INFORMATION MANAGEMENT TOOL KIT

FOR

FIRST NATIONS GOVERNMENT IN BRITISH COLUMBIA

2010

Volume 1 – For the Executive Director/Band Administrator/Senior Administrator

Prepared by
Alexandra E. Bradley, CRM
Harwood Information Associates Limited

Cataloguing In Publication Data

DISCLAIMER

The contents of this publication are for general information purposes only for First Nations organizations and are not intended to provide legal advice or opinion of any kind. The contents of this publication should not be relied upon. No lawyer-client or other relationship is created by using the contents of this publication. The contents of this publication should not be seen as a substitute for obtaining competent legal counsel or advice or other professional advice. If legal advice or counsel or other professional advice is required, the services of a competent professional person should be sought. While the First Nations Public Service has made reasonable efforts to ensure that the contents of this publication are accurate, the First Nations Public Service does not warrant or guarantee the accuracy, currency or completeness of the contents of this publication. The First Nations Public Service expressly disclaims all representations, warranties, conditions and endorsements. In no event shall the First Nations Public Service, its directors, agents, consultants or employees be liable for any loss, damages or costs whatsoever, including (without limiting the generality of the foregoing) any direct, indirect, punitive, special, exemplary or consequential damages arising from, or in connection to, any use of any of the contents of this publication.

First Nations Public Service of British Columbia
Information Management Toolkit

Table of Contents
Volume 1

Table Of Contents

Table Of Contents

1. Introduction to Recorded Information Management in British Columbia First Nations Governments

The purpose of this tool kit is to provide general records and information guidance to staff in the various First Nations government organizations in the province of British Columbia (BC).

In most First Nations government organizations in BC, the person responsible for recorded information management (RIM) will be the Chief Administrative Officer. Recorded information management will be one of many responsibilities for this individual. Therefore, while the professional literature of records and information management contains much more detailed information on every aspect of the management of recorded information, this publication provides basic principles and fundamental operating processes, based on industry standards and best practices. It is written as a practical handbook enabling the manager to read selectively about aspects of records management, and then follow up, if required, through the lists of references to additional information that are included in the Appendices. The manual also includes the basic records management instruments including a records classification and retention schedule, a model bylaw, as well as samples of forms and practical tips for all aspects of records management.

In addition, the Tool Kit includes Volume 2, with daily record keeping procedures and routines designed for the staff person who is designated to manage records. This includes information management procedures for mail management, file opening and closing, records storage and approved disposal or archival preservation of records. There is also a model classification and retention schedule (included as Appendix 1 and 2) that is based on the typical functions or portfolios present in First Nations organizations. The retention requirements have been reviewed and updated current to December 2009. The standards-based approach reflects the International Standards Organization (ISO) *ISO 15489 Information and Documentation – Records Management – Part 1 General*[1]*, and Part 2 – Guidelines.*[2] It also reflects the Canadian General Standards Board *CAN/CGSB – 72.34-2005 Electronic Records as Documentary Evidence,*[3] released in December, 2005.

Records are produced and maintained in diverse formats. In this complex environment, a variety of housekeeping approaches are required. Most importantly, all employees have a records management role to play. These requirements are outlined in detail in the following chapters.

[1] International Standards Organization (ISO), *Information and Documentation – Records Management – Part 1: General* (ISO/15489-1), First Edition, (Geneva, Switzerland: ISO, 2001, http://www.iso.org), (ISO/15489-1).
[2] ISO, *Information and Documentation – Records Management – Part 2: Guidelines* (ISO/TR15489-2), (Geneva, Switzerland: ISO, 2001, http://www.iso.org), (ISO/TR15489-2).
[3] Canadian General Standards Board, *Electronic Records as Documentary Evidence*, CAN/CGSB-72.34, (Ottawa: Canadian General Standards Board, 2005, http://www.techstreet.com), (CAN/CGSB-72.34).

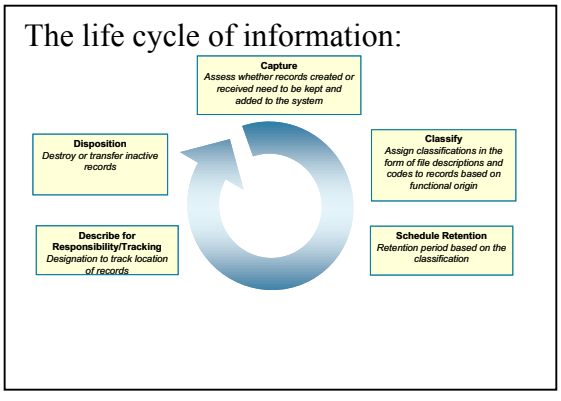
Acknowledgements

The authors would like to thank the advice and assistance of the members of the Records Management Manual Advisory Committee (INSERT acknowledgements here).

1. 2 Recorded Information Management Defined

In today's organizations, information is at the centre of all business functions, whether it be required for decision making, strategic planning, regulatory compliance or future reference. First Nations governments have a duty to create, receive and use records as a normal part of conducting business. How governments manage information can directly affect their ability to operate efficiently and with full knowledge of past precedents and future requirements. With the ongoing requirement for information access, First Nations governments must be certain that information created today will be available over time and into the future, for as long as the information is required. Herein lies the greatest challenge for record keeping!

Recorded information management is defined as "the systematic control of records throughout their life cycle" by ARMA International. ARMA International is the professional association of records and information managers.[4] The ISO standard earlier cited expands on the concept of life cycle management to include the "field of management responsible for the efficient and 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."[5]



[4] ARMA International, *"What is Records Management? Why Should I Care?"* (Lenexa, KS: ARMA International, 2005).
[5] ISO/15489-1, p. 3 and subsequently incorporated into CAN/CGSB-72.34, p. 12.

The records management discipline is now often referred to as "recorded information management" or RIM, in recognition of the fact that records come in many formats, ranging from the conventional physical formats such as paper, drawings, photographs, to the more recent digital formats such as electronic documents, spreadsheets and databases, graphical materials and web content. This RIM terminology helps to dispel the perception that staff may hold when they hear the term "record" as referring only to the paper record in a centralized collection.

Records management in a local government organization typically includes:

- Setting policies and standards;
- Assigning responsibilities and authorities;
- Establishing and promulgating procedures and guidelines;
- Providing a range of services relating to the management and use of records;
- Designing, implementing and administering specialized systems for managing records; and
- Integrating records management into business systems and processes.[6]

A systematic approach to the management of records is essential for organizations and society to protect and preserve records as evidence of transactions. A records management system results in a source of information and business activities that can support subsequent activities and business decisions, as well as ensuring accountability to present and future stakeholders.[7]

1. 3 Understanding What is a "Record"

A clear understanding of what we mean by the term "record" is one of the foundations for program development and implementation. The records management standards define a record as "information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business."[8]

Although this is the accepted records management definition of a record, First Nations are subject to federal and provincial legislation, depending on particular programs and circumstances.

Within the Federal sphere, public organizations must comply with legislative definitions of "record", including the following from the *Personal Information Protection and Electronic Documents Act [2000, c. 5].* In section 2(1):

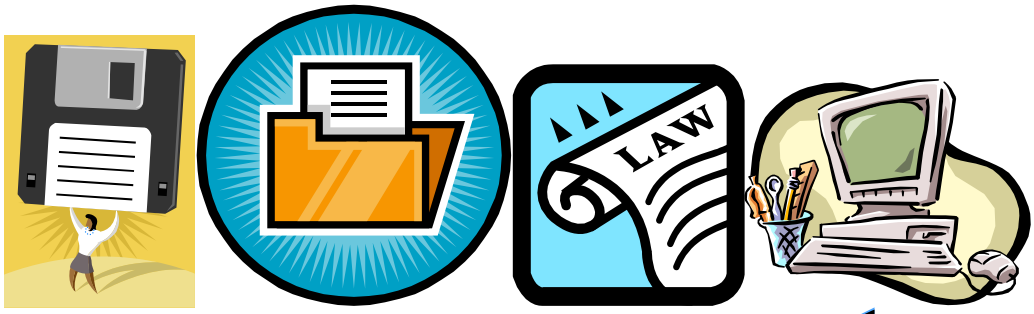
[6] ISO/15489-1, p. 4, Section 4 Benefits of records management.
[7] *Ibid*.
[8] ISO/15489 -1, p. 3, and subsequently incorporated into CAN/CGSB-72.34-2005, p. 12.

