Information
Management

Information Security Classification

February 2005

GOVERNMENT OF ALBERTA

Produced by

Information Management Branch
Government and Program Support Services Division
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web sites:
www.im.gov.ab.ca
www.gov.ab.ca/foip
www.pipa.gov.ab.ca

ISBN 0-7785-3698-X

Contents

Appendices:

Executive Summary

Purpose

This Information Security Classification guideline has been developed by the Government of Alberta Information Management Advisory Committee to assist ministries in establishing effective security classification practices. The objectives of the guideline are to:

- ensure personal information and confidential information are protected from unauthorized use and disclosure;
- protect the intellectual property of the Government of Alberta;
- facilitate the identification of information to support routine disclosure and active dissemination of information;
- facilitate the sharing of information with other jurisdictions to support e-government and integrated service delivery; and
- ensure information shared between the federal government and ministries for public safety is adequately protected.

This document is not a mandatory standard, but rather a guideline for ministries.

Classifying Information Assets

Four levels of security classification have been identified. They are:

Unrestricted Public Information (including information deemed public by legislation or through a policy of routine disclosure). Available to the public, all employees, contractors, sub-contractors and agents.

Protected Information that is sensitive outside the Government of Alberta and needs to be protected. Authorized access (to employees, contractors, sub-contractors and agents) on a "need-to-know" basis for business-related purposes.

Confidential Information that is sensitive within the Government of Alberta and is available only to a specific function, group or role.

Restricted Information that is highly sensitive and is available only to specific, named individuals (or specific positions).

This classification is consistent with security classification schemes developed by other jurisdictions in Canada.

Information that has been received from another jurisdiction **MUST**:

- maintain the classification level assigned by the originating jurisdiction and;
- be handled according to the rules and procedures established by the originating jurisdiction.

Implementing the Security Classification

Implementing information security classification will mean that ministries will need to consider and implement appropriate practices related to:

- labeling information;
- storing information;
- transmitting information;
- disposing of unneeded information;
- protecting the integrity of information;
- allowing appropriate access and disclosure; and
- establishing accountability.

The guidelines provide examples of practices to be considered in each of these areas.

Finally, in cases where information has been classified in the national interest (i.e., Confidential, Secret, Top Secret), there are special requirements to satisfy the Government of Canada security policy. These include requirements for security screening of Government of Alberta employees, specific handling requirements, and a Memorandum of Understanding with the appropriate federal government authority.

1. Introduction

The Government of Alberta is committed to managing its information assets to support service delivery to Albertans, efficient and effective operations and to protect the value of its investments. The Information Management Framework[1] outlines principles and directives for managing all government information assets. Information security is an important part of this asset management framework.

About this guide

This guide presents a common approach to security classification and guidance for ministries on its use. It is not a mandatory standard, but rather a guideline for ministries. It is intended for use by information management professionals within ministries to assist them in establishing effective security classification practices.

In this part of the guide, the rationale for security classification and related legislation and policy are discussed.

In Part 2, a guideline for classifying information assets is presented. This guideline has been developed to be consistent with the security classification guidelines recently prepared by the National CIO Council Subcommittee for Information Protection (NCSIP) for the Public Sector Chief Information Officer Council (PSCIOC), which is available at http://www.im.gov.ab.ca/imtopics/pdf/PublicSectorSecurityClassGuide.pdf.

Part 3 of the guide identifies a range of practices that are needed to implement the guideline. These practices relate to labeling, storing, and transmitting information assets that have been classified as well as practices related to ensuring appropriate access to information and protecting the integrity of information. This part of the guide also presents a model accountability framework for information security. Ministries will want to implement practices that are cost effective and based on a threat and risk assessment.

[1] The framework, "Information Assets in the Government of Alberta: A Management Framework," was adopted by Deputy Ministers' Committee in April, 2003. It is available at http://www.im.gov.ab.ca/imf/pdf/IMFrameworkSummary.pdf.

Finally, in Part 4, an approach to implementing security classification is discussed.

NOTE: Several documents referenced in this guide are available in the Shared Repository (SHARP) which is a web site generally accessible only to Government of Alberta employees, consultants contracting with the Government of Alberta and employees of other governments who are registered users of the site. To request access to a restricted document, contact the SHARP Administrator at ea-toolset@gov.ab.ca.

