Privacy Framework

Issue Date: October 2, 2003

Authority

The Freedom of Information and Protection of Privacy Act , Part IV, Sections 24 – 33
The Canadian Standards Association Model Code for the Protection of Personal Information, CAN/CSA-Q830-96 (CSA Code)
Cabinet Minute # 6168, February 19, 2003
CIC Board Minute 206/2003

Applicability

This policy applies to CIC and its subsidiary Crown Corporations

Purpose

The Policy:

- applies to personal information about the Crown sector's stakeholders that is collected, used and/or disclosed, in the course of business operations;
- applies to personal information retention and disposal;
- applies to the management of all personal information, regardless of whether oral, written and/or electronic; and
- remains subject to the requirements or provisions of any relevant legislation, regulations, contracts, agreements or court order or other lawfully binding arrangements.

Definitions

Collection - The act of gathering, acquiring, recording or obtaining personal information from any source, including third parties, by any means.

Consent - Voluntary agreement to the collection, use and disclosure of personal information for defined purposes. Consent may be express or implied and can be provided directly by the individual or that person's authorized representative. Express consent can be given orally, electronically or in writing, but is always unequivocal and does not require an inference on the part of the Crown corporation. Implied consent is consent that can reasonably be inferred from an individual's action or inaction.

Customer - An individual who:

- Uses, or applies to use, a Crown corporation's products or services; or
- Corresponds with a Crown corporation.

Disclosure - Making personal information available to others outside the organization.

Employee - An employee, pensioner or member of the Board of Directors of a Crown Corporation.

Information Management - The systematic control of records from their creation, or receipt, through their processing, distribution, organization, storage and retrieval to their disposition.

Interested Parties - Employees, customers, vendors, contractors, or other third parties who have provided personal information about themselves to the Crown corporation.

Personal Information - As per Section 24 of *The Freedom of Information and Protection of Privacy Act.*

Record(s) - Recorded information, regardless of medium (paper, computer disc, etc) or characteristics, created, received, retained or destroyed by an agency in support of its core business. A record may refer to a single document or group of documents in a file or file folder.

Records may be administrative (e.g. management of property, material, facilities, human resources, finances and information systems) or operational (e.g. records unique to each Crown related to specific services or functions as authorized by statute).

Security - The establishment and maintenance of measures to protect all corporate assets. Security is necessary for privacy, but the proper handling of personal information requires a broader set of privacy management functions.

Third Party - An individual, other than the interested party, or organization outside the Crown corporation.

Use - The treatment and handling of personal information within the Crown corporation.

Governance - Based on this overarching privacy framework, each Crown will have a governance model to suit its business and operational needs. The governance model will enable the corporation to integrate its privacy management program into its daily operations.

Policy Statements and Process

This framework provides guidance for a workable and sustainable privacy management approach. It is intended to:

- Guide Crown Investments Corporation (CIC) and subsidiary Crowns in the development and implementation of their respective policies, procedures, monitoring and reporting;
- Help ensure the protection of citizen's private information, balanced against the need to ensure the public and business mandates of the Crown sector can be effectively carried out;
- Help each Crown instill the confidence and trust of all stakeholders with respect to privacy management; and
- Support a culture of privacy management within the corporation.

The framework protects the personal information entrusted to Crown corporations and ensures that privacy management is an integral part of Crown corporation business.

The framework adopts and endorses the ten *CSA Code* Principles as the foundation for Crown sector privacy management. These principles are inter-related and each Crown corporation's privacy management program will elaborate upon these principles to meet individual organizational and operational needs.

- **Accountability**: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

- **Identifying Purposes**: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
- **Consent**: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
- **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
- **Limiting Use, Disclosure and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as along as necessary for the fulfillment of those purposes.
- **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
- **Safeguards**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- **Openness**: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Each Crown corporation will appoint a Chief Privacy Officer (CPO). As the CPO, he/she will be empowered to develop and implement the corporation's privacy management program.

The primary role of the CPO is to ensure the legal framework, policies, procedures and standards are in place to protect personal information in the Crown corporation. The CPO will ensure the adequacy of the framework, and monitor, evaluate and report on implementation and ongoing effectiveness of the Crown's privacy management program.

As part of the governance model, the CPO's roles and responsibilities may be delegated to others as required. The person assigned as CPO may have other responsibilities provided they are not in conflict of interest with his/her CPO role.

Privacy Management Program

Crown corporations will develop and maintain a privacy management program. Privacy management must be built through specific initiatives or actions that integrate privacy management into day-to-day corporate operations (see Appendix A for more detail).