> "Record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

Public organizations in British Columbia must comply with various legislative definitions of "record", including *FOIPPA*. *FOIPPA* embeds a broader definition. This broader definition is derived from section 29 of the *Interpretation Act.* Section *29* defines "record" this way:

> "record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise;[9]

Thus, one of the key records management issues for First Nations governments is that, technically, everything is a record. Records have varying values to organizations, and most staff are able to discern between records of passing or transitory value, and records of substantive or business value. RIM programs within First Nations government should assist their organizations with policy development and processes to enable staff to quickly choose between the substantive and the transitory information.



A "record" should exhibit the following characteristics:

- A record should correctly reflect what was communicated or decided or what action was taken, and should be able to support the needs of the business;

[9] R.S.B.C. 1996, c. 238.

- **Authenticity of a Record** – a record can be proven to be what a record purports to be; to have been created or sent by the person purported to have created or sent it, and at the time purported;
- **Reliability of a Record** – a record can be trusted as a full and accurate representation of the transactions, activities or facts, and can be depended upon in course of subsequent transactions;
- **Integrity of a Record** – a record is complete and unaltered;
- **Useability of a Record** – a record can be located, retrieved, presented and interpreted.[10]

Substantive records will exhibit these characteristics. This is contrasted with transitory records. Transitory records are "required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record."[11] Transitory records include the copies, duplicates in form, drafts and notices, advertisements and other items that have no ongoing informational value to the staff and should not require staff resources or expenditure of funds for processing and storage. Additional information relating to transitory records is included in Appendix B of this manual.

1.4 Why is Records Management Important?

Records management is often undervalued in organizations and misunderstood as simply "filing." In practice, records management serves a vital administrative function by providing the right information to the right people at the right time, in the right medium, and at the lowest possible cost to the organization.

Many Canadian and international standards have established the requirements to manage recorded information in organizations. These requirements impose legal and legislative obligations on organizations.

First Nations governing bodies in British Columbia are required to manage their recorded information in ways that promote transparency and openness and must make records accessible to the public in accordance with policies and legislation. The federal legislation includes: the *Indian Act*, *Human Rights Act,* the *Privacy Act,* the *First Nations Jurisdiction Over Education in British Columbia Act*, and a number of other acts and regulations. Corresponding Provincial legislation includes the *School Act,* FOIPPA, and , to name a few. Underlying such legislation is

[10] ISO/15489-1, Section 7.2 Characteristics of a record, p. 7.
[11] CAN/CGSB-72.34, p. 13.

an expectation that First Nations governments have an established recorded information management program.

Not only are records by-products of conducting business and are essential for the continuation of business, they can single-handedly protect an organization in litigation. A failure of records management can also condemn an organization caught in litigation.

1.4.1 Chain of Evidence

In the legal realm, records created by First Nations governments are considered documentary evidence. Generally speaking, in order for records to be admitted into courts as documentary evidence, the records must be made in the usual and ordinary course of business in order to qualify as an exception to the rule that makes hearsay inadmissible in court and other legal proceedings. Various standards have been created to ensure organizational records are admissible in court.

In First Nations governments in British Columbia, all documents created or received are records that can become evidence in courts of law, used for government investigations, or used in other legal proceedings. In order for records to be used as evidence, they must be created in the following five ways:

1. The following records created by First Nations organizations in the usual and ordinary course of business may become evidence: office paper and electronic records from the corporate records management system, records contained in document management systems, records held in databases and records in Internet applications like web pages or electronic-business transaction software.

2. The policies and procedures created by First Nations governments to meet business requirements and to comply with best practices for RIM.

3. Records created by First Nations governments to comply with international and national records management and information standards. The International Standards Organization standards for records management are an example of international standards.[12] An example of a national standard is the Canadian General Standards Board standard, *Microfilm and Electronic Images as Documentary Evidence*.[13]

[12] ISO/15489-1 and ISO/TR15489-2.
[13] CAN/CGSB-72.11-93, (Ottawa: Canadian General Standards Board, 2000, http://www.techstreet.com) (CAN/CGSB-72.11-93).

4. Records created by First Nations governments to comply with information technology requirements and standards.

5. Records created by First Nations governments proving compliance with applicable provincial and federal legislation or court rulings.

These five ways combine to make records admissible as evidence. These five ways also work as a process. One way to think of this process is that it operates as a chain of evidence. A chain of evidence is the documentation or available testimony from persons knowledgeable in the organization that proves that the evidence, from the time it has been created to the time it is introduced as evidence in court, has not been altered or tampered with in any way. Each of these five ways is a separate link in this chain of evidence.

The chain of evidence is only as strong as the weakest link in the chain. If the chain of evidence is strong, then the records are likely to be admitted into court as evidence. For example, if a First Nation government faces legal proceedings where a claim is made that the First Nations government illegally destroyed records, the First Nations government needs to prove that it destroyed records in the usual and ordinary course of business, following applicable laws and its own records management practices. The First Nations government will need to prove that:

1. Its records management system captured all relevant records (be they paper records or records from its document management system or its Internet applications), that it had a records retention policy outlining when and how records were to be destroyed, and that the records were destroyed according to its records retention policy;
2. It followed its own records disposal policies and procedures and that it complied with best practices for records destruction;
3. It complied with any specified international and national records management and information standards governing records disposal that it adopted for use;
4. It complied with applicable information technology requirements and standards governing destruction of electronic records; and
5. It complied with applicable provincial and federal freedom of information legislation or other law that regulated destruction of records.

If any one of these five elements of proof is lacking, then the chain of evidence is weak and the First Nations government may then face fines or court judgments against it. Records that a First

Nations government may need to be admitted into evidence may not be admitted, to the detriment of the First Nations government.

How to prove that these five ways of evidence-creation operate as a chain of evidence is through the use of a unifying standard. Since First Nations governments are generally increasing their use of electronic records, the unifying standard must provide for the admissibility of electronic records into evidence. *Electronic Records as Documentary Evidence* is an example of such a unifying standard.[14]

First Nations governments can follow this *Electronic Records as Documentary Evidence* standard in order to prove the chain of evidence to have their records admitted into courts and other legal proceedings as evidence. This standard sets out the policies, practices and documentation required for organizations to use in order to prove the integrity and authenticity of their electronic records. First Nations governments can use this standard to lessen the risk of government investigation and litigation. First Nations governments can also use this standard to increase their effectiveness in producing electronic records and increasing the likelihood that their electronic and paper records will be admitted as evidence in courts of law or other legal proceedings.

1.5 Business Case for Recorded Information Management

RIM programs are based on developing and adopting policies, procedures and practices. RIM programs are designed and implemented to meet the operational needs and regulatory requirements of the First Nations government.

Records systems should have the following characteristics:

- **Reliability** – capable of continuous and regular operation in accordance with procedures that are documented and maintained as proof to:
    - Routinely capture all records within the scope of the business activities they cover;
    - Organize the records in a way that reflects the business processes of the records' creator;
    - Protect the records from unauthorized alteration or disposition;
    - Routinely function as the primary source of information about actions that are documented in the records; and
    - Provide ready access to all relevant records and related metadata**;**

[14] CAN/CGSB-72.34.

- **Integrity**, including control measures such as access monitoring, user verification, authorized destruction and security, to prevent unauthorized access, destruction, alteration or removal of records;
- **Compliance**, in accordance with all business requirements, regulatory environment and community expectations, and subject to regular assessment of such compliance;
- **Comprehensiveness**, covering the complete range of business functions;
- **Systematic,** ensuring that records are created, maintained and managed systematically, through the design and operation of the records and business systems, and with accurately documented policies, assigned responsibilities and formal methodologies.[15]

RIM programs are not only about organizational efficiency, but also about risk management and demonstrating compliance. Risks to First Nations government may be defined individually by staff, but can include:

- Catastrophic loss of vital information through natural or man-made disasters;
- Unnecessary legal or other costs incurred through lost or inadmissible information;
- Breaches of privacy or confidentiality that result in claims or costs;
- Redundant labour costs expended to recreate lost information; and
- Loss of credibility or embarrassment through information mismanagement.

1.5.1 Teamwork among Administration, Finance, Records Managers, IT, and Legal Advisors

The business owner of the records management program in First Nations government, as stated or implied in statutes, is the Chief Administrative Officer. Under administrative oversight, three groups have knowledge and skills that contribute to an effective records management program:

- the records managers provide the technical knowledge of RIM industry best practices;
- the information technology ("IT") managers provide the technical infrastructure support, including the operating support of the various applications creating records; and
- the legal advisors support the risk and legal requirements of the First Nations government.

