to ensure that physical records under their custody are duly protected. Sensitive information shall not be left unattended during the day and shall be locked in filing cabinets at the end of each day.

53. The Bank has implemented technological controls to protect the digital information collected by it. These controls are defined in the *Information Technology and Information Security Policy* of the Bank. All staff members of the Bank are required to comply with the *Information Technology and Information Security Policy* of the Bank and ensure that computer terminals and laptops provided to them by the Bank are secured with passwords and digital records under their custody is duly protected.

54. The Bank will use contractual or other means to provide a comparable level of protection when personal information is transferred or shared by the Bank with the Parent Bank or an external service provider. This includes measures to taken by both parties during the process of transferring/sharing of the information, on an ongoing basis during the term of the agreement, and upon termination of the agreement.

Openness

55. The Bank will make readily available its policies and practices relating to the management of personal information. The Bank is required to provide this information in a form that is generally understandable.

56. The Privacy Officer of the Bank may issue a privacy statement in a simple and clear language for the purpose of providing a generic overview of the privacy process adopted by the Bank to the clients. This statement shall include the following details:

    a. The title and the office address of the Privacy Officer of the Bank who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

    b. The means of gaining access to personal information held by the Bank;

    c. A description of the type of personal information held by the Bank, including a general account of its use;

    d. A copy of any brochures or other information that explain the organization's policies, standards, or codes; and

    e. Type of personal information that is generally disclosed by the Bank to affiliated entities and service providers for the purpose of providing services to clients.

57. The Privacy Officer will address specific requests about the privacy related processes adopted by the Bank on a case-by-case basis.

Individual Access

58. The Bank will inform an individual, upon receiving a written request, of the existence, use, and disclosure of his or her personal information and will provide access to that information. This includes providing information about the use that has been made or is being made of the client's information and list of third parties to which it has been disclosed.

59. The Bank will respond to an individual's written request within thirty days after the receipt of the request at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable.

60. In accordance with PIPEDA, the Bank may extend the time limit for a maximum of thirty days if meeting the time limit would unreasonably interfere with the activities of the Bank or the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet. The Bank may also extend the limit for the period that is necessary in order to be able to convert the personal information into an alternative format.

61. If the Bank extends the time limit for responding to a request, the Bank shall, no later than thirty days after the date of the request, send a notice of extension to the individual, advising

them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the OPC in respect of the extension. If the Bank fails to respond within thirty days, the Bank is deemed to have refused the request.

62. The Bank shall respond to requests involving information provided by the Bank to a government institution or a part of a government institution in accordance with sub-section 9. (2.1) of PIPEDA.

63. The Bank may respond to an individual's request at a cost to the individual only if the Bank has informed the individual of the approximate cost and the individual has advised the Bank that the request is not being withdrawn.

64. The Bank will give access to personal information in an alternative format to an individual with a sensory disability who has a right of access to personal information and who requests that it be transmitted in the alternative format if its conversion into that format is reasonable and necessary in order for the individual to be able to exercise rights defined in PIPEDA. The Bank does not readily maintain information in alternative format.

65. In accordance with section 9. (1) of PIPEDA, the Bank will not give an individual access to personal information if doing so would likely reveal personal information about a third party, unless the information about the third party is severable.

66. An individual can challenge the accuracy and completeness of the information provided to him/her by the Bank and have it amended as appropriate.

67. The Bank will take appropriate measures if an individual successfully demonstrates the inaccuracy or incompleteness of personal information held by the Bank. Depending upon the nature of the information challenged, the Bank will amend, make correction, delete, or add information in its records. If required, the amended information will be provided to affiliated entities and service providers having access to the same information.

Access Request about information disclosed to a government institution

68. An individual might request the Bank to inform or give the individual access to the individual about the following types of information:

    a. Disclosure of information to a government institution or a part of a government institution;

    b. The existence of any information that the organization has relating to a disclosure to a subpoena, warrant or order; or

    c. A request made by a government institution or a part of a government institution.

69. The Bank will take the following steps if a request is received for access to any type of information mentioned above:

a. Notify the concerned institution or part in writing about the access request made by the individual without delay, and

b. Respond to the request only after receiving a notification from the concerned institution or part whether or not the institution or part objects to the organization complying with the request. The government institutions or part are required to provide such notification within thirty days after the day on which it is notified.

70. If the Bank is notified that the institution or part objects to providing the requested information to the individual, the Bank will take the following steps:

a. Refuse the request to the extent that it relates to information referred above;

b. Notify the Office of the Privacy Commissioner of Canada (OPC) in writing without delay about the refusal; and

c. Not disclose any of the following information to the individual.

i. The information that the Bank has relating to a disclosure to a government institution or a part of a government institution,

ii. The notification provided by the Bank to the institution or part or the Commissioner, and

iii. The institution or part objection to providing requested information to the individual.

