

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### Purpose

1. To ensure that the National Capital Commission (NCC) fulfills its obligations under the [Privacy Act](#) (PA).

### Policy Statements

1. Individuals shall have access to all of their [personal information](#) held by the NCC subject to the [exemptions](#) and [exclusions](#) listed in the PA. The NCC shall adhere to legislative deadlines in processing formal requests for personal information.
2. Personal information [may be disclosed informally](#) when there is an established practice that respects the PA.
3. Personal information shall be collected by the NCC only when it has [parliamentary authority](#) to do so. In addition, the NCC shall only collect the minimum personal information required to achieve the purpose.
4. Personal information shall be protected and, unless prior consent is given by the individual concerned, shall be used or disclosed only for the purpose for which it was collected, or for a purpose consistent with the original purpose, or for a purpose authorized under [sub-section 8\(2\)](#) of the PA.
5. Except where an individual consents to an earlier disposal, personal information shall be kept for a minimum of two years after the last time it was [used for an administrative purpose](#).
6. The NCC shall take reasonable steps to ensure that personal information held by the NCC is accurate and as up-to-date as possible.
7. The NCC shall limit the collection, use and disclosure of the social insurance number (SIN), either for [administrative or non-administrative purposes](#), to those authorized by statutes or regulations and for administering pensions, income tax, health and social programs. The NCC shall not withhold any right, benefit or privilege nor impose any penalty by reason of an individual's refusal to disclose the SIN except for the authorized uses.
8. The NCC shall manage any [data matching](#) of personal information according to the Treasury Board of Canada Secretariat (TBS) [Policy on Privacy Protection](#).
9. All personal information holdings at the NCC shall be described as much as possible in the [personal information banks](#). The information in these banks shall be updated every year.
10. The NCC shall ensure that appropriate privacy protection clauses are included in contracts or agreements when contracting, and establishing agreements or arrangements with private sector organizations, public sector organizations or other government entities.
11. The NCC shall establish necessary directives, protocols or guidelines to ensure that the NCC fulfills its obligations under the PA or meets TBS requirements, and that these are disseminated to all employees.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### Authorities

#### Executive Management Committee (EMC)

- APPROVE the Privacy Policy.

#### General Counsel and Commission Secretary

- RECOMMEND approval of the Privacy Policy.
- APPROVE the Privacy Procedures.

### Roles and Responsibilities:

#### Chairperson of the National Capital Commission (NCC) – Head for the *Privacy Act*.

- RESPONSIBLE for the administration of, and compliance with, the *Privacy Act*.
- DELEGATES authorities, responsibility, duties, and functions under the *Privacy Act*.

#### Chief Executive Officer of the NCC

- RESPONSIBLE for the administration of, and compliance with, the *Privacy Act*, as delegated.

#### Vice President, Public, Legal and Corporate Affairs

- RESPONSIBLE for the administration of, and compliance with, the *Privacy Act*, and policies as delegated.

#### Vice President Corporate Services (Chief Security Officer)

- RESPONSIBLE for ensuring compliance with the Policy on Government Security and the Policy on Privacy Protection.

#### Chief, Access to Information and Privacy (ATIP)

- RESPONSIBLE for the administration of, and compliance with, the *Privacy Act*, as delegated.
- DEVELOP and IMPLEMENT the Privacy Policy and Procedures.
- ACT as the ATIP coordinator.
- ENSURE that the Privacy Policy and Procedures are complete, current, and available in both official languages.
- ENSURE adherence to the Privacy Policy, *Privacy Act* (PA), and procedures.
- PROVIDE personal information to individuals on request. APPLY exemptions and exclusions when required, as prescribed in the PA.
- ENSURE that legislative deadlines are met.
- REPRESENT the NCC during the investigation of complaints by the Office of the Privacy Commissioner of Canada (OPC) and in the Federal Court when requests for review are submitted.
- PROVIDE training, advice, and guidance to NCC management and staff on all aspects of the PA.
- MONITOR and REPORT on the NCC's compliance with this policy and the PA to General Counsel.
- PREPARE the annual report on the administration of the PA within the NCC for tabling in Parliament.
- MAINTAIN and MONITOR a reading area for individuals to review their personal files.
- PROVIDE advice and recommendations to ensure NCC conformity with the PA and TBS directives.
- DETERMINE if a new or amended Personal Information Bank (PIB) is required for a new collection, use, or disclosure of personal information and for registering the bank with the Treasury Board of Canada Secretariat.
- RESPONSIBLE for the annual update of the NCC personal information banks, and Classes of Records that are included in NCC's Info Source Chapter on the internet.
- CONFIRM if a privacy impact assessment (PIA) is required and APPROVE the PIA.
- RESPONSIBLE for signing off on the PIA and to send it to the Office of the Privacy Commissioner (OPC) and to the Treasury Board of Canada Secretariat (TBS) as required.
- FOLLOW up with Offices of Primary Interest (Branches) up on any changes.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