A team effort is now required among First Nations government staff. Team effort is now required because new media and the regulatory environment bring together issues that are of common interest to the administration, records management specialists, information technology staff and legal advisors.

[15] ISO/15489- 1, Section 8.2 Records system characteristics, pp. 8-9.

The new reality is that all three sets of expertise are required. Each one of these groups has a perspective and body of knowledge essential to the success of any RIM program. This success is achieved most effectively when there is communication and cooperation among all of these groups to ensure overall program functionality.

1. 6 Required Program Components

Until recently, most work in records management was based on practical experience and shared understanding. Today, the foundation for program requirements is defined in various international and Canadian standards. These program requirements include adequate policies and processes to assert control over the records as they progress through the life cycle. The ISO and Canadian standards define basic instruments of records management to include records classification, disposition authority and security and access evaluations. All RIM programs should begin with the development of policies and a solid records classification and retention schedule.

To assist First Nations governments, these instruments are provided as appendices to this Tool Kit, in the model bylaws as the overall program policy, and the records classification and retention schedule. All other components of a First Nations government's RIM program should be developed as time permits and as funds are available.

1.6.1 Standards Defining Program Design and Operation

Throughout this manual, there are references to two sets of standards that have recently been produced and provide the foundation for the work included here. Purchasing information for these standards is provided in Appendix E of this manual.

One of these standards is the ISO 15489-1 *Information and Documentation – Records Management – Part 1: General.* This standard is described as the "main and overarching standard for records management, providing an excellent framework and broad view of the principles and core issues".[16] The ISO/TR15489-2 *Information and Documentation – Records Management – Part 2: Guidelines* is the companion technical report to Part 1. The ISO/TR15489-2 standard shows how to achieve a successful program implementation.

At the same time, a Canadian project, begun under the Uniform Law Conference of Canada, has resulted in the publication in December, 2005 of CAN/CSGB-72.34-2005 *Electronic Records as Documentary Evidence.* This standard specifies principles and procedures for creating all forms of electronic records and to enhance their admissibility as evidence in legal proceedings.

[16] Hans Hofman, "Standards: Not 'One Size Fits All'," *Information Management Journal,* May-June, 2006: 40.

We will refer to these two sets of standards throughout the Tool Kit.

1. 7 Support and Resources

Like the corresponding issues in accounting, human resources, law and other business operations, record keeping issues are best handled by experienced professionals. Recorded information management programs require designated staff to be responsible for the overall program operation as well as the technical components. Where First Nations governments do not have dedicated records management staff, a designated staff member should be supported to develop competence, skills and knowledge in this discipline.

At minimum, the executive support must be provided by one designated manager. In addition, user group leadership can also be delegated to individual support staff or user group coordinators.

1.7.1 Personnel Competencies of Records Staff

Recorded information management is a specialized field of information management that is concerned with the systematic analysis and control of records associated with business activities.[17]

The practice of records management is an area of specialization, requiring a specific blend of education, knowledge, skills and aptitudes. Six domains of specific competency and four levels of experience have been identified by ARMA and are described as follows:

- Technical Recorded information management, including the knowledge and skills required to systematically manage records and information from creation or receipt through processing, distribution, organization, storage and retrieval, and ultimate disposition.
- General management, including knowledge and skills necessary to administer, implement, or maintain the program, including the supervision of RIM staff, budgeting, providing customer service, providing input to management, and strategic planning.
- Risk management, including knowledge and skills necessary to mitigate and manage the potential for damage to or loss of records and information.
- Communications and Marketing, including the knowledge and skills necessary to effectively communicate through speech, writing, or behavior and to effectively champion the benefits of a RIM program within an organization.
- Technology competencies, including knowledge and skills necessary to develop, maintain, and use information processing systems, software applications, and supporting hardware and networks for the processing and distribution of data.
- Leadership, including knowledge and skills necessary to motivate groups of people toward the achievement of the RIM program goals within the context of the organization's overall goals. [18]

INSERT Picture: Competency Wheel

As a consequence of this work, positions for records management personnel have moved beyond the three-level traditional ranking of positions (clerk, supervisor, manager) into a lattice of various types of positions. The roles will depend upon the size of the organization and the complexity of the records management program.

---

[17] ARMA International, *Information Management: A Business Imperative – FAQs for Corporate Executives and Decision-Makers*, (Lenexa, KS: ARMA International, 2005), (http://www.arma.org), p.2.
[18] ARMA International, *Records and Information Management Core Competencies* (Lenexa, KS. ARMA International, 2007)

Designated staff will require continuous training and support in their respective RIM roles. At minimum, continuing education activities in the records management profession provide staff with current information on new regulations and requirements for the program operation. At the same time, attendance at trade shows and other technology demonstrations provides staff with opportunities to examine new software and new computer applications, not only for records management use, but also to help determine the overall impact of records on the organization.

1.7.2 Staff Training and Ongoing Support

Everyone in a local government organization has a role to play in a RIM program. The general staff member or "end user" is the key to success of every records management program. No matter what their role in the organization, each staff member will be responsible for creating, receiving and using recorded information in their work. Many of the requirements defined in this manual require specific types of training for all staff in the organization. It is imperative that training be provided to staff in order for them to understand their roles and responsibilities and be able to identify business records. Quality assurance or auditing is also necessary to ensure that staff are following the defined processes.

The importance of staff training and change management cannot be emphasized enough. At minimum, programs for training should encompass the roles and responsibilities of all members of management, employees, contractors, volunteers and other individuals responsible for creating or receiving records during their work.[19]

Clearly, distinct levels of training will provide appropriate levels of detail, according to the responsibilities assigned to personnel. Examples of types of training that may be useful include the following:

- orientation training for new employees, including documentation in appropriate handbooks or literature;
- classroom training for employees with specific responsibilities assigned;
- on-the-job training and coaching;
- briefing sessions and seminars on specific records issues or initiatives;
- publications providing short "how-to" guides on aspects of policies and practices;
- computer based presentations, interactive or static materials on networks and intranet sites;

[19] ISO/15489-1, Section 11 Training, p. 17.

- help text within computer systems; and
- formal training courses in educational institutions or professional organizations.[20]

Staff training ensures that all processes are communicated to staff. Change management ensures that staff understand the reasons for these processes and their benefits to staff, especially if these processes are new or differ significantly from the ways in which staff have managed records in the past.

Be aware that no matter how often staff are told about requirements, they will usually only perform tasks once they understand the importance and can see the value or reward in doing these tasks first-hand.

[20] ISO/TR15489-2, Section 6 Training, p. 23.

2. Program Design and Operation

The information in this chapter is intended to help First Nations governments establish RIM programs.

This chapter also references the model bylaw and key tools of records management operations, the Model Classification and Retention Schedule, and provides tips about how to use these tools. To match the descriptions here, there are detailed procedures and sample materials in Volume 2 of the Information Toolkit, to help the records staff to establish the processes described.

No two organizations will build their RIM programs in the same way. The timing and development of RIM programs depends on the corporate culture, availability of personnel, financial resources and information technology infrastructure.

2.1 Steps in RIM Program Development

When an organization begins a records management program, a design and implementation methodology is essential. The ISO standard and technical paper outlines the following steps to encompass this process:

- a preliminary investigation provides the organization with an understanding of context in which it operates, identifies the major factors influencing the need to create records, and defines problems with records in order to complete risk assessment;
- an analysis of business activity enables the documentation of business processes where records are produced and the development of records management tools such as the classification and disposition authority;
- identification of requirements for records including systematic analysis of business needs, legal and regulatory obligations, as well as an organization's exposure to risk if records are not created and kept;
- an assessment of existing systems will measure the extent to which they capture and maintain records and identify any gaps between the requirements and current practices;
- identification of strategies for satisfying records requirements will identify the appropriate policies, procedures, standards, tools and tactics needed to meet the requirements;
- design of a records system converts the strategies and tactics into a plan that fulfills the records requirements;
- implementation of a record system involves the necessary steps to install the records management elements designed previously, incorporating the appropriate project management and staff training required; and

- post implementation review to measure and evaluate the effectiveness of the system, address deficiencies and maintenance processes.[21]

Information in this manual is based on analysis and understanding of the record – keeping requirements for British Columbia First Nations governments, and is intended to provide a head start for those who are developing or updating their RIM programs.