Why security classification is important

There are several reasons why ministries should be concerned about information security classification. These include:

- **Protection of personal information**. The *Freedom of Information and Protection of Privacy Act* (FOIP) and the *Health Information Act* govern the collection, use and disclosure of personal information. The FOIP Act also governs the management of personal information – its protection, retention, and accuracy. Security standards support the effective application of the Act in the conduct of day-to-day business.
- **Protecting confidential information from unauthorized access**. In the normal business of government, certain information must remain confidential. Examples of such information include the annual Provincial Budget, human resources files, case management files, Cabinet documents and investigation files in many ministries. Applying proper security classification and practices can safeguard against unauthorized access to confidential government information.
- **Protecting intellectual property**. The Government of Alberta has significant investments in intellectual property. The Information Management Framework requires that these investments be protected to benefit Albertans. Appropriate security practices are needed to ensure an adequate level of protection.
- **Supporting routine disclosure and active dissemination**. Under the Information Management Framework, ministries are required to develop plans for the routine disclosure and active dissemination of information to Albertans. Security classification of information assets is a critical component in identifying and facilitating the disclosure of information to the public. It can also help identify information that needs to be protected but might be inter-filed with or combined with unrestricted information.

- **Facilitating intergovernmental cooperation and integrated service delivery**. More and more work of the government is carried out in partnership with other service providers and other levels of government. Moreover, secure information sharing and access is needed in an electronic service delivery (ESD) and electronic business (E-business) environment. When information is shared with individuals outside the 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.
- **Protecting information that supports public security and law enforcement**. Many ministries within the Government of Alberta – Solicitor General, Justice, Health and Wellness, Agriculture, Food and Rural Development, Intergovernmental and International Relations, the Special Investigations Unit of Government Services, Emergency Management Alberta (Municipal Affairs) and Gaming Investigations (Gaming) routinely receive information from the Government of Canada related to public safety and law enforcement. This information is shared under Memoranda of Understanding and must be adequately protected to ensure continued sharing of this information.

NOTE: For information that is classified in the national interest by the Government of Canada (i.e., Confidential, Secret, Top Secret), there are special requirements for security screening, specific handling requirements, and a memorandum of understanding. Sharing of information classified in the national interest is discussed in Appendix 2.

Related legislation, policies and standards

Information security classification should be viewed in the context of related legislation, policies and other standards in the Government of Alberta.

Freedom of Information and Protection of Privacy Act (FOIP)

FOIP legislation governs the public's right to access government information as well as the collection, use and disclosure of personal information. The legislation also governs the management of personal information – its protection, retention and accuracy.

If unrestricted (i.e., publicly available) information is properly identified, access to this information can be provided without requiring Albertans to make a formal request under FOIP legislation.

Standards and practices related to the legislation can be found in the Freedom of Information and Protection of Privacy Guidelines and Practices Manual (http://www.gov.ab.ca/foip/guidelines_practices/index.cfm).

NOTE: A decision to deny access to a record or any part of it related to an access request under the *Freedom of Information and Protection of Privacy Act* must be based **solely** on the exemption provisions of FOIP as they apply at the time the request is made and must **not** be based on a security classification.

Health Information Act

The *Health Information Act* governs the handling, use and sharing of information related to the health of individuals in the province.

Standards and practices related to the legislation can be found in the Health Information Act Guidelines and Practices Manual at: http://www.health.gov.ab.ca/resources/publications/pdf/HIAguidelines2.pdf.

Records Management Regulation

Under the Records Management Regulation, all ministries are required to develop records retention and disposition schedules related to the length of time records must be kept (retention) and how records are to be disposed of (either through destruction or transfer to the Provincial Archives of Alberta). Under this Regulation, the Minister responsible for the Regulation may establish policies, standards and procedures for the security of records under the control of the Government of Alberta. The Regulation is available at http://www.qp.gov.ab.ca/documents/regs/2001_224.cfm.

Information Management Framework

Deputy Ministers adopted the Information Management Framework (IMF) [http://www.im.gov.ab.ca/imf/pdf/IMFsummary.pdf] to bring greater discipline and consistent practices in the management of all information assets. The IMF outlines six broad principles related to the management of information assets. These principles are to be achieved through 18 directives for ministries. This information security classification guideline supports the directives related to "accessibility principle" in the IMF.

Information and Communications Technology (ICT) Security Framework

In today's world, threats to the security of information and information technology assets are constant. The ICT Security Framework establishes a comprehensive plan to enable the Government of Alberta to be vigilant and effective in protecting these assets from disruption, unauthorized access or corruption of the electronic information. This information security classification is consistent with the ICT Security Framework. Supporting this framework are security policies, security architecture, technical standards and documents of best practices. Most of these documents are available only to Government of Alberta employees and external stakeholders who are registered users of the SHARP web site.