71. The Bank will not respond to such access request before the earlier of the day on which it is notified by the concerned institution or part and thirty days after the day on which the institution or part was notified.

Refusal to provide access

72. In addition to the information referred to in the previous section of this Policy, the Bank is also not required to give access to personal information in the following circumstances:

a. Providing access to requested information would reveal confidential commercial information;

b. Providing access to requested information would reasonably be expected to threaten the life or security of another individual;

c. The information was collected under a provision provided in PIPEDA that allows collection without knowledge or consent of the individual; or

d. The information was generated in the course of a formal dispute resolution process.

73. If the information mentioned in paragraph 65 and 72 of this Policy is severable from the record containing other information for which access is requested, the Bank will give access after severing the information mentioned in paragraph 65 and 72.

74. The exceptions mentioned in the previous paragraph do not apply if the individual needs the information because the individual's life, health, or security is threatened.

75. If the Bank is not able to provide access to all the personal information it holds about an individual, due to an exception as defined in PIPEDA, the reasons for denying access shall be provided to the individual. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

76. If the Bank decides not to give access to personal information under circumstances as defined in this Policy, the Bank will notify OPC in writing. Such notifications will include any information that the OPC may specify.

Challenging Compliance

77. Any individual can challenge Bank's compliance with PIPEDA by writing to the Privacy Officer of the Bank. The Bank has issued a Compliant Resolution Brochure that provides the contact details of the Privacy Officer of the Bank as well as the contact details of the OPC.

78. The Privacy Officer of the Bank can be contacted by mail or email at the following addresses:

    Privacy Officer

    SBI Canada Bank

    Suite 106, 77 City Centre Drive

    Mississauga, ON. L5B 1M5

    Facsimile: 905-896-6545

    Privacy.Officer@sbicanada.com

79. The Privacy Officer shall investigate all privacy-related complaints. If a complaint is found to be justified, the Privacy Officer shall make recommendations to the concerned function of the Bank to take measures, as deemed appropriate by the Privacy Officer and P&CEO of the Bank.

80. The Bank might be served with notice of a complaint or investigation by OPC. In such an event, the Bank shall comply with Privacy Commissioner's lawful exercise of authority.

81. The Bank shall also not obstruct or knowingly mislead the Privacy Commissioner or retaliate against a whistle blower acting in good faith.

Privacy Breaches

82. A privacy breach is defined as unauthorized access to or collection, use, or disclosure of personal information. In the context of this Policy, it refers to unauthorized access to or collection, use, or disclosure of personal information of clients or an employee of the Bank that was collected and maintained by the Bank.

83. The term “Employee Snooping” refers to unauthorized access to personal information held by an organization by its own employees. SBIC expects its employees to access, use, and/or disclose personal and/or confidential information held by the Bank on a strict “need to know basis” and only at times that information is required for legitimate business purposes. This includes but is not limited to the personal information of clients as well as employees of the Bank. To safeguard personal and confidential information, SBIC can take appropriate measures including those aimed at identifying cases of snooping by way of monitoring employees’ activity. Any unauthorized or unlawful access by employees to the personal or confidential information held by the Bank might result in disciplinary action, including termination of employment.

84. The Privacy Officer of the Bank will be the primary point of contact for all breaches or suspected breaches, including incidents of employee snooping.

85. Upon notification or identification of a breach or a suspected breach, the matter shall be immediately reported to the Privacy Officer of the Bank. The Privacy Officer will subsequently notify the Risk Management Committee (RMC) of the Bank and the Audit Committee of the Board (ACB).

86. The concerned branch/corporate function head will take appropriate action to contain the breach and inform the Privacy Officer about the measure taken in this regard. The Privacy Officer might suggest additional measures, as deemed appropriate.

87. After ensuring that appropriate measures have been taken by the concerned branch/corporate function to contain the breach, the Privacy Officer will do a preliminary assessment of the breach and provide initial recommendations to the RMC on further measures that shall be taken by Bank for determining the extent of breach, evaluating the risks associated with the breach, notifying the affected parties, and taking measures for prevention of future breaches. Based on the initial assessment, the Privacy Officer might also recommend assembling a team for conducting a detailed investigation.

    The Privacy Officer will provide a copy of the guideline issued by OPC, “*Key Steps for Organizations in Responding to Privacy Breaches*” along with his/her recommendations to the RMC. The RMC will consider the above mentioned OPC guidelines while reviewing the recommendations provided by the Privacy Officer and will determine the next steps to be taken by the Bank in case of privacy breach.