All RIM programs are always "work in progress", as no program is ever complete or finished. The dynamic nature of local government means that the RIM program will be always responding to organizational program development, new regulations and other factors that affect local government operations.

2.2 Information Survey

Information provided in this manual should be tailored to meet specific local conditions. First Nations governments are encouraged to survey their own collections of records and to evaluate their current record keeping practices in order to obtain a clear picture of the current state of records and management practices and processes. This survey will also enable records management staff to determine how much customization of the information provided in this manual is required.

The information survey or inventory is a tool for collecting data about records. The survey will reveal the nature and extent of current collections, in all formats, and in all locations in government offices. Staff will then have a clear picture of the subjects and functions of records, as well as the mix of formats and the date range and extent of collections.

A sample survey form is provided in Volume 2 as part of information management operations.

2.3 RIM Policy

The purpose of a RIM policy is to define a set of expectations upon staff, and to link the expectations to a series of practices. For RIM programs, the policy ensures that an organization's business need for evidence, accountability and information about its practices are met.

[21] ISO/TR15489-2, Section 3 Strategies, design and implementation, pp. 2-7.

The objective of the RIM policy is the creation and management of authentic, reliable and usable records, capable of supporting business functions and activities for as long as they are required.[22]

Further:

> A RIM policy statement is a statement of intentions. It states what the organization intends to do, and sometimes includes an outline of the programme and procedures that will achieve those intentions…An effective policy statement will … identify a senior member of staff with lead responsibility for records management and for overseeing policy and program implementation. The policy statement… should be supported by procedures and guidelines, planning and strategy statements, disposition authorities and other documents that together make up the records management regime."[23]

The recommendation here is that local governments prepare a records management bylaw to address their records management requirements. The Model Records Management Bylaw is included in this manual as Appendix A for information purposes.

2.4 Model Bylaw Content

The Model Records Management Bylaw is offered as a model bylaw for First Nations governments who choose to use it. Use of this model bylaw is voluntary. This model bylaw is for general information purposes only and is not intended to provide legal advice or opinion of any kind. The law referred to in this model bylaw is current as at the date of this writing. First Nations governments intending to rely on this information, should use the relevant official paper versions of the statutes and regulations. Prior to using this model bylaw, First Nations governments should seek competent legal advice to ensure that the information contained in the model bylaw and relevant law applicable to it are current and applicable to the specific needs of the local government.

An explanation of each provision of the Model Records Management Bylaw is provided in Appendix A.

[22] ISO/15489-1, Section 6 Policy and responsibilities, p. 5.
[23] ISO/TR15489-2, Section 2 Policy and responsibilities, p. 1.

2.5 The Life Cycle of Information

RIM programs are based on the notion that all information has a life cycle and that systematic control is exercised over every phase of the life cycle. This is to ensure the consistent capture, filing and availability of records for business purposes, the systematic and controlled disposal of records once their value to the organization has ceased, and the preservation and continued availability of those records over time that have enduring value to the organization.

For paper records, the sequence of controls and operations can be described in a linear fashion: records are created or received, used, stored, and ultimately destroyed or preserved in perpetuity in an archives. With electronic records, the decisions about capture and classification, access and disposition status may happen at the point of creation of the record. There will be more discussion about electronic records processes in this manual in Chapter 3 – Electronic Records Considerations.

2.6 Information Capture and Registration

Information capture is the process of determining that a record should be made and kept, whether the record is created internally or received from an external source.[24] At this stage, staff decide whether or not it is a business record.

In light of the earlier discussion about what are records in the First Nations government world, the process here requires having business rules that outline to staff what are the requirements for both the substantive and transitory records that staff create or receive. A business rule is an internal rule developed by an organization in order to conduct business. A business rule can often be used to set out a process to accomplish a specific task or used to define a procedure for how business needs to be conducted. Some organizations will refer to these as internal policies and procedures. In this context, a business rule will help staff to identify what information is transitory, and what staff should do to manage transitory records.

Generally, substantive records are identified and placed for filing. Specific locations and devices such as the "in-box" provide staff with defined locations where the records will be collected, then passed on for whatever processes are required to code and put them away into the correct folders or containers. Transitory records are also marked and placed in some sort of controlled physical holder, but generally have little other processing undertaken, because the retention for

[24] ISO/TR15489-2, Section 4.3.2 Capture, p. 14.

these will be for a specified (read short term) period of time. No unnecessary labour is expended if these records have little or no enduring value. There are samples of transitory record types included in Volume 2.

The filing of paper records links documents into a sequence that connects the individual document to other documents and enables contextual information about that document to be inferred by anyone retrieving the information. Moreover:

> This context links the document to others, whether by time, by physical proximity, by ownership of the file or folder, and by the title of the folder. Adding papers to a file becomes a conscious process of determining which classification suits the particular document and deliberately placing it in a predefined and known sequence of documents.[25]

In those systems where formal registration is used, the register provides evidence that a record has been created or captured into a records system. Most registration systems involve assigning a unique identifying code, and recording a description of the record in a register.[26] The tracking of citizens' complaints, letters to Chief and Council, or listing of cheques received into the finance department are examples of processes where formal registration of records takes place. Such registers are usually maintained as separate records.

2.7 Managing Active or Current Records

"Active records" are defined as those records created and received in a business environment during the time the records are needed to conduct and support current business actions.[27] However, because of the long term mandate of local government, some of these "current" projects may depend upon records that are ten, twenty, or thirty-plus years old.

Once captured into a records management system, records must be made available for use by staff to conduct the business of the First Nations government body. In the life cycle model, this phase is called "the period of active use." The records that staff will require are generally those records about the current projects or present activities of the various work groups.

[25] *Ibid*.
[26] *Ibid*., Section 4.3.3 Registration, p. 15.
[27] Ann Bennick, *Active Filing for Business Records,* (Lenexa, KS: ARMA International, 2000), p. 3 (Bennick).

The emphasis in this phase is on the ability to find and retrieve information. Staff efficiency, service to citizens, compliance with law and regulations and any other requirements depend upon an efficient retrieval system.

Components of an effective active records system include the following:

- a standardized file structure, including a file coding or numbering pattern;
- written rules for the file system development;
- up to date printed and/or computer searchable listing of existing file titles;
- identification of appropriate filing supplies;
- identification of appropriate filing equipment for each type of media, including efficient and safe floor layout and design;
- standard procedures for maintaining and updating the system;
- standard procedures for transferring files to inactive storage (physical or logical) after expiration of their usefulness in the active office; and
- written procedure manuals for end users and employees who maintain the file system, and ongoing education and training programs.[28]

The ISO standard describes classification of business activities as a powerful tool to assist in many of the processes involved in the management of records including:

- providing linkages between individual records which accumulate to provide a continuous record of activity;
- ensure records are named in a consistent manner over time;
- assisting in the retrieval of all records relating to a particular function or activity;
- determining security protection and access appropriate for sets of records;
- allocating user permissions for access to, or action on, particular groups of records;
- distributing responsibility for management of particular sets of records
- distributing records for action; and
- determining appropriate retention periods and disposition actions for records.[29]

The ISO Technical Report also describes a classification system that is based on business activities as one of the key instruments for RIM programs.[30] A prime example of a classification

[28] *Ibid.,* p. 7.
[29] ISO/15489-1, Section 9.5 Classification, p. 13.
[30] ISO/TR15489-2, Section 4.2 Instruments, p. 8.

system that is based on First Nations business activities in BC is the Model Classification System, included in Volume 2 as Appendix 1.

2.7.1 Model Classification System (included in Volume 2)

The Model Records Classification and Retention Schedule has been developed to suit the business functions and activities of First Nations government organizations in British Columbia. The mandate for First Nations government and the legal and regulatory environment have been reviewed, and resulting lists of records and draft retention periods match the functions and subjects operated by First Nations agencies.

While there are many primaries in the complete classification system to cover the full spectrum of First Nations government mandates, individual staff members work on specific functions. Typically, staff members will use only a selection of primary headings for identifying and saving the records they receive or generate. It is useful to consider the Records Classification and Retention Schedule as a menu from which to select the "favourite" or common topics associated with staff work. Also, no two First Nations governments will have identical programs and functions. Therefore, each organization should select only the subjects that describe their functions, and add new topics where there may be gaps in the model that do not cover their business requirements.

Staff turnover is a particular challenge for First Nations organizations, as the person who sets up a filing system may not be the person who has to manage the files later on. If everyone follows the model standard filing system provided here, staff will continue to follow the same system, no matter who is filing the documents.