- Information Technology Security Policy
  https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=3882
- Information Technology Baseline Security Requirements
  https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=3078
- Government of Alberta Internet and E-Mail Use Policy
  http://www.sharp.gov.ab.ca/docDisplay.cfm?docID=2007
- Security Policy for Disk Wiping Surplus Computers
  https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=2356
- Wireless LAN Access Security Policy
  https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=3867
- Threat and Risk Assessment Guidelines
  https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=5266
- GAEA Security Architecture
  http://www.sharp.gov.ab.ca/docDisplay.cfm?docID=4124

Information and Communications Technology (ICT) Privacy Planning Tool

The ICT Privacy Planning Tool establishes a strategy for the protection of privacy in Government of Alberta information and communications technology operations. It has two key features:

- a set of ICT Privacy Principles provide general direction for ICT privacy protection in the Government of Alberta; and
- the GAEA Privacy Architecture lays out specific privacy design standards and guidelines for applications of information and communications technology in the Government of Alberta.

The ICT privacy principles and an overview of the privacy architecture are available at http://www.sharp.gov.ab.ca/ppa.

Policy for the Protection of Personal Information in Information Technology Outsource Contracts

As ministries rely on outside providers to support the delivery of information technology to staff and the public, this policy outlines the responsibilities of government to ensure that service providers protect personal information. The policy can be accessed at https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=3293

Policy for the Transmission of Personal Information via Electronic Mail and Facsimile

Public communication networks such as the Internet and other telecommunications networks are not totally secure environments. Ministries must take steps to protect personal information when it is transmitted over these public networks. The policy can be accessed at https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=3546.

2.
Classifying Information Assets

Approach

Ministries will determine the extent to which security classification needs to be applied to information assets.

The security classification of information assets should meet both business and operational needs. It should be based on a threat and risk assessment and business impact analysis.

Criteria

Four criteria are the basis for deciding the security and access requirements for information assets. These criteria are:

- **Integrity**: information is current, complete and only authorized and accurate changes are made to information;
- **Availability**: authorized users have access to and can use the information when required;
- **Confidentiality**: information is only accessed by authorized individuals, entities or processes; and
- **Value**: intellectual property is protected, as needed.

Threat and risk assessment

These criteria can be applied in a threat and risk assessment. The purpose of the assessment is to identify what the probability or likelihood of the threat is and what the impact would be if there was a loss to the integrity, availability, confidentiality or the value of information assets. Threat and risk assessments as well as Privacy Impact Assessments (PIAs) are undertaken to properly identify risks.

The Office of the Corporate Chief Information Officer has developed Threat and Risk Assessment Guidelines for information assets. This guide to conducting threat and risk assessments can be found at https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=5266.

The OCTAVE risk management methodology can also prove useful during risk assessments (http://www.cert.org/octave/)

The Office of the Information and Privacy Commissioner provides guidance in the preparation of privacy impact assessments at http://www.oipc.ab.ca/pia/. In addition, some ministries have developed their own guidelines on conducting privacy impact assessments.

Security classification guideline

The security classification guideline for information assets in the Government of Alberta consists of four categories. These categories, with a description, and examples of the types of records that might be found in that category are outlined in Table 1 on the following page.

This guideline has been developed to be consistent with approaches taken in other jurisdictions. Appendix 1 contains a comparison of this classification guideline with the security classification standard developed by the Public Sector CIO Council and the information classification standard adopted by the Government of Ontario and the Office of Management and Budget (OMB) in the United States.

Table 1
Information Security Classification Guidelines

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
Unrestricted	Information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information includes information deemed public by legislation or through a policy of routine disclosure and active dissemination. **Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the government.**	▪ Public health information ▪ Job postings ▪ Ordinary staff meeting agendas and minutes ▪ Communications to claims clerks ▪ Research and background papers (with no copyright restrictions)	▪ Little or no impact ▪ Minimal inconvenience if not available ▪ If lost, changed or denied would not result in injury to an individual or government (that is, no legal effect)
Protected	Information that is sensitive outside the Government of Alberta and could impact service levels or performance, or result in low levels of financial loss to individuals or enterprises. Protected information would include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. **Protected information is available to employees and authorized non-employees (contractors, sub-contractors and agents) possessing a need to know for business-related purposes**.	▪ Policy interpretation ▪ Draft request for proposals ▪ Business information ▪ Applications ▪ Planning documents ▪ Documents containing personal information	▪ Unfair competitive advantage ▪ Disruption to business if not available ▪ Low degree of risk if corrupted or modified
Confidential	Information that is sensitive within the Government of Alberta and could cause **serious** loss of privacy, competitive advantage, loss of confidence in government programs, damage to partnerships, relationships and reputation. Confidential information includes highly sensitive personal information. **Confidential information is available only to a specific function, group or role**.	▪ Personal case files such as benefits, program files or personnel files ▪ Industrial trade secrets ▪ Registration information ▪ Personnel files ▪ Grade 12 Provincial Examinations ▪ Policy Advice ▪ 3rd party business information submitted in confidence	▪ Loss of reputation or competitive advantage ▪ Loss of confidence in the government program ▪ Loss of personal or individual privacy ▪ Loss of trade secrets or intellectual property ▪ Loss of opportunity (e.g., insurance, health coverage) ▪ Financial loss ▪ High degree of risk if corrupted or modified

