



Now and Tomorrow, Excellence in Everything We Do

DEPARTMENTAL POLICY ON PRIVACY MANAGEMENT





1. Effective Date

- 1.1 This policy takes effect on April 1, 2014.
- 1.2 This *Departmental Policy on Privacy Management* replaces the *Human Resources and Skills Development Canada Departmental Privacy Policy*, dated April 2007, and revised on October 2009.

2. Authority

- 2.1 This policy is issued under authority of the Deputy Minister of Employment and Social Development.

3. Application

- 3.1 This policy applies to all employees, agents and contractors of:
 - a) Employment and Social Development Canada (ESDC or the Department), including all ESDC branches, Service Canada and the Labour Program, and
 - b) Departmental portfolio entities where the Deputy Minister of Employment and Social Development Canada is the designated Accounting Officer.

4. Context

- 4.1 As the steward of personal information, ESDC is committed to meeting the highest standards of protection of personal information and respect for privacy. It is critical for the Department to maintain the trust of Canadians as an essential pre-condition for the collection, use and disclosure of their personal information. Accordingly, the protection of personal information is of such importance that it has been incorporated in the ESDC *Code of Conduct*.
- 4.2 The Department's statutory and non-statutory programs require the collection, use and disclosure of detailed, and at times highly sensitive, personal information. With the breadth of ESDC's mandate, the Department retains personal information on virtually all individuals in Canada, and has one of the largest personal information holdings in the country. It shares personal information with numerous partners, including federal departments and agencies, other governments in Canada and abroad, and non-governmental organizations. Because of the inherent risks of managing these large holdings of personal information, the Department's enabling legislation includes a "Privacy Code" that imposes additional rules for the use and disclosure of personal information under its custody and control, and specifies significant penalties for its intentional misuse.
- 4.3 This policy and its directives set out the Department's application of the *Privacy Act*, the *Privacy Regulations*, the *Department of Employment and Social Development Act* "Privacy Code", Treasury Board privacy policies and directives, and the ESDC *Code of Conduct*, with the aim of fostering a robust policy regime for the protection and judicious use of personal information. They have been designed to be referred and applied in conjunction with applicable *Privacy Act* and *Department of Employment and Social Development Act* delegation orders.



5. Integrated Framework for Privacy Management

- 5.1 To achieve ESDC's personal information protection objectives, and to build privacy into the design and architecture of programs, services, systems and technologies, the Department has established an Integrated Framework for Privacy Management consisting of the following pillars:
- a) *Governance and Accountability*: Established roles, responsibilities, and mechanisms to support the Department's conformance to legal requirements, regulations, policies, standards, and public expectations.
 - b) *Stewardship of Personal Information*: Appropriate privacy protections to safeguard personal information through its life-cycle.
 - c) *Culture, Training, and Awareness*: A privacy-respectful culture where employees, partners, and delivery agents understand their privacy obligations and are aware of tools, resources, policies, and processes related to privacy and personal information protection.
 - d) *Effective Risk Management*: Deliberate and systematic efforts to limit the probability and impact of negative events and maximize opportunities through risk identification, assessment, and prioritization.
 - e) *Assurance of Compliance*: Formal processes and practices to ensure adherence to privacy legislation, policies and standards.


6. Definitions

- 6.1 The definitions used in the interpretation of this policy are set out in Annex A.

7. Policy Statement

Objectives

- 7.1 Consistent with the Integrated Framework for Privacy Management and the Departmental Privacy Principles, as set out in section 10, the objectives of this policy are:
- a) The application of strict controls on the methods the Department and its employees, agents and contractors use to collect, use, retain, disclose and dispose personal information, in compliance with the *Privacy Act* and the *Department of Employment and Social Development Act* "Privacy Code";
 - b) The protection of personal information from unauthorized collection, use, disclosure, alteration, retention, or disposal;
 - c) The provision of responses to *Privacy Act* requests that are within the time limits and parameters set out in the *Act* and *Privacy Regulations*;
 - d) The development and implementation of directives, instruments and procedures for the effective governance, management and protection of privacy and personal information in compliance with all relevant statutes and Treasury Board policies; and

- 
- A decorative header image showing silhouettes of various people, including a person with a stroller, a person in a wheelchair, and a person with a cane, representing diversity and accessibility.
- e) The creation and sustainment of a stewardship of personal information culture throughout the Department.

Expected Results


7.2 The expected results of this policy are:

- a) The sound management and safeguarding practices established within the Department and applied by its employees, agents and contractors for the protection and handling of personal information in a manner that respects both the privacy of individuals and the provisions of the *Privacy Act* and *Department of Employment and Social Development Act* "Privacy Code";
- b) The identification, assessment and mitigation of privacy threats and risks for programs, activities and service offerings involving the management of personal information;
- c) Complete, accurate and timely responses to Canadians and individuals present in Canada, who exercise their rights of access to, and the correction of, their personal information under the control of the Department, subject to specific exemptions contained in the *Privacy Act* and the *Department of Employment and Social Development Act* "Privacy Code";
- d) Consistent public reporting by the Department on the administration of the *Privacy Act* through its annual report to Parliament, statistical reports, and *Info Source*; and
- e) Accountabilities, governance structures, mechanisms and the allocation of sufficient resources to protect and manage personal information in the Department.

