Information Management Manual
2010

Office of the Information Commissioner of Canada

Commissariat à l'information du Canada

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this manual is to provide direction to OIC staff on the management of corporate information.

1.2 Organization of the Manual

The first section of the manual outlines its purpose. Sections two to seven of the manual comprise the governance, business rules and support for information management covering all OIC functions.

Section eight of the manual provides specific accountabilities for IM within OIC functions, along with detailed descriptions of:

- Corporate records within the function
- The file classification structure
- Approved retention and disposition schedules.

The remaining functions and annexes provide information on IM responsibilities and:

- Procedures for departing employees
- Handling of sensitive records
- Use of the electronic network.

1.3 Definition of Terms Used

See Annex A for a definition of the terms used in this document.

2 Governance and Accountability

The management of information in the OIC is based on federal legislation, Government of Canada IM policy and business rules originating within the OIC. As such, managing information in the OIC occurs through an accountability structure with set roles and responsibilities.

2.1 Legislation and Policy

Library and Archives of Canada Act - Specifies that the records of Federal Government institutions and ministerial records (regardless of recording media) shall not be destroyed or disposed of without the consent of the National Librarian and Archivist. To comply, institutions must:

- obtain consent of the National Librarian and Archivist before disposing of any record that is under institutional control; and
- arrange for the transfer of historical information to Library and Archives Canada in accordance with schedules or other agreements.

Access to Information Act - Requires an ability to find and disclose to requesters, within 30 days, records under the control of the institution, subject to specific and limited exemptions. The Act also makes it a criminal offence for any government employee to knowingly destroy, mutilate, alter, falsify or conceal a record.

Privacy Act - Requires that personal information be made available to an individual upon request unless a specific exemption applies. The Act also states that information on individuals must be used only for purposes that are consistent with the reason for collecting the information, and personal information should not be retained unnecessarily but should be disposed of when it is no longer required.

Personal Information Protection and Electronic Documents Act - Legitimizes the use of electronic records in the provision of Federal information and states that an electronic signature may be as valid as a pen signature where law requires the use of a signature.

*Policy on Information Management (*Treasury Board Secretariat) - The policy reinforces that information is a strategic business resource that needs to be managed accordingly. The requirements of the policy are to:

- manage information to facilitate equality of access and promote public trust, optimize information sharing and re-use, and reduce duplication, in accordance with legal and policy obligations
- document decisions and decision-making processes throughout the evolution of policies, programs and service delivery
- ensure that information created and acquired is relevant, reliable and complete
- limit the collection, use and disclosure of personal information in accordance with the *Privacy Act*
- manage information in accordance with the *Official Languages Act*
- manage information to ensure its authenticity, accuracy, integrity, clarity and completeness for as long as it is required by statutes and policies
- implement governance and accountability structures for the management of information
- use electronic systems as the preferred means of creating, using and managing information
- protect essential records to ensure the continuity of key services and business operations
- preserve information of enduring value to the Government of Canada and to Canadians
- dispose of information no longer required for operational purposes in a timely fashion
- foster supportive environments for information management and ensure that employees meet their responsibilities for managing information
- assess the effectiveness and efficiency of the management of information throughout its life-cycle.

Government Security Policy - The purpose of this policy and its related standards is to ensure all sensitive information and other assets of the Federal government are appropriately safeguarded. The policy calls upon institutions to:

- "classify" information (as confidential, secret or top secret) when its unauthorized disclosure or other compromise could reasonably be expected to cause injury to the national interest;
- "designate" information (as protected) when its unauthorized disclosure or other compromise could reasonably be expected to cause injury to interests other than the national interest;
- apply the information classification and designation system by means of a corporate guide;
- conduct threat and risk assessments;
- apply physical and information technology security measures to control access to and prevent compromise of classified or designated information; and
- name a senior official to co-ordinate and direct the ongoing implementation of the policy.

2.2 IM Accountability Structure

Information being a strategically valuable resource will be managed, controlled and supported in the OIC through an accountability structure in the same manner and following the same discipline as other resources.

The IM accountability structure is comprised of the following roles.

- Information Commissioner
- Chief Information Officer
- Information Management Division
- Heads of the various functions
- Employees
- Information and Records Management specialists
- Information Technology specialists
- Information Management practitioners

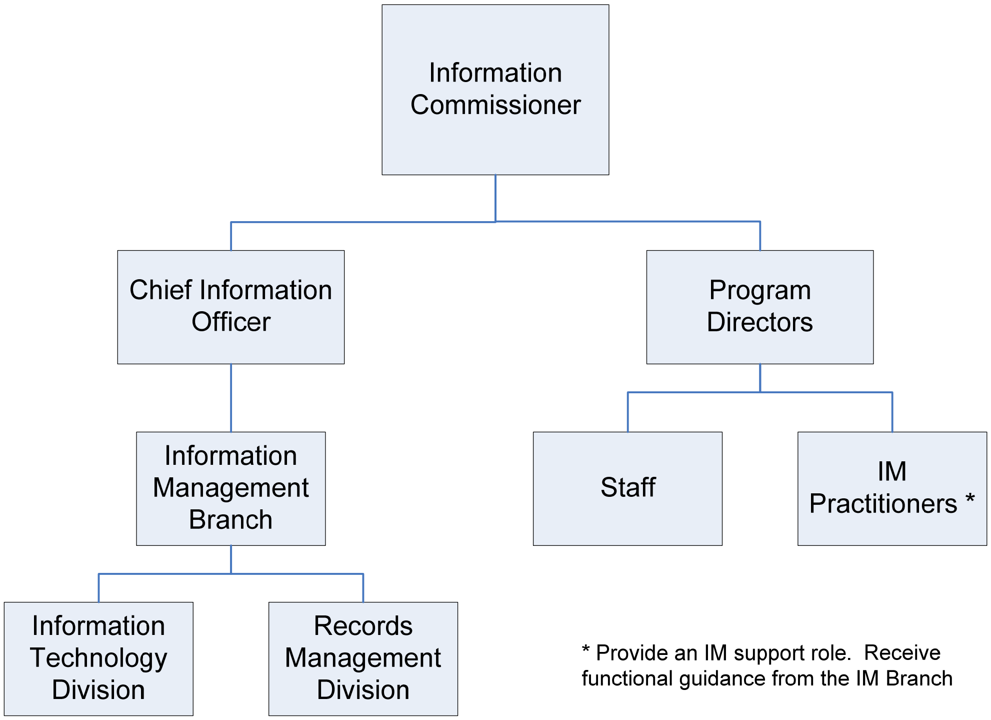
Information Commissioner
Chief Information Officer
Program Directors
Information Management Branch
Staff
IM Practitioners *
Information Technology Division
Records Management Division
* Provide an IM support role. Receive functional guidance from the IM Branch

Figure 1 – IM Accountability Structure

Also providing a role in the accountability structure are information management stakeholders such as:

- Departmental Security Officer
- Access to Information and Privacy Administration
- Records function and Library Services.

3 IM Roles and Responsibilities

Information Commissioner

IM responsibilities of the Information Commissioner include the following.

a. Support and allocate appropriate resources to the implementation of IM policy and related instruments in support of OIC's requirements and in compliance with Government of Canada statutes and policy.

b. Promote a culture that recognizes information as a strategic resource and an integral part of Government of Canada program and service delivery.

c. Designate a senior executive with responsibility for OIC-wide accountability for the management of information.

Chief Information Officer

IM responsibilities of the Chief Information Officer include the following.

a. Report to and represent the Information Commissioner for the purposes of managing the OIC's program for managing information.

b. Oversee the implementation, compliance and maintenance of the OIC's IM program in compliance with OIC policies and with Government of Canada statutes and policy.

c. Ensure that IM is designed into the planning, budgeting and business processes of the OIC and into the design of new or updated information systems.

d. Provide IM advice and guidance to managers, staff and information management and technology specialists.

e. Ensure the protection of enduring and essential information over time and through technology changes.

f. Facilitate the security of information under the control of the OIC.

g. Oversee the establishment of disposition authorities with Library and Archives Canada, and the formal disposition of records.

