An Overarching Personal Information Privacy Framework For Executive Government

Province of Saskatchewan

September 2, 2003

Table of Contents

Introduction

On February 12, 2003, Deloitte & Touche submitted to the Government of Saskatchewan the report, Government of Saskatchewan, Privacy Assessment. After conducting Privacy Assessments on 17 departments and Crown Corporations, the report identified a number of potential next steps and made 11 recommendations to Government as a whole. These eleven recommendations were in addition to the several recommendations made to each of the 17 departments and Crown Corporations.

The first recommendation was:

> "1. Overarching Privacy Framework – The Government of Saskatchewan should develop an overarching privacy framework including supporting policies for all of the government departments and Crown Corporations that we examined. This Privacy Framework should recognize the need to balance privacy rights of the individual with respect to their personal information and the legitimate needs of the departments and the Crown Corporations in fulfilling their public interest mandate." (p. 13)

On Thursday, February 20th, the government announced it would make changes to strengthen its privacy policies and procedures. Also, it announced that it would implement all 11 recommendations made in the Deloitte & Touche report, including the development of an overarching privacy policy for Executive Government. It also announced that Crown Corporations would follow a parallel path within each Corporation.

This Privacy Framework (this "Framework") fulfills the commitment of government to develop an overarching privacy framework.

This Framework is the overarching corporate government mechanism for setting out its direction with respect to privacy matters. It is intended to ensure a balance between the privacy rights of individuals with respect to personal information and the legitimate needs of government departments and agencies in fulfilling their public interest mandate. At the same time, the purpose is to raise, for individual citizens, the level of protection of their personal information.

The intended audience of this document is Executive Government. The main intent is to state the privacy policy expectations of government and to provide this Framework for the implementation of those policy directions. This is also a public document provided to inform citizens about what is being done to protect personal information.

The objectives of this Framework are to:

- Support the development and implementation of specific policies and procedures that recognize the particular circumstances of the departments and agencies.

- Support the focussed development and implementation of consistent personal information policies and procedures.

- Provide benchmarks for the adoption and implementation of the personal information policies and procedures.

- Provide processes for identifying and addressing inadequacies in the existing privacy policies, standards and practices, now and into the future.

In order to achieve these objectives, this Framework is comprised of a vision, principles, and goals that guide further policy development. Further, it provides objectives, benchmarks, and actions aimed at achieving the vision. It does not provide the policies that result from the identified actions. Rather it provides the vision, principles, and context for these policies to be developed over the next few years. This Framework provides a common basis for policy development at the department or agency level.

This document sets out the Privacy Framework as a permanent, yet continually developing statement of direction and action.

Background and Context

Over the past several years the Province of Saskatchewan has been addressing the issues of access to information and privacy. These actions include the passage of *The Freedom of Information and Protection of Privacy Act*, its implementation, and a number of initiatives related to Information Technology Enterprise Architecture and Security. As a complement to *The Freedom of Information and Protection of Privacy Act* that applies to the Government of Saskatchewan, *The Local Authority Freedom of Information and Protection of Privacy Act* was passed at about the same time. This is an act respecting a right of access to documents of local authorities and a right of privacy with respect to personal information held by local authorities. In many ways these efforts parallel initiatives in other provinces in Canada and around the world.

In Canada, a significant development has been the establishment by the Canadian Standards Association of the *Model Code for the Protection of Personal Information – Q830* (the "CSA Model Code"). The CSA Model Code provides for a set of principles, guidelines and implementation supports for organizations to adopt or adapt and has proven useful in the developing this Framework.

The Federal Government's *Personal Information Protection and Electronic Documents Act* (PIPEDA) attaches the CSA Model Code's 10 principles as Schedule 1 and states (section 5) "…every organization shall comply with the obligations set out in Schedule 1." It goes on to make a number of relatively minor exceptions to the principles. This legislation does not apply to provincial governments.

As with any government initiative, the following conditions are necessary for successful actualization of the initiative:

- The presence of the appropriate legislative authority;
- The appropriate policies, and procedures to add precision to the legislative authority;
- The organizational structures and mandates to effectively carry out the directions;
- The appropriate implementation strategies; and
- The evaluation or accountability system to continually monitor compliance and effectiveness of the initiative.

Similar to other organizations in Canada, the Saskatchewan government experience has evolved over the last decade or more. In the early 1990's the emphasis was on access to information. Although in this province the legislation is *The Freedom of Information and Protection of Privacy Act*, the emphasis was on the freedom of information and it is commonly referred to as the "Freedom of Information Act" or "FOI Act". The implementation processes surrounding the Act were extensive and effective. The limitation appears to be the continuing maintenance and support given to the initiative and the level of evaluation and monitoring. At the same time, the issue of protection of privacy was becoming an ever more dominant issue in the minds of the public.

This Privacy Framework is designed to place Saskatchewan at the strongest possible privacy protection policy position, while balancing the Government's need to meet its public policy obligations.

Scope

The development of a Privacy Framework requires a clear specification of the scope of this Framework. To provide that clarity, six different questions are addressed. They are:

1. Legislative Basis for Privacy - What is the legislative context for the issue of privacy and the implementation of a Privacy Framework?
2. Information Privacy - What is privacy?
3. Government of Saskatchewan - To which parts of government does this Framework apply?
4. Personal Information - What is personal information?
5. Personal Information – Management Information - What is the difference between these?
6. Electronic Versus Other Media - Does this Privacy Framework apply to only electronic information or all information held by government?

1. Legislative Basis for Privacy - What is the legislative context for the issue of privacy and the implementation of a Privacy Framework?

The starting point for this Framework is full compliance with all legislation governing the protection of personal information in the possession or control of government. There are many legislative enactments that touch upon the issue of privacy, some of which are described in more detail below.

The Freedom of Information and Protection of Privacy Act provides rules for the government regarding the collection, use, disclosure and overall protection of personal information and for access to information held by the government.

The Local Authority Freedom of Information and Protection of Privacy Act is similar to *The Freedom of Information and Protection of Privacy Act*, but applies to local governments, such as municipalities, rather than the provincial government.

The Health Information Protection Act (HIPA) was passed in 1999, amended during the 2003 legislative session, and is in force as of September 1, 2003. It applies to personal health information held by government and other service providers in the Health sector and provides rules regarding the collection, use, disclosure and overall protection of personal health information.

The Archives Act, passed in 1945, was the first legislated attempt by government in Saskatchewan to preserve historical records for future generations. *The Archives Act* and its support system, the Administrative Records Management System (ARMS) and the Operational Records System (ORS), have been developed, in part, as a response to the passage of *The Freedom of Information and Protection of Privacy Act*. These records management systems allow for the development of record schedules that impose timelines for the retention and disposal of government records. These timelines or "retention periods" are determined in relation to legal, audit, and privacy requirements.

In general, the thrust of modern privacy regimes is to ensure that personal information in the hands of government is not retained longer than necessary. Departments and agencies will need to consider this as they implement ARMS and ORS.

The Electronic Information and Documents Act establishes the legal recognition of electronic information in signing of contracts, and filing information electronically. This highlights the need to treat electronic records in much the same fashion, from a privacy perspective, as paper records.

The Privacy Act permits the commencement of a legal action against any person who wilfully violates the privacy of another person.

The Public Disclosure Act sets out the processes and parameters for disclosing information about individuals who pose a significant risk of serious harm to other persons.

In addition to the acts listed above, there are several acts that have provisions that speak to confidentiality and other matters related to privacy. Examples of these acts are, *The Child and Family Services Act, The Adoption Act, The Public Health Act*, and *The Mental Health Services Act.*

Knowledge of these legislative enactments is important to the understanding and implementation of this Framework. This Framework has been designed to build on the current legislation, but in case of conflict of interpretation the Acts shall prevail.

2. Information Privacy – What is privacy?

Privacy can be thought of in terms of personal privacy and information privacy (Provincial Auditor, Spring 2000, p. 168). Personal privacy is about the rights of the individual to be protected against intrusion. Protection of personal privacy involves safeguards with respect to such things as search and seizure, and obtaining tissues samples. This Privacy Framework addresses information privacy.

This Framework is about information privacy in the Government of Saskatchewan, not about the private sector or another level of government. Information Privacy is defined as:

> The ability of an identifiable individual to control the collection, use, and disclosure of any recorded information about themselves held by the Government of Saskatchewan or third parties on behalf of the Government of Saskatchewan.