8. Policy Requirements

8.1 In support of this policy, the Department will:

- a) Apply the directives and standards issued in direct support of this policy's objectives;
- b) Apply the Privacy Principles, as set out in section 10;
- c) Implement security controls to properly safeguard personal information under the Department's custody and control;
- d) Include appropriate privacy and security safeguards in contracts, information sharing agreements involving personal information, memoranda of understanding, service level agreements, contribution agreements and any other transactional arrangement between the Department and any governmental and non-governmental entities;
- e) Establish and implement procedures wherein the Department:
 - i) provides clear notice to individuals prior to any collection of their personal information that describes the purpose and authority for the collection;
 - ii) provides individuals with the ability to request access to their personal information, request the correction of their personal information, and file complaints concerning the management and use of their personal information; and

- 
- iii) notifies individuals of an improper collection, retention, use, disclosure or disposal of their personal information.
 - f) Proactively and rigorously identify threats and risks to, and implement effective protection and mitigation measures for, personal information under the Department's custody and control, as well as for new or substantially modified programs, activities and service offerings;
 - g) Exercise discretion by delegates under the *Privacy Act* and the *Department of Employment and Social Development Act*, in a fair, reasonable and impartial manner with respect to decisions on the processing of requests and the resolution of complaints as established in the *Privacy Act*, subject to the conditions set out in the *Privacy Regulations*;
 - h) Provide the required privacy training and tools so that all employees understand and comply with the legal responsibilities, policies, procedures, and practices with respect to the principles of values and ethics, privacy, security, information technology security, and information management as they relate to the collection, use, retention, disclosure and disposal of personal information;
 - i) Designate the Corporate Secretary as the Chief Privacy Officer, reporting to the Deputy Minister, or his or her delegate, as the Department's functional authority and senior advisor on privacy matters, and who is accountable for the development and oversight of this policy, its associated directives and instruments, and the Department's privacy management program;
 - j) Establish, maintain and support a Departmental privacy management program with resources sufficient for the coordination, protection and management of privacy activities, and comprising of a governance structure with clear accountabilities and defined objectives that are aligned with Departmental and government-wide policies, priorities and plans, risk identification and mitigation strategies, the monitoring and assessment of the privacy program's performance, reporting on outcomes, and periodic evaluations and reviews;
 - k) Establish, maintain and support oversight committees to ensure that management's direction, plans and actions on the protection of personal information in the Department are appropriate and responsible; and
 - l) Review and monitor compliance with this policy, including documenting and remedying any violations.

9. Roles and Responsibilities

9.1 The roles and responsibilities for this policy are set out in Annex B.

10. Privacy Principles

10.1 The following principles provide the basis upon which the Department's privacy policies, directives and procedures are founded. They underpin ESDC's everyday practices and decisions involving the protection and management of personal information.

- a) *Accountability*



- i) ESDC is responsible for all the personal information under its custody and control.
 - ii) The Deputy Minister of Employment and Social Development Canada is responsible for the Department's compliance with all statutes and Treasury Board policies concerning the management and protection of personal information.
 - iii) ESDC's Chief Privacy Officer is the functional authority for privacy and is responsible for the proactive management of the Department's privacy program.
 - iv) All ESDC employees are responsible for ensuring the safeguarding and protection of personal information under their custody and control.
- b) *Identifying Purposes*
- i) The Department explains to individuals, at or before the time of collection, in plain language, the purpose and authority for which personal information is being collected.
- c) *Consent*
- i) Where appropriate or when required by statute, the knowledge and the express written or verbal consent of the individual for the collection, use, or disclosure of personal information is obtained openly, transparently and voluntarily. An individual may withdraw consent at any time, subject to legal restrictions and reasonable notice.
- d) *Limiting Collection*
- i) ESDC limits the collection of personal information, including the amount and type, to that which is directly relevant and the minimum necessary to fulfill the intended purpose for collection.
- e) *Limiting Use, Disclosure and Retention*
- i) ESDC does not use or disclose personal information for purposes other than those for which it was originally collected or for a use consistent with the original collection, unless there is legal authority or required by statute.
 - ii) Subject to the relevant Records Disposition Authority, personal information used by ESDC for an administrative purpose is retained for at least two years following the last time it is used, unless the individual consents to an earlier disposal.
- f) *Accuracy*
- i) ESDC takes reasonable measures to ensure that the personal information used for Departmental purposes is as accurate, complete and as up-to-date as possible.
- g) *Safeguards*
- i) All personal information, in all forms and formats under the custody and control of the Department, are protected by security measures appropriate to the sensitivity of the information to safeguard against loss, theft or unauthorized disclosure, copying, use, and modification.



h) *Openness*

- i) ESDC makes public the descriptions and uses of the personal information that it collects and holds. Detailed information about its policies and practices to manage and protect personal information are readily available to individuals in a form that is clear and understandable.

i) *Individual Access*

- i) Upon request, a Canadian citizen or an individual present in Canada, is informed of the existence, use, and disclosure of his or her personal information under the custody and control of the Department, and will be provided access to that information in accordance with the *Privacy Act* and *Privacy Regulations*.
- ii) An individual can challenge the accuracy and completeness of their personal information. As required, ESDC amends the information and provides the amended information to third parties to whom the information had previously been disclosed, where appropriate.

j) *Challenging Compliance*

- i) Individuals can challenge the Department about its compliance with these principles as well as ESDC's policies and practices concerning the management and protection of their personal information. The Department responds to all inquiries. It investigates all complaints and takes the necessary corrective action.

11. Governance

11.1 The following oversight committees support the Deputy Minister's direction, plans and actions with respect to the protection of personal information:


- a) The Privacy and Information Security Committee provides advice and recommendations to the Corporate Management Committee on matters related to privacy and the protection of personal information, and
- b) The Corporate Management Committee oversees the implementation of the Department's management agenda, including those items considered by the Privacy and Information Security Committee.