2.7.2 Daily Office Routines

While the classification system and retention schedule will ensure that records are classified in a logical and retrievable manner, there must also be work routines and processes in place that ensure the regular capture, registration and filing of incoming, inter-office and outgoing information.[31]

Most offices operate with decentralized collections of records that are retained in locations close to the staff who most frequently access and use the records. As a result, the various custodians of records will require a common understanding of the business rules established to ensure

[31] Routines, processes and forms samples for management of active records are included in Bennick.

appropriate records controls are in place, once the records are captured and entered into the filing system.

Typically, such controls are necessary to ensure that:

- daily (or frequently) records are put away, filed and stored as required, ensuring that records are captured into systems so that staff can locate and use them;
- confidentiality or privacy requirements are managed. The First Nations government organization should have formal guidelines regulating who is permitted access to records and in what circumstances;[32]
- records locations are known to all staff who require the information. The First Nations government should have processes for tracking the movement and use of records within the records system;[33]
- records are protected from hazards. Storage conditions and processes should be designed to protect records from unauthorized access, loss or destruction, and from theft and disaster.[34]

Designation of records custodians or "offices of primary responsibility" will ensure that staff can manage duplication of information, ensuring that original documents are filed and retained according to retention requirements, and facilitating the routine discarding of duplicate materials.

Equipment standards will enable organizations to maximize storage space and reduce the footprint of storage cabinets. Supplies standards will enable organizations to save costs by bulk purchase of consumable folders, labels and accessories.

2.8 Documentation and Procedures

All aspects of the records management processes must be documented, for standardization, as well as to provide staff guidance and training. Whether the documentation consists of one procedure manual or several, devotion to specific aspects of the records management program will depend on the nature and complexity of the records management program. In whatever format or content, the records management manual will become the First Nations government's eyewitness to the comprehensiveness of the RIM program. The manual should be considered a permanent essential record and be protected accordingly.

[32] ISO/15489-1, Section 9.7 Access, p. 14.
[33] *Ibid.,* Section 9.8 Tracking, p. 15.
[34] *Ibid.,* Section 9.6 Storage and handling, p. 14.

Examples of records management procedures for active records management are included in the first volume of this manual as part of Volume 2.

2.9 Managing Inactive Records

Inactive records are those records whose value and use by staff for daily work have diminished, but are required by the organization to satisfy a regulatory, audit or secondary value. These are sometimes also referred to as semi-active records, and may also be called “dormant” or “dead files”. The challenge for most staff, when this reduction in use occurs, is to determine whether the records are still required, and if so, what should be done with them.

In the life cycle management model, this phase signals the end of the active use of the record, and begins the operation of a retention and disposition program.

Benefits of a retention and disposition program to an organization include the following:

- improved operational efficiency – a reduction in the volume of information improves the speed with which staff searches are completed by reducing the volume of information that must be searched;
- consistency in records disposition – specific procedures and actions for retention and disposition ensure that records are managed in a systematic manner conforming to the First Nations government’s RIM policies, and reduce the possibility of inappropriate, inconsistent or accidental destruction of information;
- compliance with legal/regulatory retention requirements – requirements for records retention are identified in the schedule and compliance with the program demonstrates that the local government is managing records in the regular course of business and with sound business policies and processes. Demonstrating compliance with program policies and procedures is critical for establishing organizational credibility regarding litigation issues, and should include processes for management of records during litigation and/or government investigations, such as suspension of destruction;
- reduced space requirements and cost savings – space savings are realized when the systematic appraisal of records identifies the official copies of records in all formats, and enables the systematic transfer and destruction of records according to established procedures, as well as the recouping of space through reduction of filing equipment and electronic storage media; costs are saved through minimizing equipment purchases and ensuring that prime office space is not wasted on unnecessary records storage;

- compliance with contingency management programs – essential records are identified, protected and made available in the event of a disaster, and maintained to provide an audit trail for analysis and event review.[35]

2.9.1 Retention and Disposition Schedules

The tool that predicts the life cycle of records is the records retention and disposition schedule. This is often referred to as the retention schedule, or the records disposition authority. This tool is identified as another of the principal records management instruments used in records management operations.[36] This tool is applied to the records series groupings.

The retention periods are allocated to the records on the basis of the primary and secondary values of the records. Primary values are those associated with the reasons why the records are created and used, including administrative or operational values, financial or legal values. Secondary values are those retained with the records after their main purpose has been completed, including research or enduring historic or archival value.

The appraisal process determines these values by considering the broad ranges of uses of the records, and diverse perspectives of all uses, including:

- community values;
- all stakeholder interests, internally and externally;
- the business continuity requirements of the organization in light of disasters or other unforeseen events;
- the enduring historic values, including financial, social or political value of the records;
- the costs associated with retaining the records; and
- the risks associated with destruction of records after all uses have passed.

These values must all be considered, and there will always be differing perspectives for keeping records or discarding them.

The Classification and Retention Schedule included in Volume 2, includes a recommended retention schedule, with retention values assigned to each records series. This schedule has been prepared with the appraised values described, and has incorporated legal research up to December, 2009. This schedule is provided as a guideline with minimum retention recommendations. Retention periods are stated as either time based periods, which are

[35] ARMA International Standards Task Force, *Retention Management for Records and Information*, ANSI/ARMA 8-2005, (Lenexa, KS: ARMA International, 2005), http://www.arma.org, Section 4.3 Benefits of an Information Retention and Disposition Program, pp. 3-4, (ARMA *Retention Management for Records and Information*).
[36] ISO/TR15489-2, Section 4.2 Instruments, p. 8.

triggered by the date past the time of file opening, or event based periods, which are triggered by the completion of a condition or simply event based periods.

An example of a time based period is one where the file is destroyed 6 years after it is opened (i.e. current year plus 5 years). An example of an event based period is one that is triggered by the settlement of a claim, or when an employee retires. These conditions are explained where they are identified in the schedule.

Each First Nations government should conduct an evaluation of the requirements for its records before adopting this schedule through policy or bylaw. Staff working requirements, local conditions, legal precedents or other circumstances may require amendments or extensions to the recommended retention periods.

2.9.2 Managing Records Transfer and Disposition

Inactive records may still be needed, despite their diminished reference. However, to conserve office space, staff may remove them from active space a storage facility. This action, called records transfer, removes the records to a less costly location, and maintains staff ability to find the currently active information. However, when transfer occurs, staff will need to know where the records are located, in case they are required.

Best records management practice at this stage involves developing procedures that maintain control over the records. This ensures that the business rules for all work groups include processes, forms and activities to manage the records transfer and disposition actions. Sample procedures for managing records transfer and disposition are included in Volume 2. Records transfer and disposition should occur on a planned and routine basis, as part of the usual and ordinary course of business.

Records disposition actions may include some or all of the following activities:

- physical destruction (including the overwriting or deletion of electronic records, or shredding paper records);
- storage for a further period within the creating or user group;
- transfer to a storage area or storage medium under organizational control;
- transfer to another organization that has assumed responsibility for the business activity;
- transfer to an external storage area operated by an independent contractor or organization; or
- transfer to an internal or independent archives.

2.9.3 Records Storage

Records should be stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed. Records require storage and handling that take into account their specific physical and chemical properties.[37] Storage conditions and processes should be designed to protect records from unauthorized access, loss or destruction, and from theft and disaster.

First Nations governments typically establish internal storage facilities where inactive records are stored until disposal is activated. Such facilities must be adequate to protect the records from various hazards, including environmental hazards, moisture, vermin, and also include adequate security measures to prevent loss of control over space and records order.

The preferred storage container for paper records is the cardboard letter-legal tote box, also called "Bankers boxes." Cardboard is inexpensive and can breathe, allowing moisture to escape, rather than build and create mildew that will damage records. Tote boxes fold, contain no glue and are strong enough to hold paper documents. Folders and documents are tracked by the container or box in which they are contained.

Storage facilities are equipped with industrial steel shelving, designed to hold the weight of fully loaded storage boxes (approximately 40 lbs), with a layout allowing the free movement of carts or other mobile devices between shelves.

Records will be retrieved from time to time, and so, even at this less active or dormant phase, retrieval controls must be maintained. When record storage processes are undertaken, the staff in the business office who own the records are requested to pack storage boxes and prepare inventories or indexes of stored folders. When filled, boxes are then transferred to the records custodian for processing into the storage facility.