- CONFIRM if a Privacy Breach has occurred and determines if the breach is material or minor.
- ENSURE that material breaches are communicated as soon as possible to the:
  - Chief Security Officer
  - NCC chairperson through the delegation line of authority.
  - Treasury Board of Canada Secretariat
  - Office of the Privacy Commissioner
- ENSURE that proper privacy breach protocol and mitigation measures are put in place by the Offices of Primary Interest (OPI)
- ENSURE that recommendations following a privacy breach have been implemented by the OPIs.
- DEVELOP and IMPLEMENT any policy/directive/protocol/guidelines required by the PA or by the Treasury Board of Canada Secretariat.

### **Chief, Management and Security of Information**

- ENSURE proper retention schedules for personal information are applied and disposition activities are performed regularly as agreed in the retention schedule procedures.
- ENSURE THE PROTECTION of personal information held in official corporate repositories.
- Provide awareness and guidance on protection of personal information held in other NCC computer applications.
- Responsible for planning, coordinating, and supervising all activities related to the NCC's Retention and Disposition Program and for managing the life cycle of all NCC corporate information on all mediums.

### **Staff responsible for Computer applications**

- RESPONSIBLE for performing regular disposition of personal information contained in the computer application under their control in accordance with MSI directives.
- RESPONSIBLE for THE PROTECTION of personal information contained in the computer databases under their control.

### **Manager, Corporate Security and Deputy Chief Security Officer**

- SHARED responsibility with the ATIP Coordinator regarding ensuring that proper, and easily accessible, Privacy Breach protocols and mitigation measures are put in place by the Offices of Primary Interest (OPI) for security incidents that involve the compromise of Personal Information.
- INVESTIGATE any reported security incidents related to physical files or to physical information technology equipment.

### **Manager, Information technology Security**

- INVESTIGATE any reported Information Technology Systems and Database incidents related to personal information, and briefs the chief, ATIP and to the Chief Information Officer.

### **Legal Services**

- PROVIDE legal advice relating to the legal authority to collect personal information.
- PROVIDE legal advice on the *Privacy Act*.
- USE of personal information in the context of claims and litigation.

### **Branch Heads**

- ENSURE conformity with the *Privacy Act* and with the CAPP within their area of responsibility.
- ENSURE that all their employees have completed any mandatory ATIP training.
- ENSURE that any project which may affect the collection, use or disclosure of personal information is brought to the attention of the chief, ATIP, to determine if a PIA is required, in conformity with TBS directives.
- ENSURE that PIAs are initiated and completed for new programs and for substantially modified

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

- programs in their area of responsibility.
- ENSURE that for all existing programs, where no PIA was done, that to the extent possible, privacy risks are identified and are appropriately addressed.
- RESPONSIBLE for signing off on PIAs in their area of responsibility.

### **ATIP Branch Liaison Officers**

- COORDINATE the Branch response to requests for personal information.
- ENSURE that deadlines for processing requests for personal information are respected.
- COORDINATE ATIP activities within their branch.

### **Managers and Directors**

- ENSURE conformity with the PA, CAPP and any privacy directive, protocol, or guideline within their area of responsibility.
- IDENTIFY and REVIEW all records relevant to requests for personal information.
- PROVIDE recommendations regarding disclosure or protection of requested information.
- ENSURE that deadlines for processing requests for personal information are respected.
- NOTIFY the chief, ATIP, of any change that may affect the collection, use or disclosure of personal information and COMPLETE a PIA if recommended by the chief, ATIP. This applies to, but is not limited to, new or updated software or new program initiatives.
- NOTIFY the chief, ATIP immediately when an unauthorized disclosure of personal information occurs and ensure containment and mitigation of the breach.
- FOLLOW up on the measures taken to contain and to mitigate the breach.
- NOTIFY the branch head when there is a material privacy breach.