Program Heads

IM responsibilities of Program Heads include the following.

a. Promote and ensure the implementation and compliance with IM policies, business rules and best practices.

b. Ensure that every person doing work for the OIC (employee, contractor, consultant, student and volunteer) is aware of their IM responsibilities in compliance with OIC policies and with Government of Canada statutes and policy.

c. Ensure that IM requirements are designed into the planning, budgeting and business processes of the business unit.

d. Support and promote to staff the routine disposal of transitory records in accordance with the *Authority for the Destruction of Transitory Records (Library and Archives Canada)*.

Employees

IM responsibilities of OIC employees include the following.

a. Comply with OIC IM policy and business rules and with Government of Canada IM policies and statutes.

b. Document, on behalf of the OIC, decisions, significant actions, transactions and processes. Capture these within appropriate IM systems and repositories.

c. Organize all documents within the OIC classification structure.

d. Take measures to share and re-use information, and to reduce duplication.

e. Only dispose of transitory records in accordance with the *Authority for the Destruction of Transitory Records (Library and Archives Canada)*.

Information and Records Management Specialists

Responsibilities of Information and Record Management specialists include the following.

a. Develop and implement IM policy, business rules, practices and guidelines.

b. Provide information and records management advice and guidance to OIC staff.

c. Maintain the OIC Classification Structure used to organize, retrieve and manage records in all recording media across the OIC.

d. Classify paper and electronic documents according to the UCS and perform quality assurance monitoring on the organization of records.

e. Manage the retrieval, charge-out/in, routing and security of paper files from the Records Office.

f. Coordinate the transfer of inactive records to off-site storage facilities.

g. Collaborate in identifying informational and technical requirements, and in the design and implementation of new or upgraded IM tools, systems and repositories.

h. Provide training on IM tools and systems to OIC employees.

i. Maintain appropriate security controls to electronic documents and associated metadata in RDIMS.

j. Participate in monitoring compliance with IM statutes, policies, business rules, practices and guidelines.

k. Ensure the legal disposal of records according to the *Library and Archives of Canada Act* and associated disposition authorities.

Information Technology Specialists

IM responsibilities of Information Technology specialists include the following.

a. Provide an appropriate technology environment, to facilitate IM across the OIC.

b. Develop technical specifications for IM tools, and assist in the design, configuration, testing and roll-out of new or updated IM systems throughout the OIC.

c. Perform modifications and maintenance to IM systems.

d. Perform backup and recovery functions for all electronic files and documents within IM systems.

e. Maintain security controls within IM system.

f. Provide advice to IM specialists, practitioners and management on technical issues.

Information Management Practitioners

Responsibilities of Information Management Practitioners include the following.

a. Advise the Program Head on IM issues.

b. Provide first-level IM support to staff within the business unit.

c. Maintain the classification structure at the ‘activity’ level.

d. Obtain guidance from and collaborate with IM and technology specialists.

e. Conduct quality assurance on information captured by staff within the program.

4 Information Management Tools

The following tools support the management of information in the OIC.

4.1 RDIMS

RDIMS (Records, Documents and Information Management System) is a product of the Treasury Board Shared Systems Initiative, which is a joint undertaking between the Treasury Board Secretariat and all GoC institutions. RDIMS is a standard solution endorsed by the Government of Canada (GoC) to manage information, documents and records according to record keeping best practices, the *Access to Information Act* and the Policy on Information Management.

RDIMS has been adopted by the OIC as the official repository for electronic documents that are created and received in fulfilling its mandate.

One of the main benefits of RDIMS is the ability to capture 'metadata' (descriptive information) on each electronic document or information object saved into the RDIMS repository. The metadata facilitates searching for and managing OIC information. A description of OIC metadata is provided in Annex E.

4.2 OIC Classification Structure

The OIC has adopted a structure to organize and manage all records created and received, regardless of medium. Based on the BASCS (Business Activity Structure Classification System) model developed by Library and Archives Canada, records are organized into three successive tiers: function, sub-function and activity. This classification structure is derived from the mandate and accountability structure of the OIC. This causes the classification structure to be more stable and reliable.

4.3 Business Applications

Several applications, such as IIA (Integrated Investigation Application) and LTS (Legal Tracking System), exist in support of specific OIC business functions. These applications assist in managing corporate OIC information by providing an interface to RDIMS to store, organize and manage records through a life-cycle.

4.4 Shared Electronic Folders

Electronic folders, that are accessible to staff in specific OIC functions, are also used to store, organize and access electronic documents. These shared electronic folders are available on various drives on the OIC network and are used where RDIMS has not been implemented. The use of shared electronic folders will be phased-out with the full implementation of RDIMS.

4.5 E-Mail Folders

Folders within the OIC electronic mail system are also used to organize and access e-mail messages that are sent and received. These folders are created and maintained within the e-mail accounts of individual OIC staff. E-mail messages having long-term corporate value are stored in RDIMS or in shared electronic folders.

5 IM Business Rules

Business rules translate IM policies, standards and best practices into practical requirements. They reflect the essential and mandatory conventions for the management of information.

The OIC, in accordance with GoC standards, manages corporate information in the RDIMS document and records management system. Below are the business rules for managing information in the OIC using RDIMS.

5.1 Create and Receive Documents

The preferred medium for managing OIC records throughout their lifecycle is electronic. The different record types saved and managed in RDIMS are listed below.

a. *Documents designated to Protected B* – All electronic documents created and received in the course of conducting OIC business that are unclassified or security designated to Protected B are saved and managed in RDIMS.

b. *Documents designated Protected C or higher* - All electronic documents created and received in the course of conducting OIC business that are designated Protected C or higher are stored on removable media and locked in a security approved container.

c. *Electronic mail messages* - Electronic mail messages and attachments that contain OIC business information that have long-term corporate value are saved in RDIMS.

d. *Works in progress* – Preliminary versions of documents or works in progress are saved and managed in RDIMS.

e. *Create versions of documents* - New versions of electronic documents will be made at the discretion of the author to capture significant or fundamental changes. All previous versions will be maintained in RDIMS.

f. *Reference Material* - Reference materials in electronic form that substantiate or validate a decision, position or action taken as part of OIC business are saved in RDIMS.

g. *Original Publications* - Original publications, e.g., reproduction proof or camera ready / web-ready copy, in electronic form produced by or for the OIC are saved and managed in RDIMS.

5.2 *Organize and Classify Documents*

Associate documents to a file number - All electronic documents stored in RDIMS will be associated to a file number in the OIC Classification Structure.

Note: The OIC Classification Structure is used across the organization to consistently organize records and to facilitate their retrieval and management. The OIC Classification Structure is based on a standard developed by Library and Archives Canada that groups records by functions and activities.

5.3 *Store and Protect Documents*

a. *Paper records* - A paper record containing a signature or handwritten notes will be scanned. The scanned image will be saved and managed in RDIMS.

b. *Access rights on electronic documents* – Access rights on electronic documents stored in RDIMS will be set to enhance operational efficiency and to protect sensitive documents.

c. *Document access rights* – The profile of electronic documents stored in RDIMS that are not security classified will, by default, be viewable to all staff. Access to documents and profiles can also be expanded based on business requirements.

d. *Document passwords* - Passwords given to documents will be removed before saving them in RDIMS. The access control settings in RDIMS are the approved method to restrict access to sensitive information.

e. *Mark documents as read only* – Documents declared final will be designated as ‘read-only’ to protect them from being altered.

f. *Documents stored on the Internet or Intranet* - When an electronic document stored in RDIMS is published to the OIC Internet or Intranet site, the document contained within the site is deemed a copy.

g. *Transfer document custodian rights* – When an OIC staff member leaves the organization, the custodian rights to documents under their control will be transferred to another OIC employee. Transferring custodian rights will be approved by business unit manager. *For more information, see Annex - C - Managing Records When an Employee* Leaves*.*

5.4 *Retain and Dispose of Documents*

a. *Assign retention periods* - All electronic and non-electronic records managed in RDIMS will be assigned a retention period. Retention periods will be assigned to records through their association to a file number from the OIC Classification Structure. Retention periods are only set in accordance with approved Records Disposition Authorities.

b. *Extend or suspend retention periods* - The retention period of an individual record or a collection of records will be extended or suspended (frozen) when the records are subject to:

- a request received under Access to Information or Privacy legislation;
- a formal investigation;
- legal proceedings; or
- other conditions that alter the normal operational, fiscal, administrative or legal value of the record(s).

c. *Delete transitory documents* - Transitory documents will be deleted from RDIMS when they no longer have value to the OIC. Transitory records will be placed into a 'queue' where an IM specialist will validate their deletion.

d. *Delete other records* – Other OIC business records (non-transitory) will be deleted or disposed of based only on disposition authorities issued by Library and Archives Canada and approved by the OIC.

e. *Dispose of metadata* - Metadata associated to electronic and non-electronic records in RDIMS will be disposed of in the same manner and at the same instance as the associated records.

f. *Manager approval* - Written approval for the disposition of all electronic and non-electronic records must be obtained from the workgroup manager prior to undertaking the disposition action.