12. Consequences

12.1 A violation of this policy or any of the related statutes, policies or procedures, may lead to administrative or disciplinary measures being taken, up to and including termination of employment. In addition, any person or body commits an offence if they use or knowingly make available information that is privileged under Part 4 of the *Department of Employment and Social Development Act*, and may be subject to additional punishment, including a fine and/or imprisonment.

13. Monitoring, Assurance of Compliance and Reporting

13.1 A review of this policy and its associated directives will be performed every five years. Additional reviews of this policy can be conducted periodically as determined by the Deputy



Minister of Employment and Social Development Canada in consultation with the Chief Privacy Officer.

- 13.2 Assurance on the implementation of this policy will form a regular part of the Departmental internal audit program, which will conduct periodic audits of privacy management in the Department's programs and services.

14. References

14.1 Acts and Regulations of Canada

Canada Pension Plan
Employment Insurance Act
Department of Employment and Social Development Act
Department of Employment and Social Development Act
Act Regulations
Old Age Security Act
Privacy Act
Privacy Regulations

14.2 Treasury Board Policies

Policy on Government Security
Policy on Information Management
Policy on Internal Audit
Policy on Privacy Protection
Values and Ethics Code for the Public Service

14.3 Treasury Board Directives

Directive on Electronic Authentication and Authorization of Financial Transactions
Directive on Identity Management
Directive on Information Management Roles and Responsibilities
Directive on Management of Information Technology
Directive on Privacy Practices
Directive on Privacy Impact Assessments
Directive on Privacy Requests and Correction of Personal Information
Directive on Recordkeeping
Directive on Social Insurance Number

14.4 Treasury Board: other policy instruments

Guidance on Preparing Information Sharing Agreements Involving Personal Information
Guidelines for Privacy Breaches
Operational Security Standard: Management of Information Technology Security
Standard on Privacy and Web Analytics

14.5 Employment and Social Development Canada Policies and Directives

Departmental Security Policy and Procedures Manual
Departmental Directive on How to Respond to Security Incidents Involving Personal Information
ESDC Code of Conduct
ESDC Recordkeeping Directive
Information Management (IM) Policy
Policy on Departmental IT Security Management

A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people. The silhouettes include individuals of various ages, a person in a wheelchair, a person with a cane, and a person pushing a stroller, set against a light blue background.

15. Enquiries

15.1 Enquiries regarding this policy should be directed to:

Chief Privacy Officer
Corporate Secretariat
Employment and Social Development Canada
140 Promenade du Portage
Gatineau, Quebec K1A 0J9

Telephone: (819) 994-1122
Email: CPO-CPRP@hrsdc-rhdcc.gc.ca



Annex A: Definitions

Certain terms contain excerpts (in quotation marks, with the reference cited) from the *Privacy Act*. Some definitions contain additional information not included in the Act.

Administrative purpose means the use of personal information about an individual "in a decision making process that directly affects that individual" (section 3). This includes all uses of personal information for confirming identity (i.e. authentication and verification purposes) and for determining eligibility of individuals for Government of Canada programs.

Annual report means a report submitted by the head of a federal government institution to Parliament on the administration of the *Privacy Act* during the financial year.

Delegate means an officer or employee of a government institution who has been delegated to exercise or perform the powers, duties and functions of the head of the institution under the *Privacy Act*.

Designated Minister means a person who is designated as the Minister under subsection 3.1(1) of the *Privacy Act*. For the purposes of this policy, the designated minister is the President of the Treasury Board.

Exempt bank means a personal information bank that describes files, all of which consist predominantly of personal information that relates to international affairs, defence, law enforcement and investigation, as outlined in sections 21 and 22 of the *Privacy Act*. The head of a government institution can refuse to disclose any personal information requested that is contained in an exempt bank.

Functional Authority means mandate to control specific or specialist activities undertaken by employees that cut across an organization's chain of command. This includes the responsibility to set goals and see to it that they are met.


Functional Direction means the exercise of functional authority through the provision of explicit or binding (i.e., non-discretionary) policies or procedures to managers and employees.

Government institution means any Department or ministry of state of the Government of Canada, or any body or office, listed in the schedule; and, any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act* (section 3). The term "government institution" does not include Ministers' Offices.

Head means the Minister, in the case of a Department or ministry of state. In any other case, it is the person designated by the *Privacy Act Heads of Government Institutions Designation Order*. If no such person is designated, the chief executive officer of the government institution, whatever their title, is the head.

Info Source is a Treasury Board Secretariat publication (available at <http://infosource.gc.ca>) in which government institutions are required to describe their institutions, program responsibilities and information holdings, including personal information banks and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the *Privacy Act*. Data-matching activities, use of the Social Insurance Number and all activities for which privacy impact assessments were conducted have to be cited in *Info Source* personal information bank, as applicable. *Info Source* also provides contact information for government institutions as well as summaries of court cases and statistics on access requests.

Management of personal information means its collection, retention, use, disclosure and disposal.



Non-administrative purpose means the use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistical, audit and evaluation purposes.

Personal information means information about an identifiable individual that is recorded in any form as defined by section 3 of the *Privacy Act*. It is information about an identifiable individual that is recorded in any form and can include: race or colour; national or ethnic origin; religion; age; marital status; blood type; fingerprints; medical, criminal or employment history; information on financial transactions; home address; and Social Insurance Number (SIN), driver's licence or any other identifying number assigned that are assigned to individuals. It also includes personal information from Departmental employees.