3. Government of Saskatchewan – To which parts of government does this Framework apply?

This Privacy Framework applies to all departments and agencies of executive government. Further, all boards, commissions, and other bodies that have been prescribed as "Government Institutions" under *The Freedom of Information and Protection of Privacy Regulations* are expected to comply with and adopt this

Framework. A list of these boards, commissions and other bodies can be found in Appendix A. The Framework does not apply to CIC Crown Corporations.

The Privacy Framework applies to all applicable information whether the information is held directly by government, held by government as supplied by third parties, or held by third parties on behalf of government.

4. What Constitutes Personal Information and Personal Health Information?

Personal Information is defined in section 24 of *The Freedom of Information and Protection of Privacy Act* (the FOI Act). Personal Health Information is defined in section 2 of *The Health Information Protection Act* (HIPA) and is a subset of Personal Information that relates to information provided or generated in the delivery of health services. Each piece of legislation then creates rules specifying when government can collect it, how it can use that information, and to whom the information can be disclosed. For the purposes of this Framework, a reference to personal information includes personal health information.

The definitions in the FOI Act and HIPA are very specific and must be consulted to determine whether a piece of information is personal information or personal health information. For the purposes of this commentary, however, we will generalize the definitions.

Personal Information: In its most basic form, personal information is any recorded information about an identifiable person. This can be as simple as a person's name and address or a person's name and place of employment. As a rule of thumb, if the information identifies an individual, is not otherwise publicly available and identifies something about that person, it is likely personal information.

However, not all information that fits the above description is personal information. The FOI Act removes the following types of information from the definition of personal information:

- Information about the salary, expenses, job responsibilities or job classification of a person employed by or under contract with the government is not personal information.
- An opinion expressed by a person about someone else is not personal information about the person who gave the opinion. It is personal information of the person who the opinion is expressed about.
- The details of a license granted by the government. For example if a license was issued to Mrs. Smith to operate a personal care home, the fact that she operates such a home, its' location and whatever other details are on the license are not personal information about Mrs. Smith.
- The amount of a grant or other discretionary payment made to a person by the government is not personal information about the person to whom the grant or benefit was paid.
- Expenses that the government paid for a person travelling at government expense.
- Information about a corporation is not personal information. (this does not mean

it does not need to be protected, rather that it is not governed by the rules for personal information).

- Personal information which has had the identifying factors removed such that one can't identify the person whom it is about, is no longer personal information.

Also the government operates various public registries from which information can be obtained (e.g. - Land Titles Office, Personal Property Registry, Corporations Branch). The Act does not interfere with the disclosure of personal information from those registries.

Personal Health Information: is a subset of personal information that relates to information provided or generated in the delivery of health services. It includes information about the physical or mental health of an identifiable individual; information with respect to a health service provided to an identifiable individual and information collected incidental to providing health services to that individual, including information collected to register an individual for a health service. Information which has had personal identifiers removed such that it is not reasonable to conclude that a person could be identified from the information is not personal health information.

One must be aware that the same piece of information can be personal information in one setting and personal health information in another. For example, a person's name and address in the possession of the Department of Finance for income tax purposes constitute personal information under the FOI Act. However, that same piece of information given to Saskatchewan Health to register the person for health services is personal health information under HIPA. The key is for what purpose the information was provided or generated. If it was for a health services purpose, HIPA will apply. While the rules for collection, use, and disclosure under the two legislative enactments are similar, they are not the same. Therefore, it is important to know which piece of legislation is applicable to the information.

5. Personal Information - Management Information – What is the difference between these?

Given a reasonably clear definition of what personal information is and is not, an equally important task is to position this framework and personal information within the broader terms of management information and corporate information.

For some time, officials within the Government of Saskatchewan have been working towards establishing the Government of Saskatchewan Enterprise Architecture (Enterprise Architecture). The effort to develop the Enterprise Architecture is aimed at providing government-wide principles, standards, and policies to direct and guide the development of management information and technology systems.

The Enterprise Architecture addresses high-level matters, in an effort to ensure management information and technology systems are developed on the basis of the business needs of government. It also addresses detailed matters in order to provide specific guidance to management information and technology specialists across

government. The aim is to ensure government is making the most efficient use of its limited management information and technology resources.

Personal information fits into this hierarchy of information types as follows: Enterprise Architecture is the broadest term representing all of the principles, standards and policies that guide a broad spectrum of considerations with respect to management information and technology development. Management information is one component of the Enterprise Architecture and includes all types of information whether they are personal or corporate. Personal information is one component of management information, and applies to information about identifiable individuals only.

What is common between matters of management information and personal information is the issue of privacy. Both types of information require the government to take measures to protect that information. Although many of the measures that protect privacy of individuals and corporations are similar, their legislative bases are different. Therefore, this Privacy Framework applies only to the matter of personal information within the context of a broader enterprise architecture system.

6. Electronic Versus Other Media - Does this Privacy Framework apply to only electronic information or all information held by government?

The Privacy Framework applies to all personal information collected by executive government whether it is stored in electronic or other means.

Vision

Within Executive Government, a culture of privacy protection is fostered and developed by ensuring that personal information is: a) collected, used, and disclosed only as required to carry out the government's legitimate business and public interest mandates; and b) properly protected through the use of appropriate security mechanisms.

Saskatchewan's Privacy Principles

An important component of most policy frameworks is the set of principles that provide a guide to more specific goals, objectives, benchmarks, and actions. Nationally and internationally, the development of privacy principles has been the subject of extensive study for well over twenty years. The results of this study provided numerous models to draw from in the development of Saskatchewan's Privacy Principles.

In Saskatchewan, *The Freedom of Information and Protection of Privacy Act* implicitly adopted a set of principles that was the fundamental building block for the explicit principles outlined below.

The other primary reference point for Saskatchewan's Privacy Principles has been the privacy protection principles included in the CSA Model Code. The ten principles in this voluntary code were established in 1996 and were intended for use by any organization involved in the collection, use, or disclosure of private information. Most subsequent efforts to develop privacy principles have used these principles as a significant reference point. The Saskatchewan Privacy Principles draw heavily upon the CSA Model Code principles.

There are a number of reasons why the CSA Model Code principles were adapted, rather than adopted in this Privacy Framework. The three main reasons are summarized as follows:

1. Since 1991, Saskatchewan has had *The Freedom of Information and Protection of Privacy Act* that provides a strong legislative basis upon which the Government of Saskatchewan Privacy Framework can build.

2. Within Government, some adhere to the view that the CSA Model Code was really intended for the private sector. The fact no provincial government has formally adopted it, and that it forms the basis of the federal government's private sector privacy legislation (PIPEDA), is cited to support this view. In the public sector, there is a greater obligation to make information available than there is in the private sector and the belief is that adopting private sector principles may cause the Government unexpected difficulties. For example, information about pay and duties for public sector employees is a matter of public record and is not considered personal information. Further, government has a mandate to maintain public registries that contain personal information (e.g. personal and property registries, and corporation registries) that require the making of certain personal information publicly available.

3. Adopting the CSA Model Code principles may infer that the Government will abide by any subsequent changes to these principles, regardless as to what the impact of these changes may be on Government. Adopting principles that have been specifically developed for Government ensures Cabinet retains control over changes that may be required from time to time.

This difference between public sector and private sector, and even more broadly the need for individual organizations to adapt the principles was recognized when CSA stated it is the "… responsibility of the users of the Standard to judge its suitability for their particular purpose." (CSA, *Model Code for the Protection of Personal Information – Q830*, 1996, p.vii).

The CSA Model Code principles are a valuable reference point for the Saskatchewan Privacy Principles. Finding the balance between the protection of personal information and the legitimate need of government to fulfill its public interest mandate is achieved by a set of principles, goals, benchmarks, and actions specifically developed for the Government of Saskatchewan.

Thus, the eleven interrelated Saskatchewan Privacy Principles that form the basis of the Privacy Framework are unique to the Saskatchewan government, but draw heavily on other sources. Each principle is comprised of a brief statement of principle, followed by a commentary that elaborates and aids in the interpretation of the principle. The commentary often includes a reference to sections of *The Freedom of Information and Protection of Privacy Act* and/or *The Health Information Protection Act* that are relevant to the principle. The principles are generalized statements of intent to which government aspires. General statements cannot address the myriad of specific circumstances which government faces in relation to personal information in its day-to-day operation and administration. Accordingly, the principles do not preclude the government from taking any action with respect to personal information that it is authorized to do in legislation.