6 Use and Management of Information

The manner that the main types of records are used and managed in the OIC is as follows.

6.1 Electronic Documents

RDIMS, when fully implemented across the OIC, will be the official repository for storing, retrieving and managing all electronic documents that are created and received while fulfilling the OIC business mandate. Users will be prompted to store electronic documents in RDIMS when saving documents in applications such as Word or Excel.

Users will have the option to invoke a number of other RDIMS functions such as creating versions of documents, setting access controls and retrieving documents through browsing or searching the RDIMS repository.

6.2 E-mail Messages

Like electronic documents, e-mail messages that have long-term value to OIC business functions will be stored in RDIMS (when the application is fully implemented). When an e-mail message is profiled to RDIMS it is declared read-only, meaning the e-mail cannot be deleted or altered.

E-mail messages that remain in a staff member’s inbox or personal folders, and a decision has been made not to file them in RDIMS, will be considered to have short-term value to the OIC. These e-mail messages are considered transitory and can be deleted from the e-mail system when necessary.

6.3 Paper-based, Non-electronic Records

Paper-based, non-electronic records will be managed by the Records Management Office following existing processes. All paper-based records will be managed through a lifecycle based on approved records disposition authorities. This will be facilitated by assigning these records to a file number in the OIC Classification Structure.

6.4 Web Content

Information content published to the OIC Internet or Intranet will be managed in one of two ways.

- When Web content originates from a document stored in RDIMS, the document will be declared ‘read only’ in RDIMS. The document stored in RDIMS is the authoritative source for the Web information content. The version of the information content residing in the Web is a convenience copy.

- Information content originating from the OIC Internet or Intranet will be managed through its entire lifecycle in RDIMS. This will occur by archiving the

Web content, or generating ‘snap-shots’ to maintain an official record of the Web content.

7 Information Security

The OIC manages sensitive records as part of fulfilling its mandate. Records that are “sensitive” contain information that can cause different degrees of injury to an individual, a company or the country if the information were disclosed in an unauthorized manner.

When managing sensitive records specific action is taken to ensure the records are identified according to their degree of sensitivity and are used, stored, transmitted and destroyed in an appropriate manner.

A guideline on managing sensitive records in the OIC is included in Annex D of this manual.

8 IM Support

Information Management in the OIC will be supported by IM and IT specialist staff and by IM practitioners within each OIC function. IM Practitioners are designated by the Program Head.

8.1 Support Process

IM practitioners exist in each OIC function to provide basic IM and IT support. IM and IT issues and requests for services that cannot be responded to by the IM practitioner are escalated to the formal support process through the OIC Help Desk. All support requests are captured in a ticketing system. The tickets are issued to IM support (Records and Information Management specialists) or to IT support (RDIMS and IT infrastructure) personnel. Support staff resolves the issue or responds to the request. Issues that are not resolved or requests that are not responded to, based on support standards, are escalated.

The Help Desk is equipped to receive and dispatch telephone and e-mail requests from users. As a minimum, the support service is available within core business hours (9:00 to 17:00 Monday to Friday). To support exceptional business requirements the Help Desk service is sometimes available for extended hours (17:00 to 22:00 Monday to Friday and 10:00 to 16:00 Saturday and Sunday).

The support process is described in the diagram below.

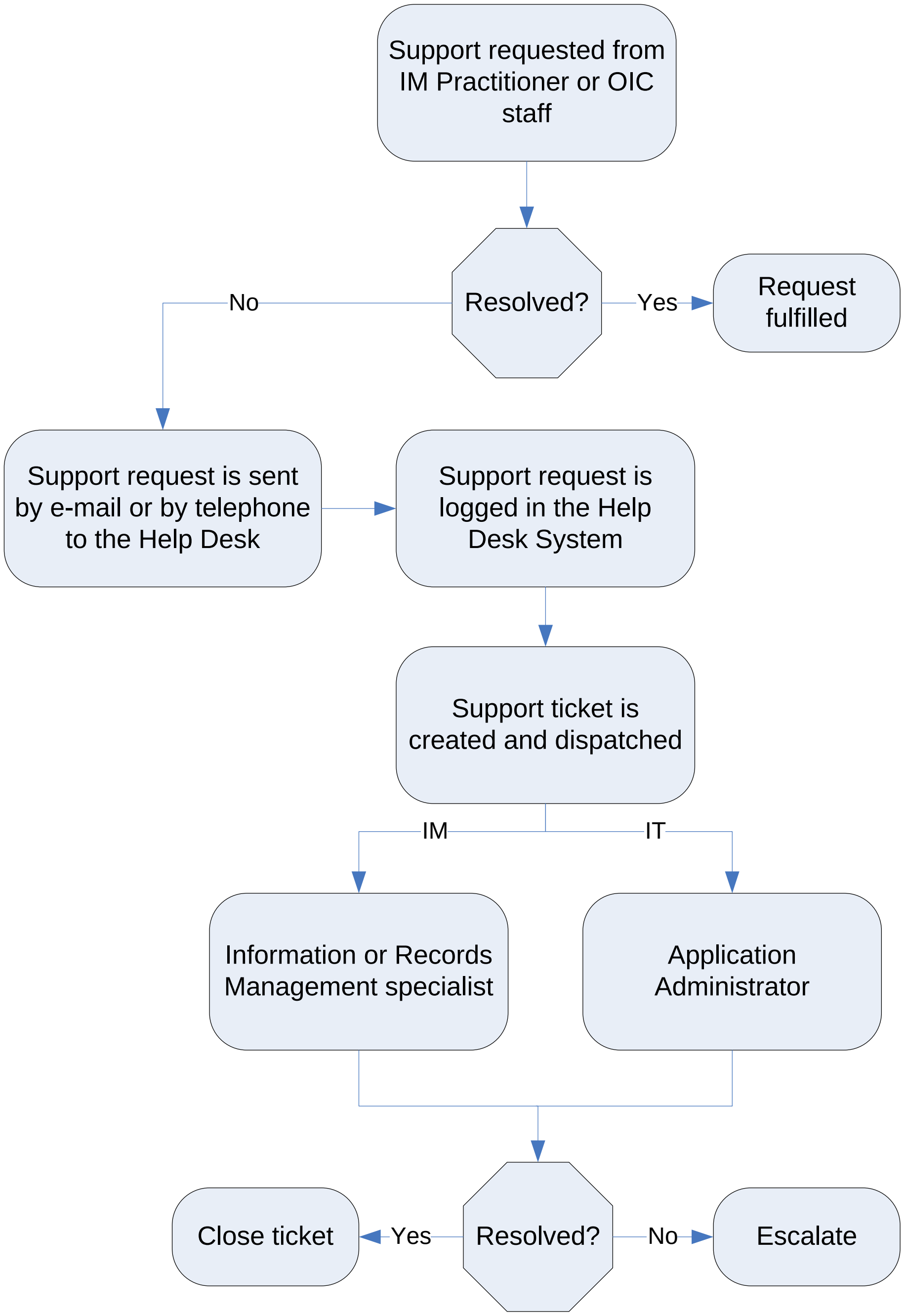
Support requested from IM Practitioner or OIC staff
Resolved?
Yes
Request fulfilled
No
Support request is sent by e-mail or by telephone to the Help Desk
Support request is logged in the Help Desk System
Support ticket is created and dispatched
IM
IT
Information or Records Management specialist
Application Administrator
Resolved?
Yes
Close ticket
No
Escalate

Figure 2 - IM Support Process

The general support activities and the roles that fulfill them are described in the section below, IM Support Activities and Roles.