### **Employees**

- TAKE reasonable measures to ensure adequate protection of the personal information that they have access to in the course of their duties.
- COMPLETE any mandatory ATIP training organized by the ATIP office.
- ATTEND privacy awareness sessions organized by the ATIP office.
- CONTAIN any unauthorized disclosure of personal information and REPORT the breach immediately to their manager.

### **References**

[Privacy Act](#)

[Privacy Regulations](#)

[Canadian Charter of Rights and Freedoms](#)

[Policy on Privacy Protection](#)

[Directive on Privacy Practices](#)

[Information Security CAPP](#)

[Information Holdings Management CAPP](#)

[Delegation Order - Privacy Act](#)

[Guidelines for Privacy Breaches](#)

[Privacy Breach Management Toolkit](#)

[Directive on Privacy Impact Assessment](#)

[Directive on Privacy Requests and Correction of Personal Information](#)

[Directive on Social Insurance Number](#)

[Standard on Privacy and Web Analytics](#)

[Policy on Government Security](#)

### **Procedures**

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### 1. Processing formal requests for personal information

ATIP Analyst	1. CLARIFY the request, if necessary. SEND an acknowledgement to the applicant. FORWARD the wording of the request, without providing any details about the applicant, to the appropriate ATIP branch representative. In case of employee requests, the ATIP analyst will retrieve the records directly from the holder of the information, if practically possible, to ensure minimal invasion of privacy.
ATIP Branch Liaison Officer	2. REFER the request to the appropriate manager(s) only (need-to-know basis), to ensure minimal dissemination of personal information. FOLLOW UP as required to ensure that the six-working-day deadline is met.
Manager	3. LOCATE relevant records. REVIEW records and IDENTIFY any concerns with the release of specific information.
	3.1 In the case of records related to a disclosure made pursuant to the <i>Public Servants Disclosure Protection Act</i> , the audit director will sequester the records and exercise his/her delegated authority to withhold them.
	4. PREPARE records package, including the branch recommendations, and TRANSMIT to the ATIP liaison officer or directly to the ATIP office when instructed to do so (requests by employees).
ATIP Branch Liaison Officer	5. SUBMIT the records package to the director (at a minimum) for approval. PREPARE the package, including the branch recommendations, and TRANSMIT to the ATIP analyst once approved.
ATIP Delegated Officer	6. REVIEW documents, while taking the branch comments into consideration, and APPLY exemptions and exclusions, if required. CONSULT other organizations when necessary, and NOTIFY the applicant if an extension of deadline is required.
	7. PREPARE the records for release and SEND the response to the applicant. CLOSE the request file.

### 2. Consultations from other organizations

Chief, ATIP	1. FORWARD the documents received from another organization to the appropriate ATIP branch liaison officer.
ATIP Branch Liaison Officer	2. REFER the documents to the appropriate manager for review. FOLLOW UP as required to ensure that the six-working-day deadline is met.
Manager	3. REVIEW the documents, and IDENTIFY any concerns with the release of specific information.
ATIP Branch Liaison Officer	4. TRANSMIT the branch recommendations to the ATIP analyst.
ATIP Delegated Officer	5. REVIEW the documents, while taking the branch comments into consideration. PREPARE a reply and SEND it to the organization concerned.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### 3. Processing formal requests for correction