The Saskatchewan Privacy Principles are:

1. Accountability

Each Government of Saskatchewan department or agency is responsible for personal information under its control.

Commentary

This principle applies to situations where departments and agencies are in possession of personal information or in situations where departments or agencies have provided the information to third parties.

Each Department or agency will designate one or more of its officials to be responsible for ensuring the department or agency's compliance with these principles.

2. Purpose

The purpose, for which personal information is collected, shall be identified at or before the time the information is collected.

Commentary

The department or agency shall document the purposes for which the information is collected.

Depending on the way in which the information is collected, identifying the purpose of collection can be done orally or in writing.

Legislative Reference

Section 25 of *The Freedom of Information and Protection of Privacy Act* prohibits a government institution from collecting personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.

Section 26(2) of *The Freedom of Information and Protection of Privacy Act* requires a government institution to tell the individual what the purpose for the information is, unless the information is exempted by the regulations.

In relation to personal health information, section 9 of *The Health Information Protection Act* requires a government institution to take reasonable steps when collecting personal health information directly from an individual to tell the individual the anticipated uses and disclosures of the information. Section 24 of that Act provides the purposes for which a government institution can collect personal health information.

3. Limiting Consent

Obtaining consent from the individual is the expected approach for the collection, use, and disclosure of personal information, but it is not always feasible, appropriate, or the only legal means of authority.

Commentary

The way in which a department or agency obtains consent may vary, depending on the circumstances and the type of information collected. When consent is required, a department or agency should seek informed consent.
This is achieved when an individual is informed of the purpose for collection, and how the information will be used or disclosed.

When collecting personal health information, individuals must be informed of anticipated use and disclosure of the information. This results in an informed consent, in circumstances where consent is required by HIPA. HIPA does not always require consent for use or disclosure but collection must still be informed.

Individuals can give consent in many ways. For example:

a) a person may provide a specific written consent for the proposed collection, use or disclosure. This could be part of an application form for services or programs, or a separate document;
b) an electronic application form may inform the individual of the reason for collection and the expected uses and disclosures that will be made of the information. By completing and sending the form, the individual is impliedly consenting to the collection and the specified uses;
c) for personal health information, HIPA allows consent to be deemed to exist, or if expressed, to be oral or written; however, for personal information, the FOI Act only permits oral consent in exceptional cases; or
d) consent may be obtained at the time that individuals use a service.

In general, consent must be obtained from the person to whom the information relates. However, legally authorized representatives (such as a legal guardian for minors, a person having power of attorney or a personal guardianship order from the court) may be able to give consent on behalf of another.

It is important for government to strive to obtain informed written consent where such is reasonably practical.

Legislative Reference

Section 26(1) of *The Freedom of Information and Protection of Privacy Act* requires a government institution to collect personal information directly from the individual to whom it relates, where practicable. This requirement has a number of exceptions mostly related to law enforcement activities.

Section 28 of *The Freedom of Information and Protection of Privacy Act* restricts a government institution's use of personal information to those purposes for which it was obtained or compiled or for a use consistent with that purpose.

Section 29 of *The Freedom of Information and Protection of Privacy Act* prohibits the disclosure of personal information by a government institution, unless the individual to whom it relates consents to the disclosure. There are a number of exceptions, with safe guards, relating to a number of situations from law enforcement to research.

Sections 5, 6 and 7 of *The Health Information Protection Act* provide rules for consent when required by the Act. In addition, sections 26 and 27 allow a government institution to use or disclose personal health information with expressed consent for any purpose; with 'deemed consent' (i.e. - the Act deems consent to exist) in certain circumstances mostly related to the purpose the personal health information was originally collected, including the provision of a health service; and without consent (but with safeguards) in limited circumstances.

4. Collection

The collection of personal information shall be limited to that which is necessary for the purposes being supported.

Commentary

Limits on the collection of personal information must be incorporated into the design of information systems to ensure that extraneous or unnecessary information is not collected. These limits apply to both the amount and type of information collected.

5. Use and Disclosure

Personal information shall be used or disclosed only for the purposes for which it was collected or for a use consistent with that purpose, except with the consent of the individual or as specifically authorized by law.

Commentary

To help ensure compliance with this principle, it is a good idea to take steps to limit the access of employees to personal information to only those who can be reasonably expected to require the information to perform their job duties.

Legislative Reference

Section 28 of *The Freedom of Information and Protection of Privacy Act* restricts a government institution's use of personal information to those purposes for which it was obtained or compiled or for a use consistent with that purpose or for a purpose for which information can be disclosed.

Section 29 of *The Freedom of Information and Protection of Privacy Act* prohibits the disclosure of personal information by a government institution, unless the individual to whom it relates consents to the disclosure. There are a number of exceptions, with safe guards, relating to a number of situations from law enforcement to research.

Sections 26 and 27 of *The Health Information Protection Act* limit the use and disclosure of personal health information to purposes for which an individual gives consent. The Act states that consent is already deemed to exist when using or disclosing for the purpose for which the information was collected, a consistent purpose and for provision of service requested or required by the individual. There are also exceptions where personal health information may be used or disclosed without expressed or deemed consent.

Various pieces of legislation have specific rules regarding disclosure of information governed by those Acts. For example, *The Child and Family Services Act* has specific rules regarding information generated under that Act.

6. Retention

Personal information should be retained only as long as necessary for the fulfillment of its stated collection purpose, or as specified by law.

Commentary

Departments and agencies should use record schedules developed under ARMS and ORS as a means of ensuring all factors, including privacy, are taken into account when establishing appropriate retention periods for a class of document. Departments and agencies should prepare the necessary disposal requests once documents have served their applicable retention periods. This will ensure that private information contained in such documents is not retained any longer than is necessary.

Legislative Reference

Section 7 of *The Archives Act* specifies that all public documents be preserved by the department to whose business they belong until their transfer to the Saskatchewan Archives Board or they are authorized to be destroyed as outlined in section 11 of the *Act*.

Personal health information must be retained or disposed of as outlined in section 17 of *The Health Information Protection Act*.

The Archives Act defines a public document as "… correspondence, maps, photographs and all other documents created in the administration of the public affairs of Saskatchewan except copies of documents created only for convenience of reference and surplus copies …" While the definition does not expressly address the issue of electronic records, the definition is interpreted by government to include such records.

7. Accuracy

Personal information shall be as accurate, complete, and up-to-date as is reasonably necessary for the purposes for which it is to be used.

Commentary

The extent to which personal information is accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

When updating personal information, always consider the reason or purpose it was collected. It is not necessary to routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Legislative Reference

Section 27 of *The Freedom of Information and Protection of Privacy Act* requires government institutions to keep personal information as accurate and complete as reasonably possible.

Section 32 of *The Freedom of Information and Protection of Privacy Act* gives an individual the right to request that a record containing personal information be corrected. If the government institution refuses to make the requested correction, the individual may require a notation to be made on the record.

In relation to personal health information, sections 13 and 40 of *The Health Information Protection Act* provide for the ability of an individual to request amendment to a record of personal health information and to require a notation to be made on the record if the request is refused. Section 19 requires government institutions to take reasonable steps to ensure the personal health information it collects is accurate.

8. Safeguards

Appropriate security safeguards shall protect personal information.

Commentary

Methods of security safeguards should include: (a) physical measures, for example locked filing cabinets and restricted access to offices;
(b) organizational measures, for example, security clearances and limiting access on a need to know basis; and (c) technological measures, for example, the use of passwords and encryption.

Care should be taken in the disposal and destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Legislative Reference

Section 16 of *The Health Information Protection Act* requires that government institutions take steps to protect the accuracy, integrity and security of personal health information in its possession.

9. Openness

The privacy principles, and the policies and procedures relating to their implementation should be readily available.

Commentary

The information available should include: (a) the name/title and address of the person who is accountable for the organization's policies and procedures and to whom complaints or inquiries can be forwarded; (b) the means of gaining access to personal information held by the department or agency; (c) a description of the type of personal information held by the department or agency; (d) a copy of any brochures or other information that explain the departments or agency policies and procedures; and (e) what personal information is made available to related organizations or third parties.