8.2 IM Support Activities and Roles

General Support Activities

Below are the general support activities and the roles that will provide the support.

Support Activities	Provided By
Help Desk / Trouble Ticket Management - Manage and track IM and IT issues and requests for support services	OIC Help Desk (Access IM / IT)

IM Support Activities

Below are the IM support activities and the roles that will provide the support.

Support Activities	Provided By
IM Planning, Advice and Guidance - IM Planning, advice and guidance for end-users and managers - Advice and guidance on the lifecycle management of information within the business units	Library and IM Manager Records Manager
IM Training and Coaching - Ongoing training and coaching on IM and RDIMS Note: Training options will also include on-line, self-paced tutorials.	IM Practitioner in each OIC function
Information Research Assistance - Advice and guidance on research (electronic and paper) - File retrieval (paper)	Records Office
Changes to the OIC Classification Structure - Requests new file numbers and changes to the classification structure	Records Office – Functions and sub-functions IM Practitioners - Activities
Metadata Management - Maintain RDIMS metadata fields and values	RDIMS Administrator
Records Management - Physical file storage management, file movement and transfers	Records Office

Support Activities	Provided By
▪ Manage electronic records	
Retention and Disposition Management ▪ Prepare submissions to obtain approved Records Disposition Authorities ▪ Establish disposition authorities ▪ Establish and maintain retention and disposition schedules ▪ Dispose of records (paper and electronic)	IM Manager Records Manager

IT Support Activities

Below are the IT support activities and the roles that will provide the support.

Support Activities	Provided By
Account and Group Management ▪ Create, remove and manage RDIMS users and groups	RDIMS Administrator
RDIMS security	RDIMS Administrator Security Officer
Storage Management ▪ Transfer and archive non-active records to off-line or near-line storage	RDIMS Administrator Database Administrator
Generate reports	RDIMS Administrator

9 Review and Update

The IM Manual will be reviewed and updated annually coinciding with the InfoSource submissions.

10 Managing Information by OIC Function

The following section describes the manner that information is managed within the various functions of the OIC and IM business rules that are specific to the function. This section also provides instruction to users on:

1. The file classification structure, by function
2. IM accountabilities, by function
3. Records disposition and retention schedules.

(Approvals by business areas – will not be covered at Ex Com on January 28, 2010)

Annex - A - Definition of Terms

Document: Textual, numerical or graphical information recorded in a manner that provides context (e.g., date, subject, author, purpose) and is structured in a self-described manner. Documents can take a variety of forms including letters, memoranda, electronic mail messages, reports, budgets, policies, contracts, strategies, plans, proposals, analyses, presentations and forms.

Disposition / Disposal of Records: The destruction of records or the transfer of records outside the control of an institution of the Government of Canada. Usually undertaken in accordance with an established retention and disposition schedule and pursuant to disposition authorities issued by Library and Archives Canada.

***Electronic Mail (E-mail) Messages*:** Communications sent or received internally or externally on an electronic mail system, including any attachments transmitted with the message as well as the associated transmission and receipt data.

Employees: All employees of the OIC, including contractors, consultants, students, volunteers and other authorized users of information under the control of OIC's information environment.

Information: A representation of facts, ideas, or opinions about objects, events, and/or processes that exists on any medium or format, and has a particular meaning within a particular context.

Related terms under the umbrella term *Information* are as follows:

> ***Government information:*** Information created, received, used, and maintained regardless of physical form, and information prepared for or produced by the Government of Canada and deemed to be under its control in the conduct of government activities or in pursuance of legal obligations.
>
> ***Record*:** Any documentary material other than a publication, regardless of medium or form.
>
> ***Transitory records:*** Records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record. Transitory records do not include records required by government institutions or Ministers to control, support or document the delivery of programs, to carry out operations, to make decisions or to account for activities of the Government.

Information Life Cycle: A series of stages through which information passes during its lifetime. The information life cycle encompasses the following: planning; collection, creation, receipt, and capture of information; its organization, use and dissemination; its maintenance, protection and preservation; its disposition; and evaluation.

Government Institution: Federal, provincial and territorial government entity such as a department, agency and crown corporation.

Management of information: An element of every job function in the Government of Canada that has to do with treating the information used or produced in the course of performing job duties as a strategic business resource and in line with legal and policy requirements.

Metadata: Descriptions of stored data. That is, information that describes the content, context and structure of recorded information objects. Examples of metadata include information on the author, subject, creation date and security designation of the information.

Records Classification Structure: A logical arrangement of records in a structure that reflects the subjects and activities of the organization. The classification structure facilitates the management of records through a life-cycle.

Records Management: A field of management responsible for the systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Records Retention Schedule*:* Identifies the period of time that specific records should be retained to meet legal, business and accountability requirements of the Office. The schedule can also identify the disposition action to be applied to the records, and the owner or custodian of the records.

Retention Period: The period of time a record is kept before it is disposed or transferred outside the control of the institution. Retention periods reflect the operational, fiscal, legal, informational, archival and historical value of the record.

Annex - B - Managing Sensitive Records

What are Sensitive Records?

Records that are “sensitive” contain information that can cause different degrees of injury to an individual, a company or the country if the information were disclosed in an unauthorized manner. The Government of Canada groups sensitive records into six main categories corresponding to the severity of possible injury. The first three categories are referred to as *designated* and the last three are referred to as *classified*.

<table>
<tr><th>Categories of Sensitivity</th><th>Description</th></tr>
<tr><td colspan="2"><b><i>Designated Records</i></b></td></tr>
<tr><td>Protected A</td><td>This information is not sensitive to the national interest but could cause embarrassment to an individual or a company if it were disclosed in an unauthorized manner. For example, loss of privacy through the disclosure of a salary figure.</td></tr>
<tr><td>Protected B</td><td>This information is not sensitive to the national interest but serious injury to an individual or a company could result if the information were disclosed in an unauthorized manner. Examples include: medical records; personal evaluations; indications of political beliefs, associations or lifestyles; sensitive contracts; police reports; financial records; and, information received in confidence.</td></tr>
<tr><td>Protected C</td><td>This information is not sensitive to the national interest but very serious injury to an individual or a company could result if the information were disclosed in an unauthorized manner. Examples include: life threatening information; serious criminal intelligence and grave socio-economic information applicable to a geographic area, time frame or interest.</td></tr>
<tr><td colspan="2"><b><i>Classified Records</i></b>
Examples of classified information include: records of federal-provincial relations, international affairs and economic interests of Canada; information under the cabinet papers system; information involving security, intelligence or security assessments.</td></tr>
<tr><td>Confidential</td><td>Information that could be expected to cause minor injury to the national interest if it were disclosed in an unauthorized manner.</td></tr>
<tr><td>Secret</td><td>Information that could be expected to cause serious injury to the national interest if it were disclosed in an unauthorized manner.</td></tr>
<tr><td>Top Secret</td><td>Information that could be expected to cause exceptionally grave injury to the national interest if it were disclosed in an unauthorized manner.</td></tr>
</table>

What is ‘Managing’ Sensitive Records?

The act of ‘managing’ sensitive records is essentially taking specific action to ensure the records are identified according to their degree of sensitivity and are used, stored, transmitted and destroyed appropriately.

Why is Managing Sensitive Records Important?

Records that are sensitive are often the most important within an organization. As a result, they need to be protected from unauthorized disclosure which could result in injury to an individual, a company or the country. Measures also need to be taken to ensure that sensitive records are not accidentally or illegally destroyed.

Managing Sensitive Records

Mark Sensitive Records

Once sensitive records have been identified, the next step to protecting them is to indicate on the record the:

- designated or classified level
- date the record was created or received, and
- whenever possible, the date or event at which declassification or downgrading is to occur (see below for more information on declassifying or downgrading records).

Indicating the sensitivity level on the record alerts those who use it that appropriate safeguards must be taken to protect the records.

Markings that identify records as being sensitive are indicated in different ways depending on the media.

- For paper and electronic documents, whether they are a draft, copy or final, mark each page.
- For electronic storage devices place a label on the outside of the device that corresponds to the highest level of sensitivity of information it contains.