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
Restricted	Information that is extremely sensitive and could cause **extreme** damage to the integrity, image or effective service delivery of the GoA. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. **Restricted information is available only to named individuals or specified positions.**	▪ Cabinet documents ▪ Cabinet deliberations and supporting documents ▪ Personal medical records ▪ Provincial Budget prior to public release ▪ Criminal records ▪ Criminal investigations	▪ Loss of life ▪ Extreme or serious injury ▪ Loss of public safety ▪ Significant financial loss ▪ Compromise of the legal system ▪ Compromise of Cabinet deliberations ▪ Destruction of partnerships and relationships ▪ Significant damage ▪ Sabotage/terrorism ▪ Extreme risk if corrupted or modified

NOTES:

1. Information that has been received from another jurisdiction MUST (a) maintain the classification level assigned by the originating jurisdiction and (b) be handled according to the rules and procedures established by that jurisdiction.

2. Information that has been classified at a higher level of protection should be able to be reclassified to a lower level of protection by the information owner or originating program area.

3. Information Security Classification in Practice

Implementing information security classification will mean that ministries should consider practices related to:

- labeling information assets;
- storing information;
- transmitting information;
- disposing of unneeded information;
- protecting the integrity of information;
- allowing appropriate access and disclosure; and
- establishing accountability

This section provides **examples** of practices in these areas. The practices identified are not intended to be prescriptive. Rather, they are identified here as a guide to ministries.

It is unlikely that ministries will implement security classification to all information assets at the same time. Rather, the timing of applying information security classification will be based on the result of a threat and risk assessment and may very well be tied to the implementation of Electronic Information Management (EIM) technology.

The actual practices that are implemented will depend on the business reason for applying security classification as well as established administrative protocols (in the case of print information assets) and information technology protocols (in the case of electronic information assets).

NOTE: Information that has been classified in the national interest by the Government of Canada will require specific practices related to labeling, storing, transmission and use. These should be covered in the Memorandum of Understanding between the ministry and the Government of Canada (see Appendix 2).

Labeling information assets

Implement standard security labels for information assets. The actual labeling procedure will vary depending on the medium in which the information is stored. Table 2 identifies some common labeling methods for various types of information assets.

Table 2
Sample Labelling Methods

Type	Procedure
Hard copy documents	Rubber ink-stamps for each level may be needed to mark hardcopy documents received from outside the organization.
Electronic mail	Identify security classification in subject line of e-mail, if classified as confidential, or restricted.
Electronic documents	Identify security classification in document metadata. If the electronic document is to be printed or viewed in .pdf format, the security classification should appear on every page, including the cover page (this can be done by including the classification in the header/footer or by use of a watermark). Information about the ministry or department which created the document and date of creation should be included.
Data, databases and business applications	Identify classification in system/application metadata. Labels may be required for online screen displays and reports generated by IT systems.
Other media	The security classification may be identified on adhesive labels applied to other media such as diskettes, CDs, DVDs, and videocassettes. A message with the classification label should be displayed when the information stored on the media is accessed.

Storing information

Depending on the security classification, information assets will need different types of storage procedures to ensure that the confidentiality, integrity, accessibility, and value of the information are protected.

Table 3 identifies storage procedures for printed and electronic information in the various classification categories.

Table 3
Sample Storage Procedures

Classification	Print/Hard Media	Electronic Files
Unrestricted	▪ No special storage requirements	▪ No special storage requirements ▪ Regular back-ups to ensure availability and integrity
Protected	▪ Secure location (e.g., locked office; locked file room)	▪ All media under physical and/or logical access control of protected zone (e.g. group authorized access)
Confidential	▪ Secure location with restricted access ▪ Clean desk policy	▪ All media under physical and/or logical access control of confidential zone (e.g., authorized access and authenticated access)
Restricted	▪ Stored in highly secure zone, with access tracking ▪ Clean desk policy ▪ Audit trail for all access points (e.g., signatures)	▪ All media under physical and/or logical access control of restricted zone (e.g., singled or double authentication, encrypted data, audit and monitoring)

NOTE: Various classes of information located in one common medium/location should have the highest classification of all information located in the medium. This is important to ensure that highly classified information is not put at risk. Physical security of any media should include fire/flood/theft protection.

Transmitting information

When transmitting information that is protected, confidential or restricted, special procedures will be needed. Examples of these procedures are identified in Table 4.

The following policies on the transmission of protected, confidential and restricted information are also applicable:

- Information Technology Baseline Security Requirements https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=3078
- Policy on the Transmission of Personal Information via Electronic Mail or Facsimile https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=3546.