The primary elements are:

Management Element

Policy and process – the design and architecture to achieve business privacy requirements and business needs; guidance and confirmation with the CPO and Steering Committee (if applicable)

Administration – to implement the business solutions, ensure quality control and handle privacy requests, inquiries and complaints

Control – integration of systems with core business processes; monitor, react and measure the privacy process itself

Integration Element

Build – actual implementation of actions required to support privacy policy and/or compliance with privacy requirements. Designs, tests and implements actions into an operational model (e.g. linkage of privacy management with security management, integration of privacy education with a code of conduct).

Maintain and Sustain – development and implementation of the day-to-day actions for ongoing privacy management, linking with the governance layer. This includes performance measures to help identify and address those areas that may require improvement.

Summary

Each Crown corporation will be responsible and accountable for the development, implementation and compliance monitoring of its privacy management program.

Administrative Information

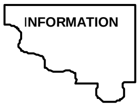
Chief Privacy Officer: Senior Vice-President and General Counsel, CIC 787-5892

Reviewed: February 4, 2016

Appendix A

Framework Layer - Key Components

<u>Information</u>

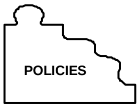


The critical and mandatory first step in the process is conducting an internal privacy and security audit and gap analysis. This includes, among other things, the following:

- Taking inventory of existing information: what information is held by the corporation, why it is held, where it is and who owns it;
- Taking inventory of existing privacy practices: why do we have the information we have, and how is it used. What happens to the information once it is given to the corporation (this includes an analysis of creation, importation, manipulation, copying, sharing, archiving, backing up, and destruction);
- Developing a classification system for information;
- Gap analysis: what policies and procedures must be put in place to align with privacy legislation?

The audit and gap analysis is a risk-assessment tool for decision-makers to address the legal, moral and ethical issues posed by the personal information held by the corporation. It provides a snapshot of how well the organization is protecting the privacy of its interested parties.

<u>Policies and Process</u>



Policies are the fundamental building blocks of the privacy framework. Generally speaking, policies are the corporate-wide guidelines for staff outlining their responsibility for the management and protection of corporate data, information and assets. Policies also control the actions and reactions of the corporation's processes for the handling of data. The privacy framework requires clearly defined policies, processes and procedures.

To be effective, policies must be easy to implement and enforce. As such, they must be concise and easily understandable. Also crucial is the need to balance the protection sought with productivity requirements. And finally, policies must be updated on a regular basis to reflect the changing needs of interested parties and the organization.

Any policies developed must clearly state why they are needed, and describe what is covered (whom, what, where, when, and how). These policies must discuss the appropriate contacts and discuss how violations will be handled.

<u>People</u>

For the privacy framework to be successful, Crown staff must have the appropriate direction and guidance. Privacy must permeate every part of the corporation to facilitate compliance and add value to the privacy framework. As such, privacy and security education is mandatory to ensure a common understanding of the basic principles and this knowledge is updated on a regular basis.

Staff will need process-driven guidance that is controlled by policy. Critical to the success of the privacy framework is clarification for the staff of what constitutes sensitive personal and corporate information.

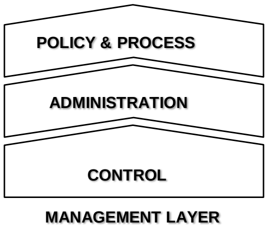
The privacy framework will take shape once staff and processes are linked by adopted and well-communicated corporate-wide policies.

Technology

Technology should be viewed as the privacy framework enabler. Technology is the key to automating the policies and procedures developed in the privacy framework. It helps to guide people through their policy and process driven tasks.

Technology can be used to effectively implement security to discourage the improper use of information.

Privacy Management



There are three layers to privacy management:

- Privacy Policy and Process Management - This would be under the mandate of the Chief Privacy Officer and the Steering Committee, if established.
  The purpose of the Committee would be to define business needs and architect solutions.
- Privacy Administration - This involves implementing the business solutions and managing the quality control of the processes put in place to solve the business requirements. It also concerns itself with processing privacy inquiries or complaints
- Privacy Control - This level of management concerns itself with systems integration from end-to-end, as well as compliance monitoring (performance measurement)

Integration with Systems

The privacy framework requires linkage to other systems, such as:

- Asset and inventory management – relates to all corporate assets (hardware, software, intellectual capital, equipment, etc); what is currently in place, how many are there, what is changing, what is being created
- Configuration management – the control data on each asset, describing what it is, who has it, purpose, etc.
- Incident management – activities related to privacy and security incident reporting and management
- Problem management – management of unresolved incidents
- Change management – handling of process and procedural changes to ensure incident prevention and compliance with privacy standards; generally achieved through application of an assessment tool
- Application management – specific aspect of change management
- Security management – physical security of corporate assets

Completing the Privacy Framework

The privacy framework is operational when all of the above elements have been fully integrated. Privacy management is an ongoing process requiring continued evaluation, maintenance and/or adjustment to emerging developments.