Keep in mind that records are to be designated or classified only for the period of time required for safeguarding. Records are also to be declassified or downgraded when the protection is no longer necessary or no longer needed at the same level (see below for more information).

Storing Sensitive Records

Sensitive paper records must be stored in an approved secure room, safe or cabinet that meets Government of Canada standards[1]. Sensitive electronic records, up to Protected

[1] Plans for the construction of secure rooms must be approved by the Departmental Security Officer before construction commences.

B can be stored on the OIC network. Sensitive electronic records designated Protected C or Classified (Confidential, Secret or Top Secret) must be stored on a computer that is not connected to the OIC LAN or, on removable storage media such as a removable hard drive or USB drive ('memory stick'). Computers used to store sensitive records must be located in a secure room. If sensitive information is stored on a portable computer or on removable storage media, these must also be stored in a secure room, a cabinet or safe when not in use.

Circulating or Transmitting Sensitive Records

Sensitive paper records that are circulated must be placed in a marked file folder and kept in a secure container when not in use. Sensitive paper records must be circulated, organized and maintained within file folders as follows.

• Protected A, B and C -	Blue border
• Confidential -	Green border
• Secret -	Red border
• Top Secret -	Red border with red hatch marks

If a file folder contains a combination of unclassified and sensitive records, the entire file folder assumes the highest sensitivity level of the records in that file.

Only use the OIC e-mail messages system to send or distribute sensitive records up to Protected B. Sensitive messages that are designated Protected C or Classified (Confidential, Secret or Top Secret) must be circulated by hand.

Using Sensitive Records

When using sensitive records it is important to prevent unauthorized people from seeing, hearing, recording or copying the information. This is accomplished by using the records within adequate security zones. Usually, an adequate security zone is an enclosed office or room with a door that can be locked. It can also be an open area where access is controlled and monitored.

If leaving a room where secure records are in the open, even for a brief period, always lock the door. When finished using sensitive records always put them, or the device they are stored on, away within a secure room, cabinet or safe.

Packaging Sensitive Records for Mail or Courier

When sensitive records are sent by mail or courier they must be properly packaged. The manner they are packaged depends on the sensitivity level or the records.

Sensitivity Level	Packaging Method
Protected A	Place in a single gum-sealed envelope without security markings.
Protected B	Place in a double, sealed envelope. The outer envelope is sealed and without security markings. The inner envelope is gum-sealed, addressed and marked with the sensitivity level of

	the contents. For personal information the inner envelope should indicate *To be opened by addressee only*.
Protected C	Same measures as Protected B. Always indicate on the inner envelope *To be opened by addressee only*.
Confidential	Same measures as Protected C if sent within the OIC. In addition, enclose a self-addressed envelope with instructions for the receiver to acknowledge receipt of the material and to return the acknowledgement to the sender. If the envelope is sent outside the OIC within Canada, the U.S. or the U.K use one of the following options. • A reliable postal or courier service that provides proof of mailing and a record while in transit and of delivery. • Carried by an authorized individual with an appropriate security clearance, using a locked case tagged with a forwarding or return office address. • Classified diplomatic courier bag service. If the envelope is sent to all other foreign countries use one of the following options. • Classified diplomatic courier bag service. • Carried by an authorized individual with a security clearance, using a locked case tagged with a forwarding or return office address.
Secret	Same measures as Protected C. In addition, the inner envelope must be closed with an approved seal.
Top Secret	Same measures as Secret but Top Secret records are never sent by a postal or courier service. A record of the records being sent is created, the intended recipient is notified in advance and the records are sent in an approved locked case carried by an individual with Top Secret clearance.

Receiving Sensitive Records

All sensitive records, either Designated or Classified are to be hand delivered unopened to the addressee or to the person responsible for the program.

Keep a record of receiving Secret or Top Secret records such as the date received, the general subject and the name of the person or group the records were received from.

Agreements on Exchange of Sensitive Records

When exchanging sensitive information with organizations outside the OIC always establish a written agreement that stipulates the necessary safeguards.

The agreement for exchanging information should:

- describe the information to be exchanged and the purpose for exchanging it;
- identify all personnel who will have access to the information and stipulate the safeguards required to protect it;
- state the conditions for disclosing the information to third parties, including the need to obtain prior authority from the OIC; and,
- stipulate that Top Secret information is not to be provided without the recipient being cleared to Top Secret.

Declassifying or Downgrading Sensitive Records

Information should be declassified or downgraded when its sensitivity decreases over time or when specific events occur.

Declassifying information occurs when it no longer requires protection. Downgrading occurs when protection is no longer needed at the higher level. Declassifying or downgrading information can only be undertaken by designated employees. In the OIC, this is the Security Officer.

Information in your custody and use that was received from outside the OIC can only be declassified or downgraded in accordance with established agreements and only after consulting the originating organization.

How to Physically Dispose of Sensitive Records

Physically disposing of sensitive records must be handled differently depending on the recording media of the records (paper or electronic) and their sensitivity.

Designated Records

	Minimum Destruction Method		
Sensitivity	**Paper**	**Electronic**	**Certificate of Destruction**
Protected A	Hand shred	Delete from media	Not required
Protected B	Machine shred	Delete from media and re-format media	Not required
Protected C	Machine shred	Degauss[2] media	Recommended

[2] Degauss - A process by which a computer hard drive is unformatted by randomly scrambling the bits on the drive therefore rendering the data unreadable.

Classified Records

	Minimum Destruction Method		
Sensitivity	**Paper**	**Electronic**	**Certificate of Destruction**
Confidential	Approved shredder	Degauss and physically destroy media	Not required
Secret and Top Secret	Approved shredder	Degauss and physically destroy media	Required

Annex - C - Managing Records When an Employee Leaves

Whether you have worked within the OIC for ten months or ten years, during that time you created and received many records that are important.

When you leave your organization, these records stay within the OIC and are your legacy. They represent and document the unique contributions you made to the Canadian Federal Government and to Canadian citizens.

These records will continue to be valuable after you leave the organization so it's important that your legacy of information is well managed.

In the period just prior to your departure there are specific responsibilities that you and your manager should do.

Responsibilities of Employees

As an employee, there are four main tasks you need to complete to ensure that your legacy of information is in the best condition possible after you are gone.

1. *"Clean up" the records stored in your filing cabinets and stored on network drives, on your personal computer and on removable disks.*

   Dispose of ***transitory records*** if they are no longer valuable to the organization or to the OIC. Transitory records have short term value. For example:

   - A document received as a copy and maintained for convenience without directing you to take action
   - Information required for a short period of time to complete a routine action or to prepare another record
   - Working notes – after the necessary information has been documented within an official record
   - Reference material
   - Information about meeting reservations, holidays, etc.
   - Personal information.

2. *Organize the records according to the classification structure of the organization and store them within an established system such as:*

   - RDIMS
   - shared electronic folders on the OIC network
   - paper file folders.

The system or location where you store your records should ensure that other staff in the organization can access your records after you leave.

For guidance and/or advice, consult with staff in the Records Management Office.

3. *Prepare a concise list, with descriptions, of all your records, both paper and electronic.*

   The list only needs to identify and describe the general groups of records that you have and where they are located (e.g., drawer one of filing cabinet, network drive Z, folder X, sub-folder Y). You want to make it easy for the staff replacing you or those requiring access to understand and gain access to the records.

4. *Before you leave meet with your manager and staff of the Records Management Office.*

   The purpose of this meeting is to ensure that your manager and staff of the Records Management Office have a clear understanding of the records under your control, where they are located and how they are organized.

   Don’t have this meeting on the last day before you leave. There may be things you need to do as a result of the meeting and you want to leave yourself and others enough time.

Responsibilities of Managers

There are three records management tasks a manager should do when informed that an employee is leaving.

1. Have two meetings with the employee before they leave the organization.
   a. The first meeting, immediately after they have provided notice of their departure, is to discuss their responsibilities for cleaning and organizing any records under their control.
   b. The second meeting, a few days before the employee is scheduled to leave, is to ensure you are provided with a clear description of the records under their control, where they are located and how they are organized.
2. Assign responsibility over the records to a person who will replace the departing employee or to an employee who will assume interim responsibility. Ensure that full rights to electronic records are provided to the person assuming responsibility. Obtain passwords, keys or combinations to filing cabinets.