Table 4
Sample Transmission Procedures

Classification	Print/Hard Media	Electronic Files
Unrestricted	▪ No special procedures	▪ No special procedures
Protected	▪ Sealed envelope ▪ First class mail	▪ If electronic message contains personal information, personal information must be transmitted in such a way to prevent interception, modification, or unauthorized receipt en route or at the destination (e.g., password protected file; encryption; personal information sent in separate e-mail)
Confidential	▪ Sealed envelope, stamped confidential ▪ Receipt confirmation required	▪ Message sent in such a way to prevent interception, modification, or unauthorized receipt en route or at destination ▪ Recipient confirmation required ▪ Audit of access points (suggested)
Restricted	▪ Tamper evident packaging (e.g., double-sealed envelope with inside envelope signed to reveal evidence of tampering) ▪ Transmitted under a continuous chain of custody with receipts covering each individual who obtains custody	▪ Message sent in such a way to prevent interception, modification or unauthorized receipt en route or at destination (e.g., encryption used to send/authenticate message) ▪ Complete audit trail of each access point

Protecting the integrity of information

Integrity refers to the fact that information is current, complete, and only authorized changes are made to it. The integrity of information processed by and stored in information systems can be addressed by assigning the appropriate rights (e.g., read only, modify). If the threat to the integrity of information is significant, electronic files should be saved as read only files with changes to be made only by the author (this may be handled by access rights based on user account, work group or physical access to a specific devise). In these cases, procedures should be in place for transfer of rights when the author leaves the organization.

In some cases, stronger control such as encryption may be required. If encryption is used, a process related to key escrow must be established to ensure the availability of the information.

Allowing appropriate access and disclosure

Certain types of information will require controlled access and logs to track access and disclosure activities.

Table 5 outlines the access restrictions and any special audit trail that should be maintained.

Table 5
Allowing Appropriate Access and Disclosure

Classification	Access Restrictions	Audit/Activity Files
Unrestricted	▪ Open to the public and all employees, contractors, sub-contractors and agents	▪ None
Protected	▪ Authorized access (employees, contractors, sub-contractors and agents) on a "need-to-know" basis for business related purposes	▪ Periodic audits to show protection is, in fact, occurring
Confidential	▪ Limited to individuals in a specific function, group or role	▪ Pre-clearance based on position or contractor, sub-contractor or agent relationship ▪ Log of access/actions ▪ Periodic audits of adequate protection
Restricted	▪ Limited to named individuals (positions)	▪ All access or actions will be logged and subject to non-repudiation processes as appropriate

Establishing accountability

A clear accountability regime for all personnel will be important to ensure the protection of government information assets. Here is a **sample** accountability framework:

Deputy Minister

Deputy Ministers are responsible for government records generally and have legal responsibility under the *Freedom of Information and Protection of Privacy Act* **(**FOIP).

Specifically, the Deputy Minister is responsible for:

- defining, documenting and implementing reasonable measures to prevent unauthorized access to and the inadvertent release, destruction or damage of government records; and
- safeguarding records in their custody or under their control, including records which are in the custody of third parties under alternate service delivery arrangements.

Corporate Chief Information Officer

The Corporate Chief Information Officer is responsible for establishing corporate security policy and standards for electronic information and information technology assets.

Ministry Chief Information Officer

The Ministry Chief Information Officer is responsible for:

- reviewing, understanding and applying the information security classification standard to electronic information and information technology assets;
- liaising with the ministry Senior Records Officer and information management program on the application of the security classification to recorded information in other media;
- developing ministry security policies and standards that are consistent with the corporate Security Policy;
- recording all security breaches and violations discovered by the ministry;
- managing the response and actions taken within their ministry to breaches, violations, audits, investigations and security reviews;

- reporting these security breaches and violations along with actions taken to the Corporate Chief Security Officer and other appropriate personnel[2];
- ensuring that implementation of the security classification systems is appropriately coordinated ministry-wide;
- guiding and assisting program managers in the assessment of their information security needs and information security classification;
- assisting staff in the identification, design and implementation of reasonable security measures;
- assisting program managers in determining if the security measures in place meet their program needs; and
- providing guidance and assistance to employees in implementing this standard.

Program Managers

Program Managers are responsible for:

- reviewing, understanding and ensuring applicable legislation, policies and guidelines relating to the security of information are followed in their program area;
- developing and maintaining internal procedures that support the requirements for the effective handling and security of information;
- ensuring that information under their control is classified appropriately;
- ensuring that all information resources under their immediate control has appropriate retention periods to meet their business needs and the legal retention and disposition schedule is understood and applied by staff;
- ensuring that information under their custody or control is protected from physical damage and from unauthorized access, alteration, removal or destruction;

[2] The Office of the Corporate Chief Information Officer will be advised of any incidents that have the potential to affect more than one department. The *Freedom of Information and Protection of Privacy Act* Coordinator for the department will be notified if the incident involves the disclosure of personal information. The Alberta Records Management Committee will be informed of records lost. Incidents involving breaking of laws must be reported to law enforcement agencies and incidents involving physical loss or damage will be reported to Risk Management and Insurance Division, Alberta Revenue (losses in excess of $5,000.00 are covered by the Risk Management Fund).