10. Access

Upon request, an individual shall be given access to their personal information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Commentary

There are exceptions, as specified in *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act.*

Legislative Reference

Section 31 of *The Freedom of Information and Protection of Privacy Act* gives individuals the right of access, in accordance with the access provisions of the Act, to any records in the possession or under the control of a government institution that contain personal information about the individual, subject to the exceptions listed in the section.

In relation to personal health information, sections 12 and 32 of *The Health Information Protection Act* provide individuals with a right to access their personal health information, subject to the exceptions listed in section 38 of the Act.

11. Compliance

An individual may challenge a department or agency's compliance with these principles by contacting one of the responsible officials identified under the first principle.

Commentary

Departments and agencies shall designate a person who is responsible for receiving any question or concerns respecting the department or agency's compliance with the Principles.

An individual who questions whether a department or agency is complying with the Principles may contact the designated person with the concern. All concerns shall be investigated and result in a letter of response provided to the individual who has raised the concern. If the concern is substantiated the designated person shall ensure that steps are taken within the department or agency to bring its practices in line with the Principles.

In other cases, where the department or agency is not complying with the Principles but is still in compliance with legislation, an explanation shall be provided.

Goals, Objectives, Benchmarks, and Actions

The Privacy Principles, in conjunction with the Commentary and the Legislative References, provide a foundation for action in government with respect to personal information. In order for this Framework to be complete, the following pages provide goals, objectives and actions. To be clear with respect to accountability and expectations, a set of benchmarks are also included.

These components are presented in a tabular form. The tabular representation provides a generally linear representation of the balance between the protection of the individual citizen's personal information and the legitimate government need to fulfill its public interest mandate.

To some extent the linear representation is appropriate. The required balance can only be achieved if the principles are adopted and the accountability regime is in place. On the other hand, individuals within government have been dealing with issues of personal information, privacy, and security for a number of years. This Framework is intended to put an overall policy perspective on these activities, in order to achieve greater clarity, effectiveness, and efficiency. The implementation initiative does not need to be conducted in a linear fashion. In fact, action should not be bottlenecked at any particular point.

Included in the tabular display is frequent reference to appendices to the document. These appendices profile more detail on a number of matters that extend to the implementation level. The provision of these appendices should make the implementation activities easier. In some cases the appendices include works in progress, in that sense this Framework is a work in progress, but only from an implementation perspective. The Vision, Principles, Goals, Objectives, and Actions, once adopted are not works in progress. The tools and supports for implementation, however, are works in progress.

GOAL #1:

Accountability for the protection of personal information in Executive Government is clear and effective.

Objective	Benchmarks	Actions
1a. Executive government has clear lines of accountability with respect to personal information protection. 1b. Departments and agencies are accountable for compliance with the Privacy Framework.	Source: Deloitte & Touche Report Baseline: Two departments and agencies have a designated Privacy Officer. Short term: Executive government has identified accountability lines for the protection of personal information, and all departments and agencies have a designated Privacy Officer by October 1, 2003. Long Term: The list of designated Privacy Officers is updated annually.	1. Executive government will identify lines of accountability for the protection of personal information. 2. Executive Government will designate a Chief Privacy Officer (CPO) to monitor compliance with this Privacy Framework and each department and agency will designate a departmental or agency Privacy Officer (PO), to ensure organizational compliance with the Privacy Framework. Proposed job descriptions for the Chief Privacy Officer and Privacy Officers are included in Appendix B and C, respectively. 3. The Chief Privacy Officer (CPO) will maintain a Government of Saskatchewan Privacy Protection Checklist (see Appendix D for a draft Checklist) and will receive annual department and agency compliance reports with respect to the Checklist. The CPO will prepare a summary report for the Deputy Minister to the Premier who will provide any needed direction to the department or agency permanent head.
1c. Personal information transferred to or from third parties is protected, including F/P/T agreements.	Source: Deloitte & Touche Report Baseline: There is no standard clause in outsourcing contracts that ensure personal information protection. There is no centralized review	4. Justice, in conjunction with, Saskatchewan Property Management Corporation (SPMC), and the Information Technology Office (ITO) will develop a set of contractual guidelines

	process to ensure outsourcing contracts include a clause to protect personal information. Short term: By January 1, 2004, each department and agency reviews all outsourcing contracts to ensure they include an appropriate privacy protection clause. Long Term: By September 1, 2004, all outsourcing contracts have adequate privacy protection clauses, and are filed with the departmental or agency Privacy Officer. By April 1, 2005, each department and agency has updated its data handling procedures in accordance with the ITO standards.	and checklists to assist departments in developing clauses to ensure that personal information is protected and adequately addressed in contractual agreements. 5. Managers in Departments and Agencies will ensure that the privacy requirements are met in all outsourcing contracts. 6. The Chief Information Officer (CIO) will develop a standard set of data handling procedures that govern the protection/security of personal information transmitted/transported internally and to third party contractors.
1d. Departments and agencies have policies and procedures in place, which protect personal information. 1e. Department and agency staff is capable and trained in privacy policies and procedures.	Source: Deloitte & Touche Report Baseline: In many cases, departments and agencies have procedures that are informal, but do not specifically address privacy matters. Executive Government has an Acceptable Use Policy. Short Term: By January 1, 2004, government departments and agencies have adopted the Privacy Framework. Long Term: By September 1, 2004, all staffs are trained on privacy policies and procedures.	7. All departments and agencies will adopt the Privacy Framework. 8. Under the leadership of the Public Service Commission, all departments and agencies will implement staff freedom of information and protection of privacy education and awareness building according to the options provided by the Commission. 9. Under the leadership of the Public Service Commission, departments and agencies should develop methods for employees to regularly confirm their understanding of privacy protection.

GOAL #2:

Personal information is collected, used, disclosed, and retained for the purpose of meeting legitimate department and agency mandates, in accordance with the law.

Objective	Benchmarks	Actions
2a. The purposes of collecting personal information are clear. 2b. Personal information is only collected to meet legitimate program purposes. 2c. Personal information is used and disclosed for the purposes for which it was collected. 2d. Personal information is retained only as long as is necessary to fulfill the business purpose, and to meet legal obligations.	Source: Deloitte & Touche Report Baseline: Departments or agencies do not routinely formally document the purposes for which personal information is collected. Departments or agencies do not routinely review retention and destruction policies with current privacy policies in mind. Short Term: All new programs that collect personal information will include an explanation of the purpose, use, retention and disclosure of the information. Long Term: By April 1, 2006 all programs that collect personal information will include an explanation of the purpose, use, retention and disclosure of the information.	10. The Saskatchewan Access Directory will be revised to reflect this Framework and provide a more complete annotated inventory of personal information residing in departments and agencies. 11. Policies and procedures will be established and implemented for documenting the purposes for the collection, use, disclosure, and retention of personal information in all programs. Departments and Agencies should consider up-dating old record schedules in accordance with ARMS and ORS. Legislative requirements for disposing of records must be followed.

GOAL #3: Personal information is obtained with appropriate authority and consent.		
Objective	Benchmarks	Actions
3a. Personal information is obtained with the appropriate authority. 3b. Personal information is obtained with the informed consent of the individual, wherever appropriate.	Source: Deloitte and Touche Report Baseline: In the majority of cases departments and agencies use written but implied consent as part of the application process to access the programs that support their mandates. Short Term: By September 1, 2004 all programs have documented the authority under which the personal information is collected. Long Term: By April 1, 2006, wherever appropriate all programs that collect personal information will include an explanation of the purpose, use, disclosure, and retention of the information.	12. Departments and agencies will review their collection policies to ensure they have authority to collect such information. 13. Departments and agencies will review their consent processes to ensure informed consent is obtained, wherever appropriate.