Personal information bank (PIB) means a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution. PIBs are available for access in *Info Source*.

Privacy impact assessment means a policy process for identifying, assessing and mitigating privacy risks. Government institutions are to develop and maintain privacy impact assessments for all new or modified programs or activities that involve the use of personal information for an administrative purpose.

Privacy Commissioner means the Privacy Commissioner of Canada, an Officer of Parliament appointed by Governor in Council with the mandate to investigate complaints under the *Privacy Act*, conduct audits on personal information-handling practices of government institutions and the private sector, and act as an ombudsman.

Privacy request means a request for access to personal information under section 13 of the *Privacy Act*.

Program or activity means a program or activity that is authorized or approved by Parliament. Parliamentary authority is usually contained in an Act of Parliament or subsequent *Regulations*. Parliamentary authority can also be in the form of approval of expenditures proposed in the Estimates and as authorized by an appropriation Act. Also included in this definition are any activities conducted as part of the administration of the program.

Protection of personal information means the safekeeping of personal information collected, handled, stored, extracted, transported or transmitted, whether the information is in an electronic, paper, or other format by their organization, and the classification of the information in accordance with Treasury Board and Departmental standards.

Relevant statutes means the *Privacy Act*, the *Department of Employment and Social Development Act*, the *Canada Pension Plan*, the *Employment Insurance Act*, and the *Old Age Security Act*.

Social Insurance Number (SIN) means a number suitable for use as a file number or account number or for data-processing purposes, as defined in subsection 138(3) of the *Employment Insurance Act*. For purposes of paragraph 3(c) of the *Privacy Act*, the SIN is an identifying number, and is therefore considered to be personal information. Use of the SIN is only permitted by express legislative authority, as granted by Parliament, or policy authority, as granted by the Treasury Board. Its use is governed by the Treasury Board Directive on Social Insurance Number.

Statistical report means a document to provide up-to-date metrics on the operation of the *Privacy Act*. The reports allow the government to monitor trends and to respond to enquiries from Members of Parliament, the public and the media. The reports also form the statistical portion of government institutions annual reports to Parliament. The forms used for preparing the report are prescribed by the designated minister, as provided under paragraphs 71(1)(c) and (e) of the *Privacy Act*.



Annex B: Roles and Responsibilities

PART A: Line Responsibilities

Minister of Employment and Social Development


- a) Signs a delegation order, if a decision is made to delegate, for authorities under the *Privacy Act*, *Privacy Regulations* and the *Department of Employment and Social Development Act*, and ensures that delegates receive privacy training in accordance with the Treasury Board directives.
- b) Establishes the Department's privacy impact assessment development and approval process.
- c) Submits the Department's annual report to Parliament on the administration of the *Privacy Act*.

Minister of Labour

- a) Signs a delegation order, if a decision is made to delegate, for specific authorities under the *Department of Employment and Social Development Act*, and ensures that delegates receive privacy training in accordance with Treasury Board directives.

Deputy Minister of Employment and Social Development Canada

- a) Is responsible for:
 - i. the management and protection of personal information within the Department in accordance with all relevant statutes, regulations and Treasury Board policies;
 - ii. ensuring that all Departmental delegates and employees with functional privacy responsibilities have specialized privacy training, and that all remaining employees have privacy training and are aware of their privacy responsibilities;
 - iii. the Department's compliance with statutes and specific terms and conditions related to the use of the Social Insurance Number;
 - iv. establishing a plan for addressing security incidents involving personal information within the Department;
 - v. identifying and describing all personal information controlled by ESDC in the Department's Personal Information Banks, aligning the development process for new or substantially modified Personal Information Banks with the privacy impact assessment process, and submitting proposals for the registration of new or the substantial modification or the termination of Personal Information Banks to the Treasury Board Secretariat;
 - vi. consulting with the Treasury Board Secretariat on any proposal to establish or revoke an exempt Personal Information Bank and submitting for review to the Treasury Board Secretariat proposals to designate a Personal Information Bank as exempt;
 - vii. adhering to Treasury Board policy requirements concerning requests from, and disclosures to, investigative bodies;


- 
- viii. the Department's compliance with the *Privacy Act*, *Privacy Regulations*, ESDC's Privacy Code, and the authorities delegated by the Minister in its responses to privacy requests;
 - ix. the incorporation of privacy protection provisions mandated by statute or policy in all contracts and transactional arrangements, including transfer payment funding agreements, with either private or public sector entities; and
 - x. ensuring that the use of Web analytics for measuring and improving performance of institutional websites is implemented in accordance with the requirements to protect privacy as set out in the Treasury Board *Standard on Privacy and Web Analytics* and of ensuring that appropriate remedial action is taken to address any deficiencies.
- b) Allocates resources that are sufficient to support effective management of personal information and privacy protection processes throughout the Department.
 - c) Exercises or performs the specific powers, duties or functions delegated by the Minister.
 - d) Designates a Chief Privacy Officer for the Department as the functional authority for privacy.
 - e) Establishes and maintains an effective governance process for the Department's privacy management program.
 - f) Approves privacy impact assessments.