- ensuring that staff are aware of, trained in, and understand legislation, applicable directives and procedures relating to the security classification of government information assets; and
- reporting all actual and suspected security breaches and violations to the ministry Chief Information Officer.

Freedom of Information and Protection of Privacy (FOIP) Coordinator

FOIP Coordinator is responsible for:

- reviewing records to determine whether any FOIP exemptions or exclusions apply when requests are received under *Freedom of Information and Protection of Privacy Act* (FOIP) for records that have a security classification **[The application of a security classification to a record does not determine whether a record is exempt from access under FOIP]**; and
- taking required action related to privacy breaches.

Senior Records Officer (SRO)

The ministry SRO is responsible for:

- reviewing, understanding and applying the information security classification standard to physical records in the custody or under the control of the ministry;
- assisting the ministry CIO in implementing security classification for electronic information and supporting program managers and staff in applying security classifications to information holdings in a consistent manner;
- recording all security breaches and violations discovered by the ministry;
- managing the response and actions taken within their ministry to breaches, violations, audits, investigations and security reviews;

- reporting these security breaches and violations along with actions taken to the Corporate Chief Security Officer and other appropriate personnel[3];
- guiding and assisting program managers in the assessment of their information security needs and information security classification;
- assisting staff in the identification, design and implementation of reasonable security measures;
- assisting program managers in determining if the security measures in place meet their program needs;
- providing guidance and assistance to employees in implementing this standard;
- providing secure locked storage facilities for protected, confidential and restricted information holdings; and
- ensuring records retention and disposition schedules are created for all information holdings under the custody and control of the ministry.

All ministry staff and staff of partners and contractors

All ministry staff and staff of partners and contractors are responsible for:

- reviewing, understanding and applying the information security classification standard to information assets they create, receive, use, transmit, or store;
- meeting their obligations under the *Freedom of Information and Protection of Privacy Act*, and the Oath of Office, to protect any information under their control or custody from unauthorized disclosure to any person or organization;
- ensuring that information under their custody or control is protected from physical damage and from unauthorized access, alteration, removal or destruction according to the security and access standard; and
- reporting all actual and suspected security and privacy breaches and violations to the Program Manager.

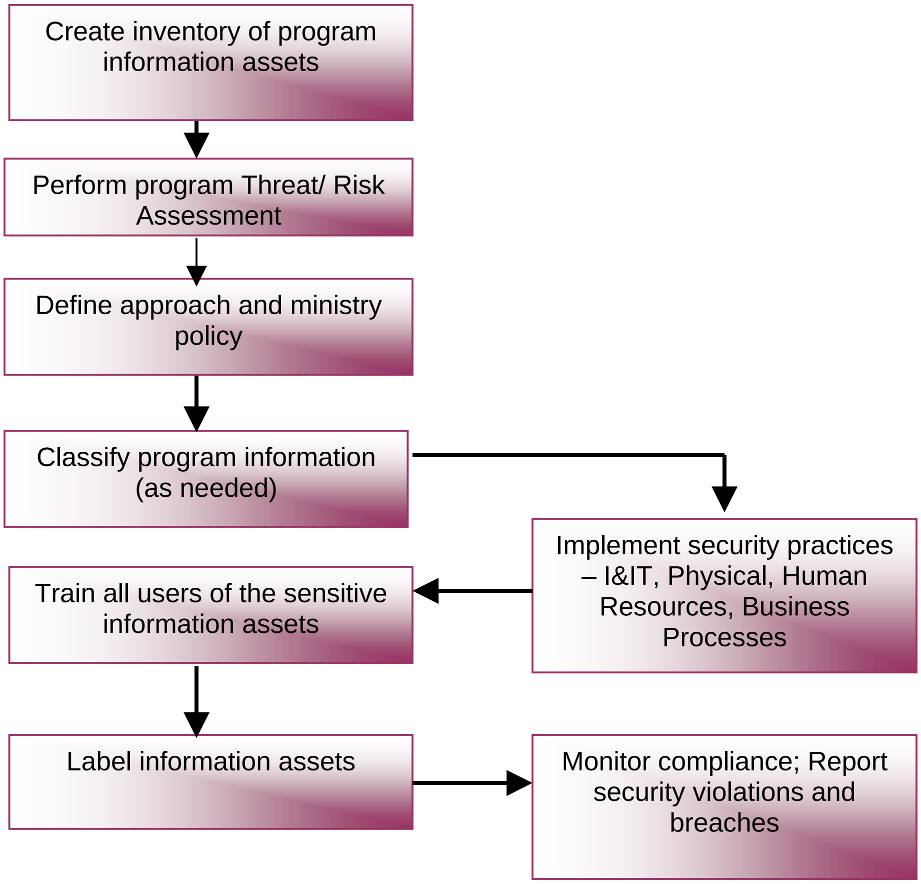
[3] The Office of the Corporate Chief Information Officer will be advised of any incidents that have the potential to affect more than one department. The *Freedom of Information and Protection of Privacy Act* Coordinator for the department will be notified if the incident involves the disclosure of personal information. The Alberta Records Management Committee will be informed of records lost. Incidents involving breaking of laws must be reported to law enforcement agencies and incidents involving physical loss or damage will be reported to Risk Management and Insurance Division, Alberta Revenue (losses in excess of $5,000.00 are covered by the Risk Management Fund).