Control methods include:

- tracking folders in boxes, through the use of contents or transfer lists, and assigning numbers to boxes;
- assigning addresses or locations on shelving units;
- tracking the box locations on the shelves; or
- tracking the boxes or documents if retrieved.

[37] ISO/15489-1, Section 9.6 Storage and Handling, p. 14.

Records management application software will include descriptive fields or components to monitor these control methods at the inactive records management stage. However, without software, this monitoring can also be undertaken through the use of paper lists, or simple databases or spreadsheets to track these activities.

External storage agencies will provide some or all of these monitoring services as a part of the storage arrangements.

More details about managing records storage, including useful forms, are included in Volume 2, and in the ARMA standard on retention.[38]

2.9.4 Records Destruction Processes

Records destruction must be controlled and authorized as a regular business process in order that destruction processes are credible.

Better example – Carrier Lumber case – 1999 government lost case, and forced to pay $150 million dollars to Carrier Lumber Company. Government appealed, then dropped case days before appeal to be heard as a result of finding more documents relevant to the case that had not been disclosed. Cost of 8 boxes of documents is $150 million.

Recent events have drawn attention to the records destruction process. In 1999, the consulting firm Arthur Andersen was convicted of obstruction of justice for illegally shredding documents and destroying evidence of the energy firm Enron Corporation. As a result of this conviction, Arthur Andersen was unable to perform audits for publicly traded US companies and this destroyed its business. In 2005, the US Supreme Court overturned this conviction on the basis that the jury instructions were too vague and broad for jurors to determine correctly whether it obstructed justice. In 2002, Arthur Andersen had 28,000 employees. In 2005, Arthur Andersen had 200 employees. Arthur Andersen still has to defend more than 100 civil lawsuits.[39]

The implementation of a records retention schedule and processes includes defining specific approval processes and destruction methods. The following factors should be included:

1. The destruction actions must always be authorized, allowing for staff to intercede if specific issues such as a government investigation, audit, access to information access

[38] ARMA *Retention Management for Records and Information.*

[39] *Information Management Journal; (July/August 2005) (Volume 39) (Issue 4) (page 6)* and *Hoover's (www.hoovers.com).*

request, litigation or legal claim require that destruction must be halted. A sample records destruction approval form is included in Appendix B – Forms and Samples;

2. Records pertaining to any actual or pending government investigation, audit, freedom of information access request, litigation or legal claim should not be destroyed. There should be processes to impose a "legal hold" when specific requirements arise;
3. Records destruction should be undertaken in a manner that preserves the confidentiality of records, including the privacy of information about individuals;
4. All copies of records that are authorized for destruction, including security, preservation and backup copies, should be destroyed at once; and
5. Records should be maintained to document the destruction actions.[40] Certificates of destruction are generally provided by service agencies, and these are retained permanently, along with information about the records series title, date range and date of destruction.

2.10 Managing Permanent Records

Most records created, received and used by First Nations government staff will be destroyed when all requirements and uses have been complete. However, there are also records that have continuing or enduring value. These records are treated as permanently valuable records. Examples of these include: bylaws and policies, minutes and proceedings of chief and council and committees, property records, infrastructure records and traditional use records. Such records will require maintenance and storage in temperature and relative humidity environments that will ensure their long term preservation.

Preservation strategies should be selected on the basis of their ability to maintain the accessibility, integrity and authenticity of the records over time, as well as for their cost effectiveness. Preservation strategies can include:

- copying of records in the same medium, e.g. creating paper copies;
- converting records, changing the format but retaining the identical content, e.g. creating microfilm or electronic imaged copies; or
- migrating records, periodically transferring electronic records from one hardware/software configuration to another, or from one generation of technology to another, to preserve the integrity of the records and ensure the ability to retrieve and use them.

There are no guarantees about the "permanence" of any records, since the chemical composition of the materials upon which records are recorded and the storage conditions will determine the

[40] ISO/15489 -1, Section 9.9 Implementing Disposition, pp. 16 – 17.

life expectancy of the media. The term "stability" denotes the extent to which a given storage medium retains physical characteristics and chemical properties appropriate to its intended medium. The stability period is equivalent to the useful life, lifetime estimate or life span of a given medium.[41] For those records requiring long term preservation, the life expectancy is 100 years for acetate-based microfilms materials, and 500 years for polyester-based materials, assuming that the microfilm is stored within prescribed conditions.[42] Stability of various digital storage formats is a key concern of archivists. Digital storage formats are currently the subject of research to determine best practices and most stable formats. There will be more discussion of this topic in Chapter 3.

A practical note is provided by archivists working with paper documents. It is recommended that staff use acid free, buffered paper to create minutes and other records of long term value. In addition, these records should not be bound, but retained in acid free folders to minimize the movement of acid into the documents.[43] This mechanism will provide a secure and proven method for storing a key set of municipal records for future access and use.

A second practical note here is that records require the same type of environment as people require. Consequently, organizations should ensure that the storage or archives facilities are dry, and with sufficient heat to prevent mould and other hazardous elements.

2.10.1 Role of Archives

There are two meanings of the word. One meaning of "archives" refers to the building or institution that houses archival material. The other meaning of "archives" refers to the material itself. In the records management context, archival records are those that have enduring value, and are transferred to the custody of an archives for preservation and safekeeping. Larger First Nations governments have established archives within their organizations. Smaller organizations may not have the volume of records to warrant a separate archival operation, but may instead develop business processes where custody of archival records is transferred to the Band Administration department when the originating departments have completed all uses with the permanent records.

Permanent records may be transferred to an external storage provider or archival agency. Formal arrangements or agreements must be made to ensure the continuing obligations to

[41] William Saffady, *Records and Information Management: Fundamentals of Professional Practice*, (Lenexa, KS: ARMA International, 2004), Media Stability, p. 100.
[42] CAN/CGSB-72.11-93, Section 3.26 Life Expectancy. Further information on media stability is documented in ANSI/AIIM standards, including MS23.
[43] Interviews by the authors with the Local Government Management Association of British Columbia Records Management Manual Advisory Committee, March 2006.

maintain the records appropriately, including the retention and disposition requirements, and any access or restrictions on access. The accountability for the records must also be defined.

Archival management is a specific discipline and has a comprehensive body of professional practice, and intersects with records management at the point where the custody of permanent records is transferred from the creating body to the archives.

The Archives Association of British Columbia (AABC) provides training materials, including guidelines for all aspects of archival practice, on its website and through its professional activities and programs.[44]

2.11 Program Maintenance

Program maintenance activities consist of the ongoing responsibilities for operating and maintaining RIM programs once they have been implemented. These activities include all of the continuous functions and controls that ensure smooth functioning and operations. A key component of maintenance is monitoring for quality assurance and adherence to standards and operating rules.

2.11.1 Quality Assurance and Auditing

The Quality Assurance Program is a necessary component that monitors and judges the records management system.[45] Defined procedures ensure that quality assurance monitoring is undertaken on all aspects of the records management system, whether it be sampling of practices with electronic records, or through detailed examination and analysis of records processes.

Audit trails are required for electronic records. The written logs are kept because they include historic activities or events that may in future impact the records. These written logs provide details of events occurring in the records management system, including data about changes to the records stored in the system. Typical audit trails consist of system generated and operator generated logs. These logs include such information as:

- system functions applied,
- the objects to which the function was applied,

[44] AABC, http://www.aabc.bc.ca.
[45] CAN/CGSB-72.34, Section 7 Quality Assurance Program.

- the outcomes,
- the person responsible,
- the date and time of the events (such as the initial capture into the system), and creation of new versions and changes.

Regular auditing of the records management system ensures that the records systems and procedures are being implemented according to the First Nations government policies and meet anticipated outcomes.[46] In addition, audits help to ensure the continued legal accountability. The monitoring processes are automatically documented to provide evidence of compliance with the RIM policies and procedures.

2.12 Program Operational Issues

The components of RIM programs, once established, require ongoing management, to ensure continued adherence to program standards and processes. There are additional regulatory and risk management issues that have an impact on the RIM program. These include:

- Records management issues associated with operations of the *BC FOIPPA (Federal Access and Privacy legislation).*
- Records security and access issues; and
- Records protection from disasters and unplanned events.

2.12.1 BC *Freedom of Information and Protection of Privacy Act* and Records Management Insert Federal ATIPP legislation here

Add Public Government Appeals Process; Information Sharing Agreements (back up); Purchasing Agreement/controls

Since 1994, local governments in British Columbia have had to comply with the provincial *Freedom of Information and Protection of Privacy Act.* [47] Effective records management practices will assist local governments with compliance under *FOIPPA*. This includes use of specific retention periods, properly applied to all records, in all recorded formats and effective written policies governing the use of electronic mail or "e-mail."