Deputy Minister of Labour

- a) Is responsible for:
 - i. managing and protecting personal information within the Labour Program in accordance with all relevant statutes, regulations, and Treasury Board policies;
 - ii. ensuring that all Labour program delegates and employees with functional privacy responsibilities have specialized privacy training, and that all remaining employees have privacy training and are aware of their privacy responsibilities; and
 - iii. the Labour program's compliance with the *Privacy Act*, *Privacy Regulations*, ESDC's Privacy Code, and the authorities delegated by the Minister in its responses to privacy requests; and
 - iv. the reporting of security incidents involving personal information in the Labour Program and responses follow established Departmental protocols
- b) Assigns resources that are sufficient to support effective personal information management and protection processes within the Labour Program.
- c) Exercises or performs the specific powers, duties or functions delegated by the Minister.
- d) Supports and aligns the Labour Program's privacy activities to the Department's privacy management program.

Senior Associate Deputy Minister and Chief Operating Officer for Service Canada


- a) Is responsible for:

- 
- A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people, including individuals of various ages, ethnicities, and abilities, some using mobility aids like wheelchairs and canes.
- i. the management and protection of personal information within Service Canada in accordance with all relevant statutes, regulations, and Treasury Board policies;
 - ii. ensuring that all Service Canada delegates and employees with functional privacy responsibilities have specialized privacy training, and that all remaining employees have privacy training and are aware of their privacy responsibilities;
 - iii. Service Canada's compliance with the specific terms and conditions related to the use of the Social Insurance Number and the specific restrictions with regard to its collection, use and disclosure;
 - iv. Service Canada's compliance with the *Privacy Act*, *Privacy Regulations*, ESDC's Privacy Code, and the authorities delegated by the Minister in its responses to privacy requests; and
 - v. the reporting of security incidents involving personal information in Service Canada and ensuring that responses follow established Departmental protocols.
- b) Allocates resources within Service Canada that are sufficient to support effective personal information management and protection processes.
 - c) Exercises or performs the specific powers, duties or functions delegated by the Minister.
 - d) Supports and aligns Service Canada's privacy activities to the Department's privacy management program.

Branch Heads and Regional Assistant Deputy Ministers

Each Branch Head or Regional Assistant Deputy Minister, within his or her specific accountabilities:


- a) Is responsible for:
 - i. the management and protection of personal information within his or her branch or region in accordance with all relevant statutes, regulations, and Treasury Board policies;
 - ii. ensuring that all branch or regional delegates and employees with functional privacy responsibilities have specialized privacy training, and that all remaining employees have privacy training and are aware of their privacy responsibilities;
 - iii. the information technology applications and systems in his or her branch or region having the appropriate security certification and accreditation, in collaboration with the Chief Information Officer;
 - iv. incorporating, in consultation with the Chief Privacy Officer, privacy protection provisions mandated by statute or policy in information sharing agreements involving personal information, memoranda of understanding, service level agreements, contracts and transactional arrangements that are negotiated by his or her branch or region, with either private or public sector entities, and, upon execution, for his or her branch's or region's compliance with the privacy protection provisions;
 - v. his or her branch's or region's compliance with personal information retention and disposition schedules;
 - vi. the quality and reliability of the personal information used for administrative purposes by his or her branch or region and enabling individuals to correct inaccurate personal information about themselves;

- 
- A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people. The silhouettes include individuals of various ages and abilities, such as a person in a wheelchair, a person with a cane, a person pushing a stroller, and a person holding a child. The background behind the silhouettes is a light blue gradient.
- vii. informing the individuals who are responsible for managing websites, as well as those functional specialists and Web content owners, of the need to meet the requirements of the Treasury Board *Standard on Privacy and Web Analytics*;
 - viii. the reporting of security incidents involving personal information in his or her branch or region to the appropriate Regional Security Officer and the Departmental Security Officer, and that the responses follow established Departmental protocols;
 - ix. informing the Chief Privacy Officer, promptly, of proposals for any new, or substantive changes to programs, service offerings or activities within his or her branch or region for which he or she is the Departmental lead; and
 - x. privacy-related planning, monitoring and performance reporting within his or her branch or region in support of the Departmental privacy program.
- b) Determines, in conjunction with the Chief Privacy Officer, whether privacy impact assessments are required for new or substantially modified programs, service offerings and activities for which he or she is the Departmental lead.
 - c) Exercises or performs the specific powers, duties or functions delegated by the Minister.
 - d) Recommends the establishment and modification of personal information banks, and regularly reviewing any exempt personal information banks, that are under his or her branch's or region's control.
 - e) Complies with the specific terms and conditions related to the use of the Social Insurance Number and the specific restrictions with regard to its collection, use and disclosure.
 - f) Supports and aligns his or her branch's or region's privacy activities to the Department's privacy management program.
 - g) Provides resources to support effective personal information management and protection processes in his or her branch or region.

EX Managers (Other than Deputies, Branch Heads or Regional Assistant Deputy Ministers)

In their respective areas of direct responsibility, EX Managers:


- a) Provide the necessary resources and tools to enable their employees to properly fulfill their stewardship of personal information responsibilities.
- b) Readily provide to their employees:
 - i. privacy training, and
 - ii. guidance when they seek information about handling and protecting personal information.
- c) Are responsible for ensuring that their employees have:
 - i. undertaken the required privacy training; and
 - ii. a clear understanding of their obligations for the protection and management of personal information;