ATIP Analyst	1. FORWARD the request to the appropriate ATIP branch liaison officer.
ATIP Branch Liaison Officer	2. REFER the request to the appropriate manager. FOLLOW UP as required to ensure that the six-working-day deadline is met.
Manager	3. CONSIDER the request, and DETERMINE if the correction is appropriate.
	4. <b><u>If it is accepted:</u></b> AMEND the record.  PREPARE memo informing the Chief, ATIP, that the record was corrected. Include a copy of the corrected information and provide the list of persons/organizations (internally and externally) with whom / with which the information was shared.  NOTIFY the persons /organizations on the list of the correction.
	4.1 <b><u>If it is accepted but the information cannot be modified:</u></b> (for example, because of the format)  ATTACH a notation to the personal information indicating that a request for correction was made and accepted (notation should be visible when consulting the erroneous information). Also include the reason why the information cannot be modified (e.g. format).  PREPARE a memo informing the chief, ATIP, that the request for correction was accepted. Include a copy of the notation and provide the list of persons/organizations (internally and externally) with whom / with which the information was shared.  NOTIFY the persons/organizations on the list of the correction.
	5. <b><u>If it is not accepted:</u></b>  ATTACH a notation to the personal information indicating that a request was made but refused (notation should be visible when consulting the information).  PREPARE memo to the chief, ATIP, indicating the reasons for refusal. Include a copy of the notation and its location in relation to the information and provide the list of persons/organizations (internally and externally) with whom / which the information was shared.  NOTIFY the persons/organizations on the list that a request for correction was received by the NCC, but that it was refused (include a copy of the relevant information).
	6. SEND a memo to the ATIP branch liaison officer.
ATIP Branch Liaison Officer	7. FORWARD the reply from the manager to the ATIP office.
ATIP Delegated Officer	8. NOTIFY the applicant, within the legislative deadline, of acceptance or refusal, and PROVIDE him/her with the list of persons who will be informed of this decision. INFORM the applicant of his/her right under the PA to complain to the Privacy Commissioner if he/she is not satisfied with the NCC's decision.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### 4. Disclosing personal information informally

Employees	<p>1. VERIFY the identity of the individual requesting his/her personal information, prior to disclosing.</p> <p>CONSULT the ATIP Office if there is any doubt as to what information can be disclosed, or if records will not be provided in their entirety.</p>
ATIP Office	<p>2. PROVIDE guidance to NCC staff in the processing of informal requests.</p> <p>PROVIDE guidance to NCC managers in establishing practices to enable the informal disclosure of personal information.</p>
Example of an Established Practice	<p>Employees requesting access to their personal information: The Human Resources Branch and Facilities Management Branch (HRFM) shall give access to the personal information it holds.</p> <p>If HR intends to withhold information, it will consult the ATIP office to confirm if the information would be withheld from disclosure, had it been requested formally under the PA.</p>

### 5. Planning new personal information collection, use or disclosure

Manager	<p>1. IDENTIFY the new need to collect, use or disclose personal information. PREPARE a preliminary description and purpose of collection, use or disclosure. SUBMIT a proposal to the chief, ATIP, to determine if a PIA is required. If recommended, initiate a PIA to ensure that all privacy risks are identified, addressed and mitigated, as per the TBS <a href="#">Directive on Privacy Impact Assessment</a>, in consultation with the chief, ATIP.</p>
Chief, ATIP	<p>2. REVIEW the proposal for PA requirements. OBTAIN additional information from the manager, if necessary. PROVIDE advice to the manager to ensure conformity with the PA requirements.</p>
	<p>3. DETERMINE if a personal information bank or a new <a href="#">class of personal information</a> is required.</p>
	<p>4. If a personal information bank is required, COMPLETE the appropriate form and SEND to TBS to obtain a registration number.</p>
	<p>5. APPROVE the PIA and send a copy to the Office of the Privacy Commissioner and TBS once the head of the branch has also approved.</p>
Manager	<p>6. AMEND the proposal if necessary, and PROCEED with collection.</p>
Chief, ATIP	<p>7. INFORM the chief, Management and Security of Information, of any new collection of personal information (for updating the Corporate Information Inventory System).</p>

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### Appendix A

#### Overview

The [Privacy Act](#) (PA) gives individuals the right to access personal information about themselves that is held by the federal government, subject to the exemptions in the PA (sections 18 to 28). It protects personal information from unauthorized disclosure, and controls its collection, use, disclosure, retention and disposal under sections 4 to 8 of the PA, which regulate how the federal government must treat personal information. One can also refer to the fair information principles found in the [Personal Information Protection and Electronics Act](#) for a better understanding of the principles regulating the management of personal information. These [principles are summarized](#) on the Office of the Privacy Commissioner of Canada's [website](#).

Without the consent of the individual, personal information under the control of the organization may be disclosed only for the purposes listed in section 8 of the PA. For some of these purposes, an action is required prior to disclosing the information (i.e. notifying the Privacy Commissioner). For this reason, it is very important to seek advice from the ATIP Division prior to disclosing information without the consent of the individual.