2.12.1.1 Commissioner's Orders and Records Management

[46] *Ibid.,* Section 10 Monitoring and Auditing, p. 17.
[47] R.S.B.C. 1996, c. 165.

A number of orders have been issued by the Information and Privacy Commissioner for British Columbia that link to effective records management. The following examples provide illustrations of the close connection.

An applicant made a series of requests to the Insurance Corporation of British Columbia (ICBC) for all records related to labour relations hearings and a judicial review involving the applicant. ICBC staff invested a substantial amount of time and effort attempting to locate these records. Eventually, ICBC located more than 1,300 pages responsive to the request. Further, the Information and Privacy Commissioner ordered ICBC to take all reasonable steps to continue searching for records and to report its results of its continued search to the Information and Privacy Commissioner. [48]

This case continued on and resulted in another order where the Information and Privacy Commissioner found that ICBC's search for records had been adequate, but expressed concern about ICBC's records management system:

> In this evidently contentious matter, ICBC kept finding more and more records as the applicant pressed his search. This concerns me. While I have considerable sympathy with the demands that access requests place on public bodies, it is important that members of the public not be paranoid in terms of what they are likely to receive in response to a request for records. Promoting careful records management in public bodies in order to be able to find records is thus an essential aspect of complying with the goals and obligations established by the Act.[49]

In another case, an employee of the Ministry of Attorney General requested access to records of his employment. The Ministry located some records, but the employee had reason to believe that the search was inadequate. He was able to list specific records that were missing. After subsequent searches, Ministry staff found some of the additional documents. The Ministry concluded that some of the responsive records had been lost or destroyed, but it was not able to explain why. The Information and Privacy Commissioner found that, on balance, the Ministry had conducted an adequate search for records, although he noted:

> However, I would be remiss if I did not comment on the fact that the process of finding records for this applicant is not a credit to the records management practices of the

[48] Office of the Information and Privacy Commissioner for British Columbia (OIPCBC), "Request for Access to Records of the Insurance Corporation of British Columbia," Order No. 12-1994, *Orders*, http://www.oipcbc.org/orders/1994/Order12.html.
[49] OIPCBC, "A decision by the Insurance Corporation of British Columbia (ICBC) to withhold records from an applicant and the adequacy of ICBC's search for records," Order No. 170-1997, *Orders*, http://www.oipcbc.org/orders/1997/Order170.html.

> Ministry. Were it not for the fact that the applicant was able to list specific missing records, he would not have been in a position to argue persuasively for additional searches. It should not be necessary for public servants to copy their personnel files regularly and safeguard them for fear that the contents of such files will not be found in the event of subsequent need. The success of the Ministry's searches in this inquiry owes much to the tenacity and knowledge of an informed applicant.[50]

2.12.1.2. *FOIPPA* and Electronic Records

In his yearly review of all the files handled by his office, the Information and Privacy Commissioner summarized the relationship between records management and electronic records as follows:

> Traditional records management theory focuses on a subset of information that can be described as business records. FIPPA [*FOIPPA*] extends the challenge of traditional records management to the entirety of paper, audio, visual and electronic information in the custody and control of any public body, from an obscure inter-office memo to a Cabinet submission.
>
> Traditional records management is also challenged by the expanding reliance on electronic records and databases. The sheer volume, and variety, of electronic records makes it difficult to catalogue, organize and preserve them in a way that keeps them accessible. These problems are exacerbated as hardware, software and storage media become obsolete, leaving behind records that can no longer be read, making a once-valuable government asset worthless.[51]

FOIPPA applies to the broad range of recorded information, including electronic mail. Electronic mail is recorded information and subject to the same rules for paper records used by local governments. Many applications to public bodies now routinely seek disclosure of all relevant electronic records and specifically include electronic mail.[52] In addition, the use of surveillance systems by public bodies in order to collect personal information by means of video, audio or

[50] OIPCBC, "A decision by the Ministry of Attorney General to refuse an individual access to some of his Human Resources records," Order No. 218-1998, *Orders*, http://www.oipcbc.org/orders/1998/Order218.html.
[51] OIPCBC, "Annual Report 2004/2005," *Annual Reports*, http://www.oipcbc.org/publications/annual_reports/2005AR/OIPC_Annual_Report_web.pdf, p.15.
[52] See for example, OIPCBC, Ministry Of Children And Family Development, [2002] B.C.I.P.C.D. No. 53 (case where employee requested all of his personal information from his employer, the OIPC held that any records requested by the applicant included electronic records), *Orders,* http://www.oipc.bc.ca/orders/Order02-52.pdf, pp. 10-11.

other electronic surveillance systems is expanding.[53] The Information and Privacy Commissioner for BC acknowledges this trend and cautions public bodies to implement such systems as a last resort rather than an initial solution in order to ensure that personal information is collected in accordance with Part 3 of *FOIPPA*.[54] Part 3 of *FOIPPA* requires all public bodies to protect the privacy of personal information. Under *FOIPPA*, the Office of the Information and Privacy Commissioner is permitted to conduct an audit of a public body's automated systems and order public bodies to change their personal information practices if they do not comply with Part 3 of *FOIPPA*.[55]

Public bodies are required to take reasonable measures to protect personal information from risks such as unauthorized collection, use or disclosure as outlined in Part 3 of *FOIPPA.* This also applies to the use of electronic mail.[56] An electronic mail policy can assist local governments in meeting the broad range of compliance requirements under *FOIPPA* and as such, an electronic mail policy should be created to fit the specific needs of the local government.[57] Public bodies may also levy charges for searching electronic mail and other electronic records that respond to formal requests for information.[58]

Some key elements of an electronic mail policy should include the following:

- The application of specific retention periods for electronic mail;
- A statement that electronic mail is the property of the local government and not the employee;
- A specific list of permitted uses of electronic mail, including specifically what is not a permitted use, such as employees using electronic mail at work for personal use;
- A description of how the local government manages records:
    - for information requests under *FOIPPA*,
    - during investigations by the Office of the Information and Privacy Commissioner or
    - during litigation;

[53] See OIPCBC, "Public Surveillance System Privacy Guidelines (OIPC Reference Document 00-01 January 26, 2001)," *Advice*, http:// www.oipcbc.org/advice/VID-SURV(2006).pdf.
[54] *Ibid*., p. 4.
[55] See requirements for ensuring the confidentiality of electronic mail, OIPCBC, "Guidelines For Audits Of Automated Personal Information Systems (OIPC Guideline 01-01 October 10, 2001)," http://www.oipcbc.org/pdfs/public/GuidelinesforAudits.pdf).
[56] See guidelines, OIPCBC, "Faxing And Emailing Personal Information," (February 2005), http://www.oipcbc.org/pdfs/public/fax-emailguidelines(Feb2005).pdf.
[57] See ARMA International*, Requirements for Managing Electronic Messages as Records*, (Lenexa, KS: ARMA International, 2004), http://www.arma.org, *(*ARMA *Managing Electronic Messages as Records)*.
[58] See guidelines, Information Policy and Privacy Branch of the Ministry of Labour and Citizens' Services of British Columbia, "Guidelines for Determination of Fee Estimates," n.d., http://www.lcs.gov.bc.ca/privacyaccess/main/fee_estimates.htm.

- The policy should state whether or not the local government monitors electronic mail use by employees; and
- The policy should set out a code of conduct for employees using electronic mail and the consequences to employees for violating the electronic mail policy.

Further information about electronic mail management is found in Chapter 3 of this manual.

2.12.1.3 *FOIPPA* and Use of Personal Information

Another key component for compliance with *FOIPPA* includes appropriate management of personal information. For example, section 69 of *FOIPPA* requires the head of a public body to make available for public inspection and copying a directory that lists the public body's personal information banks (PIBs). This includes the following information with respect to each PIB:

- The title and location of the personal information bank;
- A description of the kind of personal information and the categories of individuals whose personal information is collected;
- The authority for collecting the personal information;
- The purpose for which the personal information was obtained or compiled and the purposes for which it is used or disclosed.[59]

PIBs are those records series that are filed by personal identifiers, such as an identifying number, symbol or other particular assigned to the individual, and contain information about recognized individuals. To assist staff in identifying PIBs, the “typical” PIBS have been noted on the records classification system included in this manual. Local governments should confirm the presence of PIB’s in their records collections their organization, and prepare the directory as required by *FOIPPA*.