3. Contact the Records Management Office to inform them of the employee’s departure date.

Annex - D - Policy on the Use of the OIC Electronic Network

EFFECTIVE DATE

This policy takes effect Dec 17, 2008 and supersedes all previous directive of the same subject.

BACKGROUND

Treasury Board (TB) approved a government-wide *Policy on the Use of Electronic Networks* in February 1998. The introduction of this policy reflected a growing concern that inappropriate use of publicly funded electronic networks could reduce productivity, increase costs, compromise information assets and security, and risk embarrassment or legal liability for individuals and government institutions.

The TB policy requires government organizations to implement measures to ensure that inappropriate activity is not permitted in their working environments, and outlines provisions, which must be included in more detailed organizational policies. It assigns responsibilities to management and employees, and provides specific examples of uses, which are illegal or otherwise deemed unacceptable.

PURPOSE

This policy encourages the acceptable use of government Information Technology (IT) and electronic networks, effectively discourages inappropriate use, and ensures that the Office of the Information Commissioner of Canada (OIC) deals quickly, fairly and decisively with violations of this policy.

APPLICATION

This policy applies to all OIC authorized network users, whether employees or contract resources. It governs the use of OIC computing equipment connected to any internal or external network. This includes, but is not limited to workstations, servers, printers and smart wireless devices (i.e. Blackberry).

AUTHORITY

Authorized users, whether employees or contractors are to use OIC electronic networks for approved purposes only, in an informed and responsible manner, to protect and conserve these limited resources. The OIC will monitor compliance with this policy. Violations may lead to corrective measures, ranging from disciplinary to legal action.

INQUIRIES

Director Information Management
Policy, Communications and Operations
Telephone: (613) 947-9895

POLICY REQUIREMENTS

The focus of this policy is the acceptable use of electronic networks, which by definition includes the Internet. However, the same management philosophy applies to the use of all OIC Information Management and Information Technology (IM/IT) resources. The following guidelines are provided to advise managers and users on the application of the policy.

Authorized Uses

Access to the Organization's electronic networks, including access to the Internet through OIC networks, whether from a computer at work or at any other location, will be authorized by a user's manager or supervisor based on the user's job requirements and circumstances. For employees, authorized uses of electronic networks, such as the Internet, include the conduct of government business, professional activities, career development and limited personal use. These uses are subject to the following limitations.

General Limitations

All authorized use of electronic networks, including personal use, is subject to the provisions of this policy and any other policies of the government and the OIC.

Professional Activities and Career Development

The Internet offers a useful tool for professional and career development. While the OIC supports such use, it expects employees to act responsibly so as to ensure that this activity does not interfere with normal business operations.

Personal Use

Extensive personal use of the Internet can degrade the operation of network resources and lead to security breaches. For that reason, the following high demand, personal use activities are prohibited, unless specifically authorized by the employee's manager for business or employee career development purposes. This is a non-exhaustive list of prohibited activities and employees are advised to refrain from other demand-intensive activities undertaken for personal reasons:

- downloading specific file types for personal use, such as, MP3 files, executable program files (including computer files such as video games downloaded to run on a computer) and shareware (free software)

- listening to web radio, watching streaming video (e.g., music videos or web casts), playing interactive games and instant messaging (e.g., ICQ)

NOTE: Personal use must take place on personal time and be undertaken in a manner which will not add to organizational costs or interfere with its operations. Personal time consists of breaks, lunchtime and time before and after the employee's hours of work.

Management retains the right to place restrictions and conditions on the use of technology to ensure efficient and secure operation, information integrity and compliance with policy.

Inappropriate Uses

OIC electronic networks must not be used for the following purposes which are unlawful or deemed unacceptable by the government or the OIC:

- violations of the *Criminal Code*
- violations of statutes and regulations
- actions that can result in civil lawsuits by the individuals or entities harmed by such actions

The following are examples of unlawful activities:

- Defamation or harassment.
- Copyright and other intellectual property infringement (use of unlicensed software, etc.).
- Hacking or cracking of information or telephone systems, hardware or software.
- Intentional introduction of malware (includes viruses and spyware) to electronic networks.
- Knowingly posting inaccurate information that results in harm.
- Collecting and using data unlawfully or in violation of signed agreements and/or contracts.
- Intercepting private communications.
- Disclosing sensitive or personal information, business trade secrets, and sensitive government information without authorization.

The following are examples of unacceptable use:

- Sending classified or designated information on unsecured networks, unless it is sent in encrypted form.
- Accessing, without authorization, sensitive information held by the government.
- Attempting to defeat information technology security features.
- Causing congestion and disruption of networks and systems.
- Sending abusive, sexist or racist messages to employees and other individuals.
- Using the government's electronic networks for private business, personal gain or profit or political activity.
- Making excessive public criticisms of governmental policy.
- Representing personal opinions as those of the institution, or otherwise failing to comply with institutional procedures concerning public statements about the government's positions.
- Unauthorized removal or installation of hardware or software on government owned informatics devices or electronic networks.

Authorized individuals are prohibited from conducting any of the unlawful or unacceptable activities listed above. Doing so exposes them to disciplinary measures and possible revoking of electronic network access. Furthermore, authorized individuals cannot use government electronic networks to access or download Web sites or files, or send or receive electronic mail messages or other types of communication, that fall into the following categories:

- Documents that incite hatred against identifiable groups contained in personal messages (the *Criminal Code* prohibits incitement of hatred against identifiable groups in public conversations);
- Documents whose main focus is pornography, nudity and sexual acts (however, authorized individuals may access such information for valid work-related purposes, and may visit sites whose main focus is serious discussions of sexual education and sexual orientation issues).

The OIC expects authorized users to refrain from practices which would not bear public scrutiny or might otherwise bring disrepute on the OIC. Should users be uncertain as to whether a proposed use is acceptable or not, they should consult with their manager. IT Officers and Human Resources (HR) personnel can provide guidance.

For more information, consult the TB Policy on Use of Electronic Networks, Appendix A.

Monitoring

In addition to direct supervision, the OIC routinely monitors electronic networks to ensure their efficient operation, to isolate and resolve problems, and to assess compliance with policies and standards. Periodic and random checks may be conducted for specific operational purposes.

This routine operational monitoring does not normally involve reading files or targeting authorized users. However, if, in the course of operational monitoring or by other means, there appears to be grounds to suspect illegal or unacceptable activity - such as access to unacceptable Internet sites - a security incident review may be undertaken by the OIC. This could involve specialized monitoring and/or the reading of the contents of user's electronic mail and files without notice.

Users should be aware that external networks may also monitor their activities, and may not subscribe to the same high standards concerning disclosure of personal information. Users should also be aware that the OIC routinely monitors electronic networks for intrusion detection purposes.

High Volume Usage Monitoring

To ensure that unusually high personal usage does not degrade network resources, designated representatives may request on a daily, monthly or quarterly basis, a listing of individual accounts demonstrating an unusually high volume use of the Internet. These designated representatives will then solicit an explanation through the appropriate management channels for the high volume use. In cases where usage is business-related, a list for those high volume users will be compiled for future reference. If not business-related, the user's manager will undertake the necessary corrective action in consultation with HR, if required.

OIC Logon Banner

To remind authorized users of their obligation to use computerized resources professionally, ethically and lawfully, an "on-line" banner will periodically display key aspects of OIC's policy as part of the logon process to the network. Authorized users must specifically acknowledge using the "Enter" key to complete the logon process.

Expectation of Privacy

Authorized users are reminded that, while the OIC makes efforts to protect personal and private information that it officially gathers, IT equipment and systems are assigned to individuals for authorized use only, and that any personal or private information will be stored there at the employee's own risk. Users are reminded that OIC networks are monitored for operation and high volume Internet use and that organizational monitoring activities apply to any files stored on OIC facilities or media. For example, if an individual is under investigation for unauthorized or prohibited use of electronic networks, certain emails and their attachments may be read by management, HR and designated OIC security personnel.