4. Implementing Information Security Classification

For ministries to implement Information Security Classification, the starting point is to develop a plan of action. This planning process should be included as part of the overall planning of information management. Figure 1 identifies the key steps in such a plan.

The diagram below gives an overview of ministry steps in planning and implementing Information Security Classification in ministry programs.

Figure 1
Implementing Information Security Classification
(for information not covered by a Memorandum of Understanding with the Government of Canada)


Create inventory of program information assets
Perform program Threat/ Risk Assessment
Define approach and ministry policy
Classify program information (as needed)
Implement security practices – I&IT, Physical, Human Resources, Business Processes
Train all users of the sensitive information assets
Label information assets
Monitor compliance; Report security violations and breaches

Create an inventory of program information assets

The Records Management Regulation requires ministries to develop schedules to govern the retention and disposition of all existing recorded information under their control. The program's retention and disposition schedules are a good place to start in creating the program's inventory of documents and material assets.

Perform the threat and risk assessment

One way to assess the need for information security classification is a threat and risk assessment. The purpose of the assessment is to identify what the probability or likelihood of the threat is and what the impact would be if there was a loss to the integrity, availability, confidentiality or the value of information assets. Threat and risk assessments as well as Privacy Impact Assessments (PIAs) are undertaken to properly identify risks.

The Office of the Corporate Chief Information Officer has developed Threat and Risk Assessment Guidelines for information assets. This guide to conducting threat and risk assessments can be found at https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=5266.

The OCTAVE risk management methodology can also prove useful during risk assessments (http://www.cert.org/octave/)

The Office of the Information and Privacy Commissioner provides guidance in the preparation of privacy impact assessments at http://www.oipc.ab.ca/pia/. In addition, some ministries have prepared their own guides for conducting privacy impact assessments.

Define approach and ministry policy

Based on the assessment of information assets, the business analysis, and the threat and risk assessment, an approach to security classification can be developed. The ministry's approach should be supported by policies and practices appropriate for the ministry.

Classify program information

The result of the threat and risk assessment should help identify which information assets need to be classified on a routine basis.

In preparation for labeling program documents with a security classification, first determine the sensitivity of each type of document.

Even though an overall program may have been classified at a high level, individual documents within the program may have a lower security classification level than the overall program. There should not be any cases of a program document having a higher security classification level than the overall program. If a program document is found to have a higher security classification than the overall program then the overall program classification should be adjusted to the higher level.

Implement security practices

Information security needs to balance the protection of information assets and disclosure of information, as required by legislation, regulation and good business practice. Successful implementation of information security will allow staff and service delivery agents to perform their jobs effectively while preserving the public trust.

A holistic approach means effective protection. Security measures should be in place for information systems, human resources, physical facilities and include business procedures for storage, access and use of classified information assets.

Train users

Program managers are responsible for ensuring that anyone to whom they (or their delegates or agents) provide information is fully aware and capable of meeting the requirements for labeling, storing, transmitting information and ensuring that unauthorized persons cannot obtain the information.

All staff who handle information that is protected, confidential or restricted need to be trained on information security classification to understand why it is important, what it means, how to label and handle the information, and how to communicate any special handling measures.

Staff who work together may be able to provide support to each other during implementation if they are trained together.

Label information assets

Implement labeling practices. Security classification labels may be required for reports generated by IT systems, documents created using office desktop tools, hardcopy documents received from jurisdictions, e-mail messages, and media such as diskettes, CDs and microfiche that contain sensitive information.

Monitor compliance and report violations

An effective program for information security classification will require ongoing monitoring. Establish procedures to document and report violations and breaches of security.

Appendix 1:
Comparison with Other Jurisdictions

Other jurisdictions have also developed security classification standards for information assets. The table below illustrates how Alberta's information security classification compares with standards developed in Ontario and the guidelines developed by the Public Sector CIO Council (http://www.im.gov.ab.ca/imtopics/pdf/PublicSectorSecurityClassGuide.pdf) and the Office of Management and Budget in the United States.