- 
- d) Are responsible for the collection, retention, use, disclosure and disposal of personal information in accordance with all relevant statutes, regulations, and Treasury Board and Departmental policies.
 - e) Respond to privacy requests and support the Departmental Privacy Coordinator with respect to investigations and complaints.
 - f) In consultation with the Chief Privacy Officer:
 - i. develop and complete privacy impact assessments;
 - ii. prepare proposals to establish or modify personal information banks;
 - iii. prepare information sharing agreements, memoranda of understanding, service level agreements, and contribution agreements that involve personal information;
 - iv. include privacy protection provisions for all contracts and transactional arrangements with either private or public sector entities; and
 - v. develop privacy notices.
 - g) Limit the collection of personal information to what is directly required for the program or activity.
 - h) Comply with the statutes and specific terms and conditions related to the use of the Social Insurance Number and the specific restrictions with regard to its collection, use and disclosure.
 - i) Adhere to personal information retention and disposition policies and schedules.
 - j) Verify the quality and accuracy of the personal information used for administrative purposes within his or her area or areas of direct responsibility, and permit individuals to correct inaccurate personal information about themselves.
 - k) Implement Departmental security practices for the protection of personal information and mitigate privacy risks.
 - l) Become the incident lead for any security incident involving personal information their areas of direct responsibilities, and in the event of a security incident, are responsible, with the Regional Security Officer, for containing the security incident and implementing an action plan.

Non-EX Managers

In their respective areas of direct responsibility:

- a) Provide the necessary resources and tools to enable their employees to properly fulfill their stewardship of personal information responsibilities.
- b) Readily provide guidance to employees when they seek information about handling and protecting personal information.
- c) Verify that their employees:
 - i. understand their obligations for the protection and management of personal information;
 - ii. collect, retain, use, disclose and dispose personal information in accordance with all relevant statutes, regulations, and Treasury Board and Departmental policies;

- 
- A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people. The silhouettes include individuals of various ages, a person in a wheelchair, a person using a cane, and a person pushing a stroller, set against a light blue background.
- iii. have been provided with and have undertaken the required privacy training; and
 - iv. respond to privacy requests and support the Departmental Privacy Coordinator with respect to investigations and complaints.
- d) Limit the collection of personal information to what is directly required for the program or activity.
 - e) Comply with the specific terms and conditions related to the use of the Social Insurance Number and the specific restrictions with regard to its collection, use and disclosure.
 - f) Adhere to personal information retention and disposition policies and schedules.
 - g) Implement Departmental security practices for the protection of personal information and mitigate privacy risks.

All Employees

Every Departmental employee:

- a) Understands and complies with the policies, procedures, and practices, including values and ethics, privacy, security, information technology security, and information management for the collection, retention, use, disclosure and disposal of personal information.
- b) Protects the privacy rights of Canadians and employees by protecting and keeping in strict confidence all personal information, and is responsible for the safekeeping of information he or she personally collects, handles, stores, transports or transmits, whether the information is in electronic, paper, or other format.
- c) Undertakes the required privacy training.
- d) Seeks guidance from supervisors when in doubt or he or she has questions about handling and protecting personal information.
- e) Responds to *Privacy Act* requests, and in doing so, makes every reasonable effort to search Departmental records to identify and locate the personal information that is responsive to a request in accordance with established procedures and rules.
- f) Provides valid and request-related recommendations on the disclosure of personal information.
- g) Reports any incidents of improper or accidental access, use, disclosure or loss of personal information. Takes immediate action to stop a security incident involving personal information and secures the affected records, devices, systems or web sites, documents the security incident, and notifies his or her immediate supervisor.
- h) Proactively identifies to supervisors any privacy risks and provides recommendations to mitigate those risks or improve the secure handling of personal information.



PART B: Functional Responsibilities

Chief Privacy Officer:

- a) Is the Department's functional authority on all privacy matters, which includes the provision of authoritative advice and functional direction to all ESDC branches and regions.
- b) Is responsible for the proactive management of privacy issues in the Department and the establishment of comprehensive privacy management frameworks, programs, review processes, and risk-based approaches to privacy management.
- c) Establishes Departmental privacy directives, standards, guidelines, and processes.
- d) Establishes, maintains, and supports the Departmental privacy management program for the coordination and management of privacy activities comprising of a governance structure with clear accountabilities, defined objectives that are aligned with Departmental and government-wide policies, priorities and plans, and that is monitored, assessed and reported-on to measure performance against expected results.
- e) Monitors the compliance to relevant privacy protection and personal information statutory obligations, policies and standards and conducts regular reviews to assess whether the implementation of this policy and its associated directives and programs are effective in the Department.
- f) Evaluates legislative, regulatory, policy, program and service proposals that include the collection, use, and disclosure of personal information.
- g) Exercises or performs the specific powers, duties or functions delegated by the Minister.
- h) Develops and offers privacy training and awareness programs, products and services.
- i) Is the Department's primary point of contact on privacy matters with the Privy Council Office, Treasury Board Secretariat and the Office of the Privacy Commissioner of Canada.
- j) Prepares the Department's annual report to Parliament on the administration of the *Privacy Act*.
- k) Monitors the use of authorities delegated from the *Privacy Act* and the Privacy Code. Conducts periodic reviews of the privacy delegation orders and provides advice and recommendations to the Deputy Minister on any modifications to or on its implementation, if required.
- l) Establishes and supports, in collaboration with the Chief Information Officer and the Departmental Security Officer, an integrated approach for Departmental privacy, security and information management/information technology.
- m) Collaborates with the Chief Information Officer, the Assistant Deputy Minister Integrity Services, the Departmental Security Officer, the Departmental Information Technology Security Coordinator, the Chief Audit Executive, and the Senior General Counsel to ensure the effective management of privacy and information security matters.
- n) Establishes, in collaboration with the Departmental Security Officer, plans for the management of security incidents involving personal information.
- o) Collaborates with the Departmental Security Officer in providing oversight and support for the proper management and record-keeping of all security incidents involving personal information.