The PA also gives individuals the right to make requests for corrections to their personal information, and provides a complaint mechanism that people can use if they believe that their personal information is being improperly withheld from them or if they believe that it has been improperly collected, used, disclosed or retained. The Office of the Privacy Commissioner of Canada is responsible for investigating these complaints.

Individuals can also apply to the Federal Court for a review of a decision by an institution to refuse access to their personal information within 45 days after the results of the investigation by the Privacy Commissioner have been reported. It is important to note that exceeding the time limit to reply to a request for access is deemed to be a denial of access. In which case, a Federal Court action may be initiated after a complaint has been investigated.

Formal requests for personal information and requests for corrections are administered by the chief, ATIP, and the ATIP analyst, in collaboration with the ATIP liaison officers. The chief, ATIP, and the ATIP analyst also initiate the consultations with other departments, when required, and represent the NCC in dealings with the Privacy Commissioner and with the Federal Court.

Requests for personal information and for corrections must be processed within 30 days. This time frame can be extended only for reasons stipulated in the PA.

The NCC publishes on its website an inventory of programs and personal information holdings, as well as application forms and instructions, to inform the public on accessible NCC information.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### Appendix B

#### Disclosure of personal information to third parties (without consent)

Sub-section 8(2) of the PA provides that, without the consent of the individual concerned, personal information *may* be disclosed only for the purposes\* summarized below:

- a) the original purpose for which it was collected or for a [consistent use](#);
- b) to comply with an act of Parliament, or regulation thereunder;
- c) to comply with
  - i) a subpoena,
  - ii) a warrant,
  - iii) a court order;
- d) to provide to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada;
- e) to provide to an investigative body specified in regulations, on the written request, for the purpose of enforcing a law of Canada or a province or of carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;
- f) under an agreement between the Government of Canada and another government (such as provincial government or foreign state) for the purpose of administering or enforcing any law or carrying out a lawful investigation;
- g) to assist a member of Parliament (federal) in resolving a problem for the individual to whom the information relates;
- h) for an audit, either internal or by the Comptroller General;
- i) to provide to Library and Archives Canada for archival purposes;
- j) to provide to the chair of the board of directors or a delegated official, for research or statistical purposes (**with restrictions**);
- k) to provide to an association of Aboriginal people or to an Indian band for resolving/validating Aboriginal claims/disputes or grievances;
- l) to provide to any government institution for the purpose of locating someone in order to collect a debt owed by that individual to Canada, or to issue a payment owing from Canada to that individual;
- m) to provide to the chair of the board of directors or a delegated official, for a purpose where public interest in disclosure clearly outweighs any invasion of privacy, or clearly benefits the individual to whom the information relates.

\* Advice should be sought from the ATIP Division prior to disclosing personal information, if it is for a purpose other than the purpose for which the information was obtained.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### Appendix B (cont'd)

#### Action required (disclosure pursuant to section 8 of the Privacy Act):

- 8(2)(a)** The use (original purpose) that will be made of the personal information, which must be known to the individual at the time of the collection, and any consistent use must be described in a personal information bank on the NCC website. In cases where the NCC releases personal information for a consistent use that is not yet described in the personal information bank listed on the NCC website at the time of disclosure, the chair of the board of directors, or a delegated official, must notify the Privacy Commissioner of the use for which the information was used or disclosed, attach a copy of this notification to the personal information, and ensure that the consistent use is updated in the personal information bank description.
- 8(2)(b)** Confirm with the ATIP Office prior to disclosing.
- 8(2)(c)** Anyone who intends to release personal information pursuant to this paragraph, shall consult with Legal Services to ensure the validity of the subpoena, warrant or court order, and to determine the proper form of compliance.
- 8(2)(d)** Since the NCC's Legal Services does not report to the Attorney General of Canada, personal information would be disclosable to the General Counsel, as the NCC litigation representative.
- 8(2)(e)** The NCC shall retain a copy of every request received under this paragraph and a copy of the records disclosed for a period of at least two years from the date the request is received, and make those copies available to the Privacy Commissioner, when requested. The ATIP Office should be consulted prior to disclosing to an investigative body, and a copy of all the records related to the disclosure (including administrative records) must be provided to the ATIP Office.
- 8(2)(f)** Any new memorandum of understanding (MOU) or agreement in which personal information is collected, used or disclosed must undergo a PIA. Disclosure can be made only in accordance with the terms of the MOU or agreement.
- 8(2)(g)** Only members of Parliament can request disclosure of personal information to help an individual. \*\*\*When Parliament is dissolved, during an election, no request for information can proceed under this section. Note that any representative can obtain personal information if he/she is authorized by the individual.
- 8(2)(h)** Disclosure can be given only for a non-administrative purpose for internal audits, to the Comptroller General of Canada or other body specified in regulations for audit purposes, and only for that purpose. Only personal information meeting the predetermined purpose of the audit can be disclosed. Before disclosing personal information to internal audit, for example, the scope of the audit must be known and only personal information which meets that scope can be disclosed.
- 8(2)(i)** As per the direction received from National Archives. Refer to the Management and Security of Information Division for guidance.
- 8(2)(j)** Information shall be released only if the chair of the board of directors or a delegated official
- 1) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and
  - 2) obtains, from the person, a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