Users should be aware that activities they conduct on Internet sites, chat groups, etc., accessed from organizational networks, may be read and reported on by the public or the press. The OIC expects authorized users to adhere to government and organizational policy and to exercise mature judgment in using such facilities.

Disciplinary Measures

The OIC recognizes that many cases of inappropriate use result from unintended errors rather than deliberate acts of misconduct. However, employees should be aware that disciplinary action may be taken where there is evidence of misuse or failure to exercise due diligence. Disciplinary action is progressive in application, and can range from an oral or written reprimand to suspension or termination of employment, depending on the severity of the infraction.

Reporting of Criminal Activities

All authorized users, whether OIC employees or contractors, must act in a timely manner to prevent, report and respond to suspected violations and breaches of IT security. With the advice of OIC HR and Security, suspected illegal activity will be reported to law enforcement agencies.

ROLES AND RESPONSIBILITIES

Responsibility for the effective and acceptable use of IT and electronic networks rests with authorized users, managers, and OIC officials who are designated to undertake specific tasks under this policy. The following sections outline the responsibilities of these three groups.

Authorized Users' Responsibilities

Authorized users have an obligation to use IT and electronic networks in an informed and responsible manner conforming to network customs and courtesies. Users are responsible for complying with the policies, guidelines and standards, as set out by Treasury board and OIC. Each user should:

- **be informed**
  Maintain a level of competency consistent with his/her duties and the technologies employed, and an awareness of governing policies and practices. Take advantage of learning opportunities such as employee orientation and awareness sessions, formal in-house and external training courses, the OIC lntranet and learning centre facilities.

- **comply with the terms of access**
  Use IT resources in support of job functions and approved activities and in accordance with conditions set by management. Such conditions may restrict changes to equipment configurations, and establish responsibilities for local virus detection, backups, and secure storage of diskettes and other removable media. Users must seek direction from managers and informatics support personnel when there is doubt as to whether a proposed action or use is acceptable.

- **use IT resources prudently**
  Be self-regulating. Manage online activities to reduce the burden on servers and telecommunication facilities, especially during core hours. When possible, schedule activities to avoid peak system loads. Respect copyrights and license agreements.

- **protect the OIC's image and property**
  Be aware that some networks such as the Internet may identify the individual and OIC as the source of the communication. Take precautions to ensure that personal views are not misconstrued as official OIC positions, and that actions do not adversely reflect on the OIC. OIC information and technology must not be used for personal gain.

- **be security conscious**
  Take all necessary measures to ensure the integrity and security of OIC information, technology and networks. These measures include protecting user identifications and passwords, and controlling access to and use of facilities to prevent unauthorized use. Report security incidents to your manager or IT Security Officer.

- **Personal Accounts**
  User accounts should not be shared as a method of sharing data. If shared data is required (such as a calendar, email etc) then the helpdesk should be contacted to arrange such access. If this it not technologically practical then an exception will be granted.

Managers' Responsibilities

As part of their normal managerial responsibilities, OIC managers and supervisors are responsible and accountable for the safeguarding and effective use of OIC assets. This includes IM/IT resources and the use of electronic networks. They are also responsible for informing employees and contractors of this OIC policy. Each manager should:

- **maintain a sound IT working environment**
  Assess ongoing requirements for IT and electronic networks, and ensure these resources are used effectively in support of business goals, and consistent with OIC practices concerning security and information management. Inform staff and potential users of electronic networks of governing policies, procedures and standards. Encourage staff to develop expertise relevant to their duties and to take advantage of available professional development opportunities.

- **regulate access to electronic networks**
  Authorize users to access electronic networks on the basis of their business functions, security clearance, technical proficiency, and inform them of their obligation to abide by this policy and other terms and conditions of access. In particular, ensure that each authorized

user is aware of limitations on personal use, monitoring, and expectation of privacy. Cancel authorizations when employees or contractors leave the employ of the OIC, or no longer require network access.

- **promote best practices and discourage inappropriate use**
  Act promptly to correct inappropriate activities. Intervention may include counseling, training and learning opportunities. Report security incidents and suspected inappropriate use, and take disciplinary action where appropriate.

- **be security conscious**
  Take reasonable measures to ensure that use of OIC networks falls within the constraints of OIC security policies. Be aware that the OIC network is operated to secure information at the Protected "A", Protected "B" and Protected "C" mode and that information at a higher security level cannot be transmitted, stored or processed without additional safeguards.

Designated OIC Officials

All of OIC's officials are responsible and accountable for ensuring that IT resources and electronic networks are used effectively in support of business objectives in an environment that discourages uninformed and unacceptable practices.

To support these goals, the *Assistant Information Commissioner, Policy, Communications and Operations* has delegated OIC authority primarily to:

o *The Director, Information Management* is responsible, through consultation and the IM/IT governance process, for promoting the effective use of OIC information technology and electronic networks, and for IM/IT services in support of a reliable and secure environment.

- The *Manager, IM/IT*, is responsible for supporting training programs which ensure that staff is knowledgeable in the use of technology. As part of regular supervisory activities, will also monitor the use of information and technology to ensure that these resources are used productively, effectively and acceptably for business purposes. Upon discovery of policy infractions, will notify the employee's manager.

Specific functional authorities to implement this policy are delegated across the organization as noted in the following subsections.

Network Administration

The OIC's Manager of Information Management/Information Technology (IM/IT) is responsible for day-to-day management of OIC networks, and provides services based on the manager's authorization to allow authorized users access to specific IT resources for specific purposes. The IM/IT manager routinely monitors network operations at three levels:

- **workstation**
  Each workstation is uniquely identified, and configured with hardware and software to meet the user's requirements. Workstation integrity is monitored through logon verification and virus checks, logon banner, user census requests, automated scans of installed hardware and software, and physical examinations for service and inventory purposes.

- **network**
  OIC networks include a large number of Local Area Networks (LANs), which are primarily monitored for overall operational performance, capacity management, and exception reporting purposes. Logs can be used to identify workstations associated with specific activities such as unusually heavy traffic volumes or security violations.

- **firewall**
  Firewalls provide a secure gateway or interface to external electronic networks such as the Internet. Monitoring usually includes logging all transactions by originating workstation and destination. Automated software can be used to provide detailed and aggregate information including sites visited, the number and duration of visits, files transferred, and e-mails sent and received. Automated filtering tools can be used to block or filter access to some sites, and adjust service levels and priorities.

IT Security

The *Manager, Information Management/Information Technology (IM/IT)* is responsible for developing the OIC Information Technology Security Program. This includes conducting IT Threat and Risk Assessments related to potential misuse of electronic networks, designing security programs to reduce these risks, and conducting non-criminal security investigations of suspected infractions.

The *Manager, IM/IT* provides functional direction and training to users, and supports managers and authorized users of IT and electronic networks by providing advice and assistance concerning acceptable use, and through security awareness programs.

The *Manager, IM/IT* is authorized to review security incidents related to inappropriate use under procedures established by the Director, Information Management and the Manager, IM/IT.

Human Resources

The *Director of Human Resources* supports managers and employees by providing advice and assistance concerning acceptable use and staff relations practices. The *Director of Human Resources* may participate in security incident reviews related to inappropriate use. This may include consultation with the Director, Information Management, Security officials and Legal Counsel.

Privacy Coordinator

The Director, Information Management advises OIC officials on policies and procedures to ensure that personal information about users is properly protected, appropriately collected, retained and disposed.

Audit

The Director Information Management is responsible for conducting periodic audits of the OIC's compliance with this policy and the effectiveness of its implementation.

REFERENCES

Relevant legislation:

Access to Information Act;
Canadian Charter of Rights and Freedoms;
Canadian Human Rights Act;
Copyright Act;

Criminal Code;
Crown Liability and Proceedings Act;
Export and Import Permits Act;
Financial Administration Act;
National Archives of Canada Act;
Security of Information Act;
Patent Act;
Privacy Act;
Trademarks Act.

Treasury Board Publications:

Access to Information Policy;
Conflict of Interest and Post-Employment Code for the Public Service;
Communications Policy of the Government of Canada;
Government of Canada Internet Guide;
Government Security Policy;
Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown;
Policy on the Management of Government Information;
Policy on the Prevention and Resolution of Harassment in the Workplace;
Policy on the Use of Electronic Networks;
Regulations - Privacy and Data Protection;
Telework Policy;

Other Publication:

Technical Security Standard for Implementation Technology (TSSIT), Royal Canadian Mounted Police.