Director, ATIP Operations

- a) Responds to *Privacy Act* requests in accordance with the Act, and the authorities delegated by Ministers, including extensions, translations, formats and exclusions.
- b) Exercises or performs the specific powers, duties or functions delegated by the Minister.
- c) Responds to complaints received from the Privacy Commissioner in accordance with the authorities delegated by the Minister.
- d) Manages the disclosure of information to third parties via public interest disclosures.
- e) Retains records of privacy requests and disclosed information made to investigative bodies.
- f) Notifies the Privacy Commissioner of all public interest disclosures under the *Privacy Act*.
- g) Notifies program leads of an individual's request to correct personal information retained by the Department.
- h) Responds to legal instruments in which the Department is asked to share personal information (e.g., subpoenas, court orders and search warrants).
- i) Coordinates with the Treasury Board Secretariat, and the Office of the Privacy Commissioner on matters related to the position's roles and responsibilities.

Director, Privacy Management

- a) Supports and provides leadership for the implementation of the Department's privacy management program.
- b) Provides advice and support to ensure the effective management of Departmental privacy matters.
- c) Determines, in conjunction with the responsible ESDC program or project leads whether privacy impact assessments are required for new or substantially modified programs and activities.
- d) Collaborates with, and provides technical expert advice to, program and project leads on the development, completion and approval of privacy impact assessments in accordance with established Departmental processes.
- e) Provides technical expert advice to:
 - i. Departmental leads on establishing, modifying, and reviewing Personal Information Banks (including exempt banks);
 - ii. Branches and regions for the preparation and amendment of information sharing agreements involving personal information;
 - iii. The Chief Financial Officer and/or other Departmental procurement authorities to ensure that all contracts and transactional arrangements with either private or public sector entities contain privacy protection provisions mandated by statute or policy, as necessary; and


- 
- A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people, including individuals of various ages, ethnicities, and abilities, some using mobility aids like wheelchairs and strollers.
- f) Program and service leads for the provision of notifications and obtaining consents from individuals for the collection of personal information. Reviews Memoranda to Cabinet and Treasury Board submissions for privacy implications.
 - g) Updates the Department's *Info Source* information.
 - h) Coordinates with the Treasury Board Secretariat, and the Office of the Privacy Commissioner, on matters related to the position's roles and responsibilities.

Regional Directors, Strategic Policy, External Relationships and Corporate Affairs

- a) Respond to *Privacy Act* requests in the Regions in accordance with the Act, and the authorities delegated by Ministers, including extensions, translations, formats and exclusions.
- b) Exercise or perform the specific powers, duties or functions delegated by the Minister.
- c) Monitor compliance of regional operations to this policy and the Department's privacy management program. Manage regional privacy processes and standards, and monitor compliance under the functional direction of the Chief Privacy Officer.
- d) Contribute in the resolution of complaints received from the Office of the Privacy Commissioner, as requested by the Chief Privacy Officer or the Departmental Privacy Coordinator.
- e) Provide authoritative privacy advice to regional employees.
- f) Provide required Departmental privacy training to regional employees,
- g) Provide advice and support, in consultation with the Chief Privacy Officer and the Head of the Service Management Branch, to regional integrity services and business lines to ensure the effective management of privacy and the protection of personal information,
- h) Seek advice and implement functional direction from the Chief Privacy Officer.

Chief Information Officer

- a) Ensures the appropriate management direction, processes and tools are in place to efficiently manage personal information under the custody and control of the Department. Establishes and implements key methodologies, mechanisms and tools to support Departmental personal information recordkeeping requirements throughout the information lifecycle.
- b) Consults and collaborates with the Chief Privacy Officer on matters of mutual interest.
- c) Liaises with the Library and Archives Canada to determine the duration of personal information retention and disposition.
- d) Provides advice on information technology security requirements for Departmental programs and services.
- e) With the Departmental IT Security Coordinator, ensures that appropriate security measures are applied to all Departmental information management and information technology assets, activities and processes.
- f) Ensures that security requirements for information technology projects are met through the development and implementation of technical security specifications.

- 
- A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people. The silhouettes include individuals of various ages, a person in a wheelchair, a person using a cane, and a person pushing a stroller, all set against a light blue background.
- g) Provides the security certification of information technology systems as the accreditation authority.
 - h) Establishes and supports, in collaboration with the Chief Privacy Officer and Departmental Security Officer, an integrated approach for Departmental privacy, security and information management/information technology.
 - i) Consults with the Departmental Security Officer on areas of mutual interest to ensure an integrated approach for Departmental Security.
 - j) Establishes standards and requirements and monitors compliance on the electronic storage, transportation, transmission and disposal of personal information.
 - k) Monitors data extracts and exchanges to confirm compliance with established agreements.

Departmental Security Officer

- a) Includes the protection of personal information as part of the Departmental security program.
- b) Provides advice to management, including the Chief Financial Officer, Chief Information Officer, and Chief Privacy Officer, with respect to the protection of personal information.
- c) Provides assurance to the Chief Financial Officer that security management controls are effective with respect to the integrity of electronic financial transactions and related authentications and authorizations.
- d) With the collaboration and support of the Departmental IT Security Coordinator, is responsible for ensuring that physical, personnel and information technology security are coordinated to protect information and information technology assets.
- e) Ensures that applicable legislation, delegated authorities and policies are followed and respected for disclosures of personal information in an emergency.
- f) Establishes and supports, in collaboration with the Chief Privacy Officer and Chief Information Officer, an integrated approach for Departmental privacy, security and information management/information technology.
- g) With the collaboration and support of the Chief Privacy Officer, is responsible for the oversight and proper management and record-keeping of all security incidents involving personal information of clients or employees.
- h) Informs the Deputy Head, the Assistant Deputy Minister of Integrity Services Branch, and the Chief Privacy Officer of any security incidents involving personal information, and conducts internal investigations, including assessments and analyses, to minimize the risk of recurrence. Provides notification to other internal stakeholders, as required.
- i) In collaboration with the Chief Privacy Officer, establishes plans for the management of security incidents involving personal information.