- 8(2)(k)** Disclosure can be made to any Aboriginal government, association of Aboriginal people, Indian band or government institution to research or validate claims, disputes or grievances of any of the Aboriginal peoples of Canada. Refer to the ATIP Office, if such a disclosure is requested.
- 8(2)(l)** Confirm with the ATIP Office prior to disclosing.
- 8(2)(m)** The chair of the board of directors or a delegated official shall notify the Privacy Commissioner in writing of any disclosure where reasonably practicable or in any other case forthwith on the disclosure, in order that the Privacy Commissioner may notify the individual, to whom the information relates, of the disclosure if deemed appropriate. Refer to the ATIP Office for guidance. An evaluation must be completed to ensure that the public interest in disclosure outweighs the invasion of privacy that will result. The decision will be made in consultation with the General Counsel.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### **Definitions**

#### **Applicant**

Person who is requesting access to personal information under the PA or who is exercising his/her rights under the PA to a review by the court.

#### **ATIP analyst**

The analyst who has been delegated certain activities relating to the administration of the PA and related regulations, directives and guidelines within the NCC.

#### **ATIP branch liaison officer**

Person who coordinates the retrieval of records within his/her branch, and provides guidance to staff on the process. The branch liaison officers are the primary contacts for the ATIP Office regarding any privacy-related issue.

#### **Class of personal information**

A summary of the type of personal information held by a federal government institution that is not retrievable by a personal identifier (such as unsolicited complaints or correspondence).

#### **Consistent use**

Use of information directly connected to the purpose for which it was collected (normally a purpose the individual might have reasonably expected).

#### **Data matching**

Activity that involves comparing personal information from several sources, including personal information banks, for making decisions (usually done electronically, but it may also be done manually).

#### **Exclusion**

Information to which the PA does not apply. It consists of library or museum material, publicly available personal information, as well as confidences of the Queen's Privy Council for Canada.

#### **Exemption**

A provision of the PA which enables the institution to refuse disclosure of information in response to a request received under the PA (e.g. personal information about another individual, legal advice). See sections 18 to 28 of the PA for the complete list of exemptions.

#### **Parliamentary authority**

The collection of personal information is permitted in an act of Parliament. Example: for most government institutions, employee personal information is collected under the authority of the *Public Service Employment Act*.

#### **Personal information**

Information about an identifiable individual recorded in any form and as defined in section 3 of the PA.

#### **Personal information bank**

A description of the type of personal information held by a federal government institution which is used for administrative purposes and/or organized to be retrieved by name, identifying number or symbol, or other particular assigned to an individual.

#### **Privacy Commissioner**

An officer of Parliament appointed by order-in-council, with the powers of an ombudsman to receive and investigate complaints with respect to the handling of personal information by federal institutions. The Privacy Commissioner may also initiate complaints and examine compliance with sections 4 to 8 of the PA.

# CORPORATE ADMINISTRATIVE POLICIES AND PROCEDURES

## Privacy

### **Privacy impact assessment**

An assessment used to identify the potential privacy risks of new or redesigned federal government programs or services. It also helps eliminate or reduce those risks to an acceptable level.

### **Request for correction**

A request made by an individual, who was given access to personal information about himself/herself which is available for use for an administrative purpose, that a correction be made to the information as he/she believes that there is an error or omission therein.

### **Use for an administrative purpose**

The use of an individual's information in a decision-making process that directly affects that individual.

### **Use for a non-administrative purpose**

The use of personal information for a purpose not related to any decision-making process that directly affects the individual.