Goal #4: Personal information is sufficiently accurate, up-to-date and complete to fulfill its purposes.		
Objective	Benchmarks	Actions
4a. Departments and agencies have formally documented processes for ensuring the accuracy of personal information. 4b. Individuals are able to challenge the accuracy and completeness their personal information and have it amended. 4c. Citizens are able to challenge departments and agencies compliance with the Privacy Framework.	<u>Source:</u> Deloitte and Touche Report <u>Baseline</u>: None, in many cases processes are informal. <u>Short Term:</u> An inventory of possible methods for ensuring accuracy is developed by April 2004, and departments and agencies begin to document their accuracy processes. <u>Long Term:</u> By April 1, 2005, departments and agencies will have documented processes in place for ensuring the accuracy of personal information. By September 1, 2004 departments and agencies will have documented processes for citizens to challenge compliance with the Privacy Framework.	14. The Chief Information Officer (CIO) in conjunction with the Chief Privacy Officer (CPO) will develop an inventory of possible methods for ensuring accuracy of information. (e.g. - audits, verification processes, edit checks, etc.) 15. The Chief Information Officer (CIO) in conjunction with the Chief Privacy Officer (CPO) will establish a review process to ensure departments have appropriate accuracy processes in place. 16. Working with their Privacy Officers, Departments and agencies will develop a process for individuals to follow, if they wish to obtain information and/or challenge the information or compliance with this Framework.

GOAL #5: Personal information is secure.		
Objective	Benchmarks	Actions
5a. Departments and agencies have secured personal information and have a data classification system.	Source: Deloitte and Touche Report Baseline: No department classifies information with respect to sensitivity. Short Term: A schema for classifying the sensitivity of personal information is available to departments and agencies, by January 2004. Long Term: Beginning in 2004-05, departments and agencies will classify thirty percent of their personal information per year according to the classification schema.	17. The Chief Information Officer (CIO), in conjunction with Justice, will develop a data classification system and implementation strategy for departments and agencies. Departments and agencies will implement the data classification strategy. See Appendix E for an example of the classification system developed by the Canadian Public Sector Chief Information Officer Council.
5b. Departments and agencies have security safeguards to protect personal information and other management information.	Source: Deloitte and Touche Report Baseline: Departments and agencies have no consistent security policies in place nor have they defined minimal physical, electronic, or organizational monitoring and enforcement criteria. Short Term: By April 1, 2004, Executive government will have defined minimum criteria. Long Term: Beginning in April 1, 2005, departments and agencies will be at 50% compliance with the criteria, and by April 1, 2006 at 100% compliance.	18. The Chief Information Officer (CIO) and SPMC, in conjunction with Justice, will define physical, electronic, and organizational monitoring and enforcement criteria specifically designed to protect personal information and other management information. Departments and agencies will implement the enforcement criteria.

Conclusion

This Privacy Framework sets out the Government of Saskatchewan's commitment to foster a culture of privacy protection by ensuring that the collection, use, disclosure, and retention of personal information is consistent with the government's legitimate business and public interest mandate, and that the information is properly secured.

The Privacy Framework is comprised of a vision; a set of principles as well as a set of goals, objectives, benchmarks, and actions intended to actualize the vision and principles. This Framework also provides some of the key tools (for example, the Privacy Protection Checklist or the Draft Security Classification System) or in some cases the structures and processes for future actions (for example, the Chief Privacy officer, or the Access Directory of Personal Information). In other cases, there is further work to be done over a period of time, but given the structures and processes the way is set for achieving those goals and actions.

This Framework is intended to create the policy opportunity to move this important initiative forward and the accountability framework to hold government accountable to ensure that the actions are carried out at the appropriate levels.

Glossary

Access Directory:

> The Saskatchewan Access Directory is a compendium of information that describes the organization of the Government of Saskatchewan and the information it holds, particularly personal information. It is designed to support the implementation of *The Freedom of Information and Protection of Privacy Act* by providing individuals with a fast and easy way to find out about the information holdings of the Government of Saskatchewan.

Administrative Records:

> Records pertaining to administrative or housekeeping activities of the organization. These include the management of facilities, property, material, finances, human resources, and information systems. (ARMS Manual, Glossary of Terms, 2003. p. 1.)

Disclosure of personal Information:

> Is the transfer of personal information to a third party or another government institution. This is distinguished from the use of personal information which is the use of information within the department or agency that collected it.

Fair Information Practices

> Represent definable actions that are necessary to support privacy principles. A set of practices that are now widely accepted include (U. S. Federal Trade Commission): Notice and awareness; Choice and consent; Access (by the subject of the personal information); Information quality and integrity; Update and correction; Enforcement and recourse. (International Security Trust & Privacy Alliance, *Privacy Framework* version 1.1, San Diego: ISTPA, 2002. p. 7.)

Information:

> Data that has been given value through analysis, interpretation or compilation in a meaningful way. (ARMS Manual, Glossary of Terms, 2003. p.2)

Information Management:

> The systematic control of records from their creation, or receipt, through their processing, distribution, organization, storage, and retrieval to their disposition. (ARMS Manual, Glossary of Terms, 2003. p. 3.)

Information Management Project:

> The project established by the Saskatchewan Archives Board in November of 1991.

> Its mandate was to help prepare government departments for freedom of information legislation by developing and maintaining a common Administrative Records Classification System and Retention Schedule, and to help to develop up-to-date operational records retention schedules. (ARMS Manual, Glossary of Terms, 2003. p. 3.)

Informed Consent

> Informed consent is achieved when the individual provides consent and is informed of the purpose for collection, how it will be used, maintained, disclosed, and retained.

Operational Records:

> Records which relate to the operations and services provided by an office in carrying out the functions for which it is responsible according to statute, mandate, or policy. Unlike administrative records, operational records are distinct from common administrative functions and are unique to each government institution. (ARMS Manual, Glossary of Terms, 2003. p. 3.)

Operational Records System (ORS):

> Saskatchewan government wide standard for classification, organization, retrieval, storage, and disposition of operational records that integrates an operations records retention schedule and a block numeric classification system based on functions and subject. ORS is developed by an individual department or agency in consultation with staff of the Saskatchewan Archives Board.

Personal Information:

> Personal information is defined in section 24 of *The Freedom of Information and Protection of Privacy Act* and section 2 of *The Health Information Protection Act*. For a more extensive discussion, look to pages 9 and 10 of this document.

Privacy:

> The ability of an identifiable individual to control the collection, use and disclosure of any recorded information about themselves held by the Government of Saskatchewan or third parties on behalf of the Government of Saskatchewan.

Public Document:

> As defined by *The Archives Act*, includes certificates under the Great Seal of the province, legal documents, securities issued by the province under any Saskatchewan Loans Act, vouchers, cheques, accounting records, correspondence, maps, photographs, and all other documents created in the administration of the public affairs of Saskatchewan except copies of documents created only for convenience of reference and surplus copies of mimeographed, multilithed,

printed or processed circulars and memoranda. This definition encompasses electronic formats as well.

Record:

Recorded information, regardless of medium (paper, computer disk, etc.) or characteristics, created or received by an organization in support of its mandate. A record can refer to a single document or group of documents in a file folder. Through an ARMS "record" most commonly refers to a file folder that may contain a single document or many documents. (Glossary of Terms, ARMS Manual, Glossary of Terms, 2003. p. 4.)

ARMS (the Administrative Records Management System):

Is an executive tool for use in proper information management.

Combines a comprehensive classification system for administrative records with an up-to-date records retention schedule. (ARMS Manual, 2003. p. iii)

Deals exclusively with administrative records commonly found in all units of government. ARMS does not apply to:

- operational records
- convenience records
- published records (with some exceptions for classification)
- non-government (personal) records (p. 1, ARMS Manual, 2003)

Security:

The establishment and maintenance of measures to protect the system. Security is necessary for privacy, but the proper handling of personal information requires an even broader set of privacy management functions. (International Security Trust & Privacy Alliance, *Privacy Framework* version 1.1, San Diego: ISTPA, 2002. p. 6-7.)

Use of personal information:

Involves the use of the personal information within the department or agency. This is distinguished from disclosure, which involves the transfer of the information to another government department or agency or to a third party.