Departmental IT Security Coordinator

- a) Establishes information technology security management processes and standards. Monitors compliance to those processes and standards.

- 
- b) Works jointly with the Departmental Security Officer to ensure that physical, personnel and information technology security stakeholders are coordinated to protect information and information technology assets.
 - c) Collaborates with the Departmental Security Officer on the implementation of safeguards to protect and secure the integrity, availability, intended use and value of electronically stored, processed or transmitted personal information as well as on the safeguards applied to the assets used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy personal information electronically.
 - d) Provides advice on information technology security requirements for Departmental programs and services.
 - e) Coordinates appropriate Innovation, Information and Technology Branch units in response to security incidents involving personal information.
 - f) Prepares information technology system certification reports and statements.
 - g) Consults with the Chief Privacy Officer on areas of mutual interest.
 - h) Consults with the Departmental Security Officer on areas of mutual interest to ensure an integrated approach for Departmental Security.

Assistant Deputy Ministers of Income Security and Social Development Branch, Learning Branch, and Skills and Employment Branch


- a) Apply the requirements of this policy in the policy development, program design and research activities in their respective branches.
- b) Incorporate the requirements of this policy, as necessary, in their functional policy direction and clarifications.
- c) Develop core privacy impact assessments for their respective branch's programs.
- d) Seek the Chief Privacy Officer's advice on privacy matters.

Assistant Deputy Minister of Strategic Policy and Research Branch

- a) Applies the requirements of this policy in policy analysis, research and evaluation activities involving the use of personal information.
- b) Exercises or performs the specific powers, duties or functions delegated by the Minister.
- c) Seeks the Chief Privacy Officer's advice on privacy matters.

Assistant Deputy Ministers of Citizen Service Branch, Integrity Services Branch, Program Operations Branch, and Processing and Payment Services Branch

- a) Apply the requirements of this policy in their respective program development, service offerings and implementation activities.

- 
- A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people, including individuals of various ages, ethnicities, and abilities, some using mobility aids like wheelchairs and strollers.
- b) Incorporate this policy's requirements, as necessary, in their respective branch's functional direction to the Regions.
 - c) Apply this policy's requirements in a coordinated and consistent manner within their respective business lines.
 - d) Plan, monitor and provide performance reports on privacy-related matters within their respective business lines in support of the Departmental privacy program.
 - e) Maintain linkages and networks to identify and report on privacy-related matters on behalf of their respective business lines.
 - f) Seek the Chief Privacy Officer's advice on privacy matters.

Assistant Deputy Minister of Service Management Branch

- a) Ensures the application of this policy, including its incorporation in functional direction, is applied in an integrated, consistent and coordinated manner across Service Canada and its Regions.
- b) Assesses and reviews the operational impacts and implementation of the Department's privacy requirements in Service Canada, including the Regions.
- c) Seeks the Chief Privacy Officer's advice on privacy matters, including privacy operations.

Regional Assistant Deputy Ministers

- a) Deliver privacy services in the regions.
- b) Implement the privacy provisions contained in functional direction.
- c) Implement this policy and the departmental privacy management program in the regions.
- d) Seek the Chief Privacy Officer's advice on privacy matters, including privacy service delivery.

Chief Financial Officer

- a) Works with the Chief Privacy Officer to ensure that all procurement documents (e.g., requests for quotation and requests for proposal) contracts and transactional arrangements, with either private or public sector entities, contain privacy safeguarding and protection provisions mandated by statute or policy.
- b) Consults with the Departmental Security Officer on areas of mutual interest to ensure an integrated approach for Departmental Security.

Assistant Deputy Minister, Human Resources

- a) Directly, or through human resources specialists, provides advice and guidance regarding appropriate measures for non-compliance with this policy.
- b) Provides advice and guidance regarding the interpretation of the ESDC *Code of Conduct* in matters related to the value of stewardship, specifically the responsible usage of resources by acquiring, preserving and sharing knowledge and information as appropriate.

A decorative header at the top of the page features a row of light blue silhouettes representing a diverse group of people. The silhouettes include individuals of various ages, a person in a wheelchair, a person with a cane, and a person pushing a stroller, set against a light blue background.

Senior General Counsel

- a) Provides legal advice and support on legal issues identified by the Department relating to the management and protection of personal information and privacy, including legal advice on the interpretation of relevant legislation and regulations, policy development, Departmental operations, and the handling of complaints under relevant legislation, as well as the provision of litigation support in respect of privacy-related litigation brought against the Department.

Chief Audit Executive

- a) Provides an independent and objective assurance service of the Department's privacy framework and privacy program to senior management.
- b) Reports on the adequacy of internal controls for the management of personal information, the extent to which personal information assets are accounted for, protected and safeguarded, and the level of compliance with legislation as well as Departmental and government-wide policies and regulations.
- c) Provides management with analyses, recommendations and information resulting from its audits and reviews.