DEFINITIONS

Access means gaining entry to an electronic network that the OIC has provided to authorize users. Access to such networks may be from inside or outside OIC premises. Access may support telework and remote access situations or where authorized individuals are using electronic networks provided by the OIC on their own time for personal use.

Authorized users include employees of the OIC as well as contractors and other persons who have been authorized by the Commissioner to access electronic networks.

Electronic networks are groups of computers and computer systems that can communicate with each other. Without restricting the generality of the foregoing, these networks include the Internet, networks internal to OIC and public and private networks external to OIC.

Employee is a person employed in OIC on an indeterminate, specified period (term), casual or seasonal basis; a person employed under a Student Employment Program or a person employed under the Part-time Exclusion Approval Order (persons not required to work more than half of the normal prescribed hours of work). Employees are not considered to be persons hired to provide services under contract, such as temporary help contracts.

Monitoring of electronic networks means any action that involves the recording and subsequent analysis of activity on, or use of, a system or electronic network. Examples include recording user accounts, user activities, sites visited, information downloaded and computer resources used to perform a routine analysis of traffic flow on networks, use patterns and sites that certain work groups or individuals have visited. The information recorded and subjected to analysis does not normally involve the contents of user's electronic mail, files and transmissions.

Security incidents include breaches and violations of security. Breaches occur when sensitive information has been compromised, or when the availability or integrity of information or information technology services has been degraded. Violations are acts or omissions that contravene any provision of the OIC security policies and standards.

Unacceptable or inappropriate activity is any activity that violates OIC or Treasury Board policy, or that violates the limitations on personal use set out in this policy.

Unlawful activity includes criminal offences, contraventions of non-criminal regulatory federal and provincial statutes, and actions that make an authorized user or an institution liable to a civil lawsuit.

Annex E – RDIMS Metadata

The following metadata is captured when profiling and saving an electronic document or other information object in the RDIMS repository.

Metadata	Description
Access Control (check box) Edit (button)	The access controls assigned to the electronic document. Different types of access can be provided to individual RDIMS users or to groups of users. The pre-established types of access that can be selected are: • *View Profile*: Users may view the profile information, but not the document. • *Edit Profile*: Users may edit the document profile but not the document. • *View Document*: Users may view the document in a viewer; they may also view the profile. No edit rights are given. • *Retrieve Document*: Users may retrieve the document in its native application (i.e., the application the document was created in). They may also view the profile. Any edits made must be saved as a new document. • *Edit Content*: Users may edit the document, save as a new version, or save as a new document. • *Copy*: Users may retrieve a copy of the document and save it as a new document. Editing the original document or the profile is not allowed. • *Control Access*: Users with this right may control access to the document (i.e., change the rights of any user/group except their own account). **This is a mandatory field**.
Annual Report Interest	A check box to indicate if the electronic document is of interest for the OIC Annual Report: on to indicate *yes*; off to indicate *no*.
Annual Report Rationale	A free-form text field to provide a reason the document is of interest for the Annual Report.
Application	The software application used to create the electronic document. This field is automatically captured by the system.
Author	The RDIMS user that profiled and saved the electronic document within the RDIMS repository. This is usually the author of the document but can also be the person profiling a document received from outside the OIC. The values in this field are selected from a pre-established list. **This is a mandatory field.**
CCM+ Number	A reference number from the CCM+ application which is a correspondence control system used in the OIC. This is a free-form field.
Creation Date	The date the electronic document was profiled and saved in RDIMS. **This is a mandatory field.**

Metadata	Description
Date Made Record	The date the electronic document was set as a final and official record.
Description	Additional information to further describe the electronic document. This is a free-form text field.
Document Name	The name of the electronic document. This is free-form text field. **This field is mandatory.**
Document Process	The stage of the document within its life-cycle. For example, work in progress, final, ?? The values in this field are selected from a pre-established list.
Document Type	The general type of document based on the OIC organization or function. The values in this field are selected from a pre-established list.
File Number	The number within the file classification structure that the electronic document is filed to. The values in this field are selected from a pre-established list.
Category	The category of the investigation file.
File	The file series within the file classification structure.
File Browser	The employee a paper file is checked-out to.
Location	The physical location of the paper file.
File State	Indicator that the file is open or closed. The values in this field are selected from a pre-established list.
Last Edited By	The RDIMS user that last edited the electronic documents.
Last Edited Date	The date the electronic document was last edited.
Management Issue	*Not used.*
Secured Document (check box)	A check box to indicate if the electronic document is security sensitive: on to indicate *yes*; off to indicate *no*.
Security level	The security level of the electronic document based on the Government of Canada standard for designated and classified levels. • Protected A • Protected B • Protected C • Confidential • Secret • Top Secret The values in this field are selected from a pre-established list.

Annex – F - IM Central Protocol – Requesting Files from the Records Centre

How to Request a File

1. Email “Access IM Central (Records)” stating:
    a. File number(s) or File Name according to File Plan or Subject*
    b. Your name
    c. Your Location (i.e. Room/Cubicle 2204)
    d. Date required for receipt of the files

2. Provide subject, date, or other details that will assist in locating files for non-investigation files that pre-date the File Plans (2010).

3. You may come in person to the Records Centre and request a file. If possible, Records staff will retrieve and check the file(s) out to you while you wait.

Note: If you are requesting files for another person, please indicate the name of the person to whom the files are to be checked out.

Information to Include in your Request

- For **Investigation Files**:
    - Investigation File Number(s)
    - Number of volumes (if known)
    - Accompanying material, such as wallets, red files, etc., if required

- For **Non-Investigation Files** (i.e. Administrative Files), please include:
    - Complete File Name, taken from the approved File Plan in the IM Manual and RDIMS, for example:
        - Human Resources – Classification – Work Descriptions – LS03

Getting the File(s)

Records Centre staff will contact you when the file(s) have been retrieved and, depending on your instructions, will deliver the file to your office or have it ready for you to pick up. They will also advise you if the file you are requesting is checked out to someone else.

Information Security

Records Office staff will verify the security level of requesters asking for files that are classified above Protected B. Files are placed in a secured pouch or closed container for delivery. **See:** Annex B in the Information Management Manual, RDIMS#177901.

Service Turnaround Time

As a rule, Records Centre staff will contact you or deliver the file to you within 3 hours of reading your email or receiving your telephone call. Urgent requests for files will be dealt without delay.

Annex - G - IM Central Protocol Submitting / Returning Files to the Records Centre

1. Closed Investigation Files

- Administrative assistants will affix the IIA "File Label - Investigation" on the upper left corner of each volume of the investigation file when it is closed. Investigators will fill out the label indicating the number of volumes for each type of file: investigation files, red files and wallets.
- Security classification of files and documents must be clearly marked on the file jacket and/or documents.
- Designated individuals should bring the complete file, including Red Files, to the Records Centre **AND** change the File Location to "Transition to Records" in IIA/InTrac.
- Transport files in a blue pouch or other container appropriate to the file's security classification.

2. Non-Investigation Files

- Files must be properly labeled using the approved File Plans from the IM Manual and in RDIMS.
- Files must be sorted and labeled before submitting them to the Records Centre. Boxes filled with unlabeled files will not be accepted.

Departing Employees

- Departing employees are responsible for returning their files to the Records Centre.
- If a file is being transferred to another employee, managers must ensure that the File Location field is updated in the Case Management System.
- Managers are responsible for ensuring that any files that are submitted to the Records Centre are complete and labeled correctly.
- OIC Library material must be returned to the Library.

See: "Managing Records When an Employee Leaves", Information Management Manual, Annex C (RDIMS #177901)

Information Security

Files and documents must be properly classified and the classification level must be clearly marked on the front of File Folder and on the documents contained therein.
Files must be placed in a secured pouch or closed container for delivery to the Records Centre as appropriate to its security classification.
See: "Managing Sensitive Records", Information Management Manual, Annex B (RDIMS#177901)

We Can Help

We are here to help, so feel free to send an email to "Access IM Central (Records)" or come and see us in the Records Centre on the 4th Floor.