Appendix A

Government of Saskatchewan Departments and Agencies

Departments

- All provincial government departments

Boards, Commissions, Crown Corporations and Other Bodies

- Advisory Board of the Public Employees (Government Contributory) Superannuation Plan
- Agricultural Credit Corporation of Saskatchewan
- Agricultural Implements Board
- Agricultural Operations review Board
- Agri-Food Innovation Fund
- Automobile Injury Appeal Committee
- Board of Revenue Commissioners
- Co-operative Securities Board
- Education Infrastructure Corporation
- Farm Land Security Board
- Farm Tenure Arbitration Board
- First Nations and Métis Peoples and Justice Reform Commission
- Highway Traffic Board
- Human Rights Tribunal Panel
- Labour Relations Board
- Law Reform Commission of Saskatchewan
- Liquor and Gaming Authority
- Meewasin Valley Authority
- Milk Control Board
- Multitype Library Board
- Municipal Employee's Pension Commission
- Municipal Financing Corporation
- Office of the Rentalsman
- Oil and Gas Conservation Board
- Prairie Agricultural Machinery Institute
- Provincial Court Commission
- Provincial Mediation Board
- Public and Private Rights Board
- Public Disclosure Committee
- Public Service Commission
- Public Service Superannuation Board
- Saskatchewan Apprenticeship and Trade Certification Commission
- Saskatchewan Archives Board
- Saskatchewan Arts Board
- Saskatchewan Centre of the Arts
- Saskatchewan Communications Network Corporation

- Saskatchewan Crop Insurance Corporation
- Saskatchewan Financial Services Commission
- Saskatchewan Gaming Corporation
- Saskatchewan Grain Car Corporation
- Saskatchewan Health Information Network
- Saskatchewan Housing Corporation
- Saskatchewan Human Rights Commission
- Saskatchewan Lands Appeal Board
- Saskatchewan Legal Aid Commission
- Saskatchewan Municipal Board
- Saskatchewan Pension Plan Board of Trustees
- Saskatchewan Police Commission
- Saskatchewan Property Management Corporation
- Saskatchewan Research Council
- Saskatchewan Securities Commission
- Saskatchewan Watershed Authority
- Saskatchewan Wetlands Authority
- Saskatchewan Wetland Conservation Corporation
- Surface Rights Arbitration Board
- Teacher's Superannuation Commission
- Wascana Centre Authority
- Wanuskewin Heritage Park Corporation
- Wascana Appeal Board
- Western Development Museum
- Worker's Compensation Board
- Worker's Compensation Superannuation Board

Exclusions

The following agencies are excluded from this project:

- Crown corporations reporting through the Crown Investments Corporation

Appendix B

Chief Privacy Officer

Role, Responsibilities, Qualifications, and Accountability

Role

The role of the Government of Saskatchewan Chief Privacy Officer is to monitor that the legal framework, the policies, the standards, the education and awareness building, and the procedures for ensuring the protection of personal information are followed across the Government of Saskatchewan.

Responsibilities

Working through the Privacy Officers in each department and agency, the Chief Privacy Officer will be responsible for:

- Monitoring government operations within the legal regime of the Province of Saskatchewan.
- Implementing the Overarching Privacy Framework across government.
- Facilitating ongoing education and awareness activities.
- Measuring compliance with this Framework.
- Continually reviewing the adequacy of this Framework to ensure it meets the privacy needs of the Government of Saskatchewan.
- Conducting or organizing internal audits and assessments, and recommending improvements.
- Working with departments, agencies and the Archives to facilitate the implementation of records management systems that support privacy.
- General administrative duties to ensure the mechanisms (e.g. communications, and responding to enquiries and complaints) are in place to support the implementation of the Overarching Privacy Framework.

The Chief Privacy Officer will not be dedicated to these responsibilities only.

Qualifications

The ideal candidate for this job would have a broad understanding of how personal information is used across all government departments. Care should be given to ensure that the person/position selected is not in a conflict of interest situation.

Accountability

The Chief Privacy Officer will report to the Deputy Minister to the Premier.

Appendix C

Privacy Officer

Role, Responsibilities, Qualifications, and Accountability

Role

The role of the Privacy Officer is to ensure that the legal framework, the policies, the standards, and the procedures for ensuring the protection of personal information are followed within the department or agency for which the Officer is responsible.

Responsibilities

Working through the Senior Management and staff of the department or agency, the Privacy Officer will be responsible, in the particular department or agency, for:

- Ensuring the department or agency operates within the legal regime of the Province of Saskatchewan.
- Implementing the Overarching Privacy Framework.
- Facilitating ongoing education and awareness activities.
- Measuring compliance with this Framework.
- Continually reviewing the adequacy of this Framework to ensure it meets the privacy needs of the department or agency and the Government of Saskatchewan.
- Conducting or organizing internal audits and assessments, and recommending improvements.
- General administrative duties to ensure that the mechanisms are in place to support the implementation of the Overarching Privacy Framework.

Qualifications

The ideal candidate for this job would have a broad understanding of how personal information is used within the department or agency. Care should be given to ensure that the person/position selected is not in a conflict of interest situation.

Accountability

The Privacy Officer is a senior manager in the department or agency and will report to the Deputy Minister on these matters.

Appendix D

Government of Saskatchewan Privacy Protection Checklist

Introduction

It is the policy of the Government of Saskatchewan that all departments and agencies comply with this Privacy Framework. The following checklist is intended to assist the departments and agencies identify their areas of strengths and their areas in which additional work is required to achieve compliance with this Framework.

1. Accountability and Compliance

1.1. Has your department or agency identified a Privacy Officer?
1.2. Has your department or agency included a privacy protection clause in all outsourcing contracts?
1.3. Does your department or agency annually file all outsourcing contracts with the Chief Privacy Officer?
1.4. Does your department or agency annually review this Privacy Protection Standards Checklist to assess compliance with the Privacy Framework?
1.5. Has your department or agency taken steps to ensure employees are informed and knowledgeable of *The Freedom of Information and Protection of Privacy Act* and the Privacy Framework?
1.6. Have employees in your department or agency been provided with the opportunity to become informed and aware of privacy protection and to confirm their understanding of privacy protection as recommended by the Public Service Commission?

2. Purpose, Collection, Use, Disclosure, and Retention

2.1. Does your department or agency support the maintenance of the Access Directory?
2.2. Do the collection processes meet the following criteria:
  2.2.1. Have confirmed the authority under which the information is collected.
  2.2.2. Provide the information provider with an explanation of the purpose of collection prior to or at the time of collection?
  2.2.3. Provide the information provider with an explanation of how the information will be used prior to or at the time of collection?
  2.2.4. Provide an opportunity for the information provider to seek clarification and further explanation of how the information will be used?
  2.2.5. Provide the information provider with an explanation of how the information will be disclosed prior to or at the time of collection?
2.3. Has the department or agency reviewed the disclosure processes to ensure they are consistent with and limited to the stated purposes of collection?
2.4. Does the department or agency comply with *The Archives Act*?

3. Authority and Consent

3.1. Has the department or agency maintained documentation of the methods through which authority and consent were obtained?

4. Accuracy and Challenge

4.1. Does the department or agency follow the Methods and Processes for Ensuring Accuracy of Information developed by the Chief Information Officer?
4.2. Does the department or agency regularly review the information collection processes to ensure appropriate accuracy? Models for such reviews are available through the Chief Information Officer.
4.3. Does the department or agency have available for citizens written policy and procedures explaining the processes for citizens to challenge the accuracy of their personal information? Do these policies also make clear the processes for verifying and correcting errors?
4.4. Does the Privacy Officer have available for citizens written policies and processes explaining the processes for citizens to challenge compliance at the corporate level with the Privacy Framework?

5. **Security**

5.1. Does the department or agency use the Data Classification System maintained by Chief Information Officer? See Appendix E – The Canadian Public Sector Security Classification Guideline developed by the National CIO Council Subcommittee for Information Protection (NCSIP).
5.2. Does the department or agency follow the Physical Security Guidelines maintained by the Saskatchewan Property Management Corporation (SPMC)?
5.3. Does the department or agency follow the Electronic Security Guidelines maintained by the Chief Information Officer?
5.4. Does the department or agency follow the Organizational Security Guidelines maintained by the Chief Information Officer?

Appendix E

Canadian Public Sector Security Classification Guideline

April 19, 2001
Final

Prepared for the Public Sector CIO Council
By the National CIO Council Subcommittee for Information Protection (NCSIP)

Table of Contents

1. BACKGROUND

Ease of information exchange is a key for governments to meet their objectives for efficient, economic and effective service delivery. These exchanges however, must be achieved in a safe way while making maximum use of the Internet that is an insecure environment. It does not matter whether the business scenario is Government to Government (G2G), Government to Business (G2B), Business to Business (B2B) or Government to Canadians (G2C), organizations must be able to quickly arrange for safe, efficient exchanges in order to meet security and privacy requirements, to be timely with their services and to remain competitive in the global environment. Organizations are making significant investments in secure IT and they must protect those investments when interconnection occurs. Additionally, legislation and policy requires that the protection of sensitive organizational and personal information assets be guaranteed when arrangements are considered for their electronic exchange.