Alberta	Ontario	PSCIOC	OMB (United States)
Unrestricted: Information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information includes information deemed public by legislation or through a policy of routine disclosure and active dissemination. **Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the government.**	**Unclassified:** Public information. Internal communications.	**Unclassified:** Public information. Internal communications.	**Basic:** Will not result in injury to individuals, governments or to private sector institutions or loss of under one thousand dollars**.**
Protected: Information that is sensitive outside the Government of Alberta and could impact service levels or performance, or result in low levels of financial loss to individuals or enterprises. Protected information would include personal information, financial information or details concerning the	**Low Sensitivity:** Information that is only sensitive outside the Ontario Public Service. Generally available to employees and approved non-employees.	**Low Sensitivity:** Information that is only sensitive outside the government. Generally available to employees and approved non-employees.	**Low:** Could reasonable be expected to cause significant injury to individuals or enterprises that would result in financial losses, such as between one thousand and one hundred thousand dollars, a limited impact in service level or performance,

effective operation of the GoA, ministries and departments. **Protected information is available to employees and authorized non-employees (contractors, sub-contractors and agents) possessing a need to know for business-related purposes**.			embarrassment and inconvenience.
Confidential: Information that is sensitive within the Government of Alberta and could cause **serious** loss of privacy, competitive advantage, loss of confidence in government programs, damage to partnerships, relationships and reputation. Confidential information includes highly sensitive personal information. **Confidential information is available only to a specific function, group or role**.	**Medium Sensitivity:** Information that is sensitive within the OPS and is intended for use only by specific groups of employees.	**Medium Sensitivity:** Information that is sensitive within the government and is intended for use only by specific groups of employees.	**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 (such as between one hundred thousand and ten million dollars), legal action and damage to partnerships, relationships and reputation.
Restricted: Information that is extremely sensitive and could cause **extreme** damage to the integrity, image or effective service delivery of the GoA. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. **Restricted information is available only to named individuals or specified positions.**	**High Sensitivity:** Information that is extremely sensitive, of highest value to the Ontario government and intended for use by named individuals (positions) only. Documents that can create an identity.	**High Sensitivity:** Information that is extremely sensitive, of highest value to the government and intended for use by named individuals (positions) only. Documents that can create an identity.	**High:** Could reasonable be expected to cause extremely serious personal or enterprise injury, significant financial loss (such as over ten million dollars), loss of life or public safety, social hardship and major political or economic impact.

Appendix 2:
Dealing with Classified Information from the Government of Canada

The Government of Canada (GOC) provides many ministries in the Government of Alberta with information and intelligence. Some of this information is classified in the national interest at the confidential, secret and top-secret levels. The GOC Security Policy requires that an arrangement be established to enable such sharing and ensure that federal terms and conditions, including security clearances, are met.

GOC Information Security Classification

The Government of Canada uses two types of information security classification – "designated" and "classified." Designated information is generally information created for use by the federal government and partners. Classified information is classified to protect the national interest and is classified as Confidential, Secret, or Top Secret. These levels of classification and their relationship to the Alberta classification guideline and that developed by the Public Sector Chief Information Officer Council (PSCIOC) are illustrated in Figure 2.

Figure 2
Comparison with GOC Information Classification

PSCIOC	Government of Alberta	Government of Canada		
		Designated	Classified	
Unclassified	**Unrestricted**	**Unclassified**		
Low Sensitivity	**Protected**	**Protected A**		**Sensitive Information**
Medium Sensitivity	**Confidential**	**Protected B**	**Confidential** (If compromised, could reasonably be expected to cause injury to the national interest)	
High Sensitivity	**Restricted**	**Protected C**	**Secret** (If compromised, could reasonably be expected to cause serious injury to the national interest)	
			Top Secret (If compromised, could reasonably be expected to cause exceptionally grave injury to the national interest)	

Requirements

Generally, any sharing of classified information between the Government of Canada and the Government of Alberta will involve:

- security clearances for individuals who have access to classified information;
- a Memorandum of Understanding related to access, use, disclosure of the information;
- appropriate security safeguards for handling classified information (e.g., labeling, storage, transmission); and
- education and training of individuals with access to ensure requirements are met.

Ministries of the Government of Alberta must:

- ensure that classified information is not used, without prior written consent of the Government of Canada, for a purpose other than that for which they were provided;
- not disclose, release or provide access to the information to a third party unless the Government of Canada provides prior written consent;
- implement procedures necessary to prohibit publicity concerning the existence of any sensitive federal information unless the Government of Canada provides prior written consent; and
- maintain accountability and control procedures to manage the dissemination of, and access to the information.

More information about procedures required by the Government of Canada can be found at: http://www.tbs-sct.gc.ca/gos-sog/gossecurity_e.asp.