1.1 A Pre-requisite to Safe Information Exchange

Historically, a major impediment to broad based agreement on exchange of information has been the lack of common practices or guidelines from organization to organization in the security classification of information assets. Without a commonly understood framework in this area, quick and accurate decisions on the safe exchange of information are difficult. Governments require such structures to categorize information holdings that are "sensitive" in the national, provincial or private interest.

1.2 Canadian Approaches

The federal government has adopted a classification scheme for information that is sensitive in either the national or private interest. The federal schema is currently under review as part of a major revision to the federal government's security policy. The current schema focuses on confidentiality; however, the revision will address requirements for availability, integrity and value of information.

Several provincial jurisdictions also have adopted or proposed schema (s) that categorize their information holdings based on criteria such as **confidentiality, integrity, availability** and **value**. Freedom of Information and Privacy Acts also figure significantly in the current Provincial approaches. It is noted that there are significant differences between these classification approaches. *(NB: Use of the words 'classify or classification' does not suggest that the information is sensitive in the National Interest).*

1.3 Scope

The establishment of a commonly understood and accepted Canadian Public Sector Security Classification Guideline (Federal-Provincial-Municipal) is critical to the protection of sensitive information that governments need to exchange and have about Canadians. This common approach on classifying sensitive information will be the cornerstone for attaining compatibility between jurisdictions.

This schema is not intended to impinge upon the security approaches of individual governments. It is intended to serve as a common model to support mapping between security categories used within individual jurisdictions. The guideline will also support consistent mapping from one jurisdiction to the other in order to help identify the appropriate safeguards and facilitate the safe exchange of sensitive information under formal agreement.

This document is not a standard but rather a guideline approved by the PSCIOC to be applied by jurisdictions on a voluntary basis to facilitate secure electronic service delivery.

2. WHY A CANADIAN CLASSIFICATION GUIDELINE?

2.1 Increased Information Sharing and Access

Secure information sharing and access is needed in an Electronic Service Delivery (ESD) and Electronic Business (E-business) environment. Sensitive information must be shared or exchanged between and among federal, provincial, territorial, and municipal entities for the public good. Information exchange at all levels demands that measures be in place that will allow organizations to do so safely and securely. If personal information is being handled then protective measures that meet **privacy protection principles** and **standards** must be met. Research organizations must protect their **intellectual property** while research data and findings are being exchanged between organizations situated in a number of different provincial, federal or private sector research institutions. This is extremely important, for example, while patents are pending. Finance and other departments involved in budgets or other **political imperatives** must also protect their sensitive information for economic reasons and the well being of their constituents.

2.2 Consistency in Protective Requirements

In order for organizations to exchange sensitive information efficiently, economically and effectively, a **common and accepted nation-wide approach** is needed to classify and mark information based on sensitivity so that organizations can quickly and safely determine their obligations with respect to protective requirements and get on with their work. The obligation to protect sensitive information in Canada is often driven by legislative and/or policy requirements. It is not acceptable to argue that "time was of the essence" therefore adequate measures could not be taken. Given the competitive pressures in conducting business today, even public sector organizations are finding that they must make decisions quickly and they will be **exposed to liability** if they are uncertain about the sensitivity of the information they are handling or what the minimum requirements would be for its protection.

When information is shared with individuals outside your organization who are not aware of the value or sensitivity of an information asset, it becomes essential that the sensitivity level be established so that information requirements can be **quickly understood, communicated and acted upon.**

3. CONTRIBUTIONS TO THE CANADIAN GUIDELINE

The 'Canadian Public Sector Security Classification Guideline' was largely a business concern. It involved deciding what the impacts would be if there is a loss to **integrity, availability or confidentiality** of information assets that belong to the various programs within the public sector. Information technology, security professionals and business areas all contributed to the determination, the number of security categories, how they are to be defined and how they will be applied.

The process involved identifying a reasonable cross-section of various information assets, the threats to these assets, the probability or likelihood that a threat will occur, and if it does occur what the likely impact will be. This is commonly known as the preparation of **'statements of sensitivity'** that includes impact statements where a loss of confidentiality, integrity or availability occurs.

With input from the federal government and each of the provinces the team categorized sensitive information assets and developed a consensus position on a classification guideline with the categories that would have good potential to satisfy the greatest percentage of collective needs. Acknowledging that the Provinces did not have time to seek wide consultation or approval, it is still likely that there will be unique situations that will remain to be addressed on a case-by-case basis. Users of this Guideline will be able to map their sensitive information assets to the schema for information sharing purposes. Once these mappings are in place much time will be saved and organizations involved in the exchange of sensitive information will be far less exposed to threats.

4. SELECTING AN OPTION

The development of the Benefits Analysis Paper, Canadian Public Sector Security Classification Guideline, provided some of the background to this initiative, the contributions that would be needed from all key stakeholders and the potential benefits of having a National Classification Guideline. To assist Provincial representatives with the development of preferred classification levels and impact statements, a questionnaire and short presentation were developed by the NCISP. Provinces indicated a range in the preferred number and naming of levels. One of the consistent findings in most of the returns is the impact that 'access/freedom of information and privacy' has on the potential schema. Additionally, health and other personal information closely linked to the privacy legislation will form a major segment of information that will have to be handled by this guideline.

Information from the Provinces was consolidated to identify 'named categories' in use. Impact statements or the 'injury tests' were also identified for each of the four levels that would result from a **loss of integrity (includes non-repudiation and authentication), confidentiality or availability**. Four options were identified and one option was proposed for the guideline based on consensus views. See Table 1.

Classification Guideline - Table 1

Category	**Definition**
High	Could reasonably be expected to **cause extremely serious personal or enterprise injury**, significant financial loss in the hundreds of thousands to many millions of dollars, loss of life or public safety, social hardship and major political or economic impact
Medium	Could reasonably be expected to **cause serious personal or enterprise injury**, loss of competitive advantage, loss of confidence in the government program, financial loss in the tens of thousands of dollars, legal action and damage to partnerships, relationships and reputation
Low	Could reasonably be expected to **cause significant injury to individuals or enterprises** that would result in financial losses in the hundreds to thousands, a limited impact in service level or performance, embarrassment and inconvenience
Basic	Will **not result in injury** to individuals, governments or to private sector institutions

5. APPLYING THE CLASSIFICATION GUIDELINE

In order to properly apply the guideline internally within an organization or where information sharing is intended across jurisdictions, the following guidance is provided. If jurisdictions already use an approved guideline, this Guideline should be useful in mapping from one jurisdiction to the other in order to identify the appropriate safeguards and hence the safe exchange of sensitive information under formal agreement.

5.1 Reviewing Information Holdings

A thorough review to identify the sensitivity, and therefore the classification level of holdings, will permit the safe exchange of information within organizations or with partners where exchange agreements apply.

5.2 Instructions on Applying The Guide

An organization may apply this Guide once it has been adopted as the classification system for the organization or by naming an individual to oversee its application under an exchange agreement that applies between two different jurisdictions, or between a public sector entity and a private sector partner.

Organizations using this Guide should ensure that all individuals with delegated authorities for this function have a demonstrable and continuing need to exercise it. Further, those with delegated authority should be in possession of a current version of this guide or they should be able to access it electronically.

Information that is classified 'basic' may already be public and does not require any measures of protection beyond good office practice as indicated by the injury test.

Whenever possible, people assigning security classifications to information created in house, or to information received under partnership agreement, should also include the duration of classification by showing the date or event that triggers declassification or downgrading.

On a periodic basis, people assigning security classifications should review with the organization's access to information and privacy coordinator the decisions made to either disclose or withhold information as a result of requests under the access/freedom of information and the privacy legislation. This will help to ensure that security classification criteria remain relevant and effective.

5.3 Relationship to Access/Freedom of Information and Privacy Legislation

Most public sector information is adequately protected through sound office practices and the information therefore would have the 'basic' marking. Organizations must therefore identify the relatively small amount of information that is sensitive and requires additional protection beyond routine or normal office practice.

In some cases, identifying sensitive information relates directly to exemptions and exclusions under the access/freedom or Access to Information and Privacy Acts that establish the legal authority to refuse access to it by the general public. As situations change with circumstance and passage of time, classifiers are not required to determine definitively whether specific information will be exempt under either act t the time the information is created.

5.4 Special Types of Information in the Classification Schema

Some special types of information that will fall within certain schema categories are described below:

a. Information received in confidence from other governments or organizations (possibly private sector entities);
b. Information prepared by or obtained by a federal or provincial investigative body (could be law enforcement);
c. Personal information as defined in Privacy Acts;
d. Business information; and
e. Advice and recommendations involving Executive Council or confidences of the public that would affect the operations of Government.

These are not the only types of information that will require classification action and marking. For example, information shared between Ministries within the same Government on a partnership or agreement basis can be sensitive. This might include the sharing of information between Community and Social Services and the Revenue or Tax Ministry, or the transfer of monies to municipalities to support welfare or social aid programs.

5.5 Information Types Within the Various Categories

To assist people who assign security classifications, examples of information within the categories including 'gravity of injury' are defined in Table 1 and provided where a loss of integrity, confidentiality or availability would result:

a. High: The type of information that could reasonably be expected to **cause extremely serious injury to an individual or enterprise**. Examples would include: information on a police informant; the name of an individual applying for refugee status; witness protection information; cabinet confidence; exploration data in the mineral or oil industry; information relating to a sex offender, extended loss of service resulting in the need to institute manual processes, information relating to the case files of a major crime; major disruption in service or performance of the SDMT service capability, and loss of integrity for large financial transfers to a bank or other jurisdiction.

b. Medium: The type of information that could reasonably be expected to **cause serious personal or enterprise injury**.

Examples would include: compromise of personal medical information; exact salary figure, information compiled as a part of a violation of law; information on a completed tax return form; information relating to an individual's racial or ethnic origin; information describing an individuals finances; information on eligibility for social benefits; information on a company's credit rating; disclosure of trade secrets or intellectual property; denial of history on social assistance applicant resulting in over payment, inaccurate money transfer to a municipality due to loss of integrity, and the compromise of information received from another government relative to their position on an a particular trade issue.

c. Low: The type of information that could reasonably be expected to **cause significant injury to individuals or enterprises**. Examples would include: personal tombstone information such as disclosure of dates of birth, identifying numbers etc., status of a company product evaluation by a government organization; premature release of a government industrial cooperative program with industry that is under revision and not yet complete; denial of service resulting in status of social assistance application not being available and the premature release of the names of individuals competing for a particular job before the result is formally known; and

d. Basic: The type of information that if lost, changed or denied **would not result in injury to an individual or government organization**. It can be found on most government web sites and would include such information as the government telephone books, advertisements for job opportunities in the various ministries, government-wide initiatives such as Government-On-Line, legislation under development such as Privacy Bill C6, public health information, job classification level and range of pay scale.

5.6 Marking or Labelling Information

Information that is deemed to be sensitive must be classified for security level at the time that it is created. This will ensure that the information has appropriate protection throughout its lifecycle.

Additionally, any information that is transferred beyond the organization in which it was created must be marked unless it lacks sensitivity, meaning it would not even qualify for the 'basic' level of marking. Information that is exchanged under formal Memorandum of Agreement must be marked and the recipient organization must be able to translate the 'marking' into appropriate protective measures.

5.7 `Declassifying or Downgrading of Sensitive Information

Information should only be classified for the period that it requires protection, after which it should be declassified or downgraded. This requirement recognizes that information can lose its sensitivity with the passage of time or the occurrence of specific events.

When release of such information will cause injury as described in Table 1 then it must be classified, marked and protected accordingly. This process contributes to the overall integrity of the security system and will ensure that information can safely be made available to those who need to have it in an expeditious and safe way.

5.8 Automatic Declassification or Downgrading

Organizations should provide, whenever possible, for automatic declassification or downgrading of information by selecting a specific date or event for its declassification or downgrading or review at the time the record is created. When such information is received under Memorandum of Agreement, the recipient should ask if a declassification or downgrading date has been selected by the originating organization for the information.

It is suggested that a period be identified for all categories of information along with the date or 'event specific triggers' that will indicate downgrading or declassification. This period should be reduced appropriately where known periods exist within program areas. However, it is suggested that an automatic expiry date **not be selected** for information classified at the **medium** and **high** categories. Removing information from the 'classification schema' does have risks but this does not mean that this action is synonymous with making it publicly available. The normal access application review process would still apply.

5.9 Shared Information

The requirement to declassify or downgrade sensitive information applies not only to information within an organization but also to that provided from one ministry to another, or from another jurisdiction or partner under agreement. Before declassifying or downgrading any such information, the originator must be consulted. The originator can be represented by the 'office-of-origin'. If need be, the information can be transferred to the 'office-of-origin' for downgrading or declassification action. However, if there is a large volume of information it may be easier to consult the originator. It certain circumstances it may not be possible to consult the originator. In such cases, consultation with other appropriate officials such as the Freedom of Information Coordinator for the organization should occur.

6. PROCEDURES FOR MARKING

6.1 Electronic Media and Microforms

This Guideline has as its objective to deal with issues respecting protection of information in electronic form. However, since balanced security is required there should be comparable measures it the physical and personnel security areas.

Mark all materials used in preparing classified information; this would include notes, drafts and photocopies.

When marking information, also include the date of declassification or downgrading if it is known.

Assign a classification level or category commensurate with the highest classification of the information contained on a microform.

Mark microforms with the proper classification in eye-readable form with the microform number and the total number of microforms.

The marking of electronic storage media containing information classified at the levels cited in this schema must also be entered onto electronic documents or files so that adequate physical protection of the electronic media containing the sensitive information or data will occur. If this is not done, the sensitive information could be inadvertently disclosed or compromised. The information must also have the ‘classification or tag’ entered on information stored on hard drives, while it is in databases, and during transmission. If this is not done, sensitive information will not be protected in both its physical form and when in electronic form throughout its lifecycle.

7. DETERMINATION OF PROTECTIVE STANDARDS

This 'Canadian Public Sector Security Classification Guideline' will support the process of determining the correct safeguards but will not by itself provide the answer to the specific assurance required in safeguards. The impact statements and associated injury test cited in Table 1 will make a significant contribution to this determination.

7.1 Security Risk Management Relevance

The accepted process to determine protective standards is to complete a threat and risk assessment (TRA). The TRA process has four major components of work: environmental assessment, threat and vulnerability analysis, options analysis and safeguard identification and selection. During the 'environmental assessment' phase one must identify the information assets, develop 'statements of sensitivity' that result from a loss of integrity, confidentiality and availability of those information assets, and finally categorize those assets into useful levels. Having developed the schema levels, much of the 'environmental assessment' work has been done. The originator of information simply has to identify the category where their information assets belong and those conducting the TRA will complete the system specific threat and vulnerability analysis from which the **level of assurance** can be determined. The assurance level will determine the safeguards that will be suitable for the specific requirement.

7.2 Mapping to Public Key Infrastructure (PKI) Policy Assurance Models

If PKI is used, it should be possible to map the current classification schema to the PKI policy assurance model if one has been created. A mapping against the 'GOC PKI Policy Assurance Model' is possible and the mapping appears as follows:

Table 2: Mapping of GOC PKI Assurance Against Classification Schema

Classification Schema Category	GOC PKI Policy Assurance Model
High	High
Medium	Medium
Low	Basic
Basic	Rudimentary

In formulating the PKI Policy Assurance Levels a similar exercise was used that equates to determining the injury level through 'impact assessments' of a loss of confidentiality, integrity or availability.

8. LIMITATION OF CLASSIFICATION GUIDELINE

The Guideline is limited to identifying the proper marking to place on information so that it is clear what protective standards are required. This should be accomplished through security policies in related areas such as security risk management, education and awareness, access and release, privacy, documentation architecture etc. that this guideline does not address. Policy standards and guidelines in these other areas are required to ensure balanced security but are beyond the scope of this document.

Establishing ‘protective profiles’ or ‘minimum baseline strategies’ in communities of interest such as the ‘health area’ can be alternative strategies that will provide assurance that information is being protected at a known level.

Similar to the above ‘community if interest’ example, the Canadian Payments Association may also establish minimum protective standards in the area of finance or payments. This will allow the exchange of financial information during ESD given that an ‘industry best practice’ has been established for information safety. This will apply equally to private and public sector organizations.