2.12.1.4 *FOIPPA* and Records Available Without Request

FOIPPA requires that specified records be made available to the public by the head of a public body without a formal access request under *FOIPPA.* Section 70 of *FOIPPA* requires policy manuals to be made publicly available without a formal request under *FOIPPA*. Section 71 of *FOIPPA* permits the head of a public body to designate categories of records that are available to the public, on demand, without a request for access under *FOIPPA* and to charge the public a reasonable fee for access to these designated records.

[59] Section 69(6).

Typically, policy manuals and designated records such as these are available for public reference in public collections, at information counters or kiosks, and increasingly on local government web sites. Records management procedures need to be in place to ensure that the records are either readily retrievable by individuals without staff assistance or in records collections where staff can readily locate them when an inquiry is received.

It is common for many local governments to make as much public information as possible readily available to anyone who wishes it, without requiring a member of the public to make a formal *FOIPPA* request. This strategy of local governments assists the public to access needed public information and at the same time, reduces the local government staff time and other associated costs that are necessary in order to process information through the formal request process under *FOIPPA*. Additionally, after a formal *FOIPPA* request has been received and processed and pubic access to that information made, it is common for local governments to make that information publicly available generally without a formal request under *FOIPPA*. This strategy saves the local government time and cost since it does not need to expend staff resources again for a similar future information request.

2.12.2 Information Protection and Security

The security classifications and requirements of records must be incorporated into RIM program operations.[60] The *FOIPPA* environment, as well as sensitivity about confidential matters prior to public disclosure, requires that privacy protection and confidentiality or security measures be assigned to some groupings of records.

Generally, most information within a First Nations government is unrestricted and readily available for staff use. Most First Nations governments have specific provisions for making information routinely available when required for external requests.

However, the *FOIPPA* environment requires local governments to impose restrictions on access when required by *FOIPPA* to protect privacy. In addition, content of records may be sensitive or contain confidential business information associated with labour relations matters, land transactions, and litigation matters. Council deliberations *in camera* may also contain sensitive information. Such confidential information will require specific notations and protection provisions, including restrictions on access and use of the records.

Managing the access process involves:

[60] ISO/15489-1. Section 9.7 Access, pp. 14-15 and CAN/CGSB-72.34, Section 6.12 Security and protection, p.27.

- Categorizing records according to their access status;
- Releasing records only to those authorized to see them;
- Encrypting records to be ready only as and when required and authorized;
- Undertaking records processing and transactions only by authorized staff; and
- Assigning permissions according to areas of responsibility.

Monitoring and mapping of user permissions and job functional responsibilities is an ongoing process for all types of records and must be maintained.

2.12.3 Vital/Essential Records

Records protection from disasters is another operational RIM program concern. Recent local disasters have included forest fires and floods. As they were preparing for the Delgammuukw Court case, the band office of the Gitsan people burned to the ground. Recent world disasters have included earthquakes, tsunamis, storms and terrorist acts. In all cases, essential information for government agencies has been required in order to effectively respond to these events. Emergency planners are close allies with records managers in this work. The records management component fits within local government disaster plans and emergency management.

Vital records, [61] sometimes also referred to as essential records, are defined as those records that are:

- vital or essential for the continuation or reconstruction of an organization;
- important in establishing the legal or financial position of an organization; and/or
- important in preserving the rights of an organizations, its employees, customers, and shareholders.

These records constitute usually no more than 5% of the total volume of records in the local government. These records may be active, inactive or archival. The challenge for the Band Manager, Office Clerk, or Records Manager is to identify these records and establish protective measures for them. This component of records operations requires a combination of records management practices to select vital records, protect them, and make them available during or after a crisis. Vital records are determined by context, and how the records relate to the mandate of the First Nations government, as well as by the business cycles in which records are generated.

[61] Detailed program information is available from ARMA International at http://www.arma.org, including *Vital Records: Identifying, Managing, and Recovering Business-Critical Records*, 2003.

There are two specific components to this program: identifying the essential records, and establishing protection methods and procedures.

The Government of Canada[62] places essential records into three categories:

- **class 1 -** records required during the emergency and immediately thereafter;
- **class 2** - records required for the basic recovery phase - for health, protection of life and property; and
- **class 3** - records required for later recovery phase - for basic rights of people and organizations.

General business definitions of vital records fall into four categories:

- **class I –** Essential – to the continued life of the organization. Examples include contracts, accounts receivable, inventory, creative materials, research documentation;
- **class II** – Important – necessary to the continued operation, and reproduced at great cost. Examples include accounts payable, directives, payroll records;
- **class III –** Useful – needed for the uninterrupted operation, and the loss would cause temporary inconvenience. Examples include bank statements, correspondence; and
- **class IV** – Unimportant and should be destroyed. Examples include advertisements, announcements, requests answered.

No matter which set of criteria are used, the First Nations government's vital records should be identified according to their requirements for operation during and after the disaster or crisis.

Choices for essential records protection involve a determination of what scale of disaster is anticipated. Based on the risk assessment, records protection methods are implemented for on site or offsite protection.

Keeping records on site is considered the highest risk, but may be necessary if the records are required for daily work, and duplicate or working copies will not be sufficient. Devices for records protection include a safe, vault or fire proof containers.

Another method is to duplicate the records. There may be natural "dispersal" or duplication as part of the regular course of business, as duplicates may be provided to several departments for information or action. In other cases, the duplication may have to be planned as part of business

[62] Public Safety and Emergency Preparedness Canada (PSEPC), http://www.psepc.gc.ca.

processes, with the copies safely stored in a separate location. If possible, staff should store the original document and use a duplicate record for working purposes.

Off site storage is the preferred method, and is considered less costly and less risky than on site storage. The likelihood of disasters occurring in different locations at the same time is less probable than the single sited disaster such as fire or flood. The same question about how and when to duplicate the records must still be answered, but in this situation, the copies or originals of records will be in a vault, records centre, or some other secure location.

Recent disasters have provided several key lessons in disaster planning. Hurricane Katrina's devastation of the US Gulf Coast is teaching planners that one of the most important activities is to plan for the worst case scenario, and to test and retest the scenario. Another of the lessons learned is the importance of moving toward electronic formats[63]. Duplication through back up and dispersal of records is much easier with electronic information, and the vital records can be easily moved to another location. After the fact, recovery of electronic documents is easier than the recovery of paper documents.

Records Managers appraise records for their importance to organizations as part of records systems development. A common method for identifying vital or essential records is to place a "VR" alert in the records classification system beside the record series title. "VR" signifies "vital records". This alert, along with procedures, will be the components of the vital/essential records protection program.

2.12.4 Traditional Use and Cultural Heritage Records

Many First Nations are documenting their traditions using various methods to do so. Whether the purpose is to collect oral histories for use in title or aboriginal rights matters, or to preserve the memories of elders for the transmission of cultural knowledge, the information that is gathered will have enduring value to the organization, and will constitute permanently valuable records, requiring appropriate methods for collecting and also for preserving the information.

The mechanisms that First Nations may use are also varied, and may result in the production of sound or video recordings of interviews with community members. These interviews may be personal or family stories, interpretations or versions of legends and stories about past events, or the recollections of specific historic events. These records may have been undertaken using media, such as tape recordings that must be conserved or preserved to ensure the longevity of the information they contain.

[63] Nikki Swartz, "Dealing with Disaster" *The Information Management Journal* July/August 2006: 29 - 34

Traditional use studies may be undertaken by external experts hired by the First Nation to examine specific aspects of land or resource use, cultural practices and other elements of First Nations life. These studies may also involve the collection of stories about past practices, as well as the preparation of maps, land surveys, inventories of resources, and other studies. When engaging experts, First Nations should ensure that the language of the engagement contract clearly stipulates what information and documentation will be provided to the First Nation, and assert First Nations ownership of the final products from such studies.

The National Centre for First Nations Governance is developing a tool for First Nations to utilize, when undertaking to document and preserve their oral histories that has a basis in law, and will help ensure that the information documented can be used for various purposes, including as evidence in court cases. In the meanwhile, the following short summary is from a legal review provided by Radcliffe and Company to assist with developing this tool[64]:

> "If a First Nation undertakes such a (an oral history) project, it should ensure that the following information is documented:
>
> - How their oral histories, stories, legends, customs and traditions are preserved;
> - Who is entitled to relate such things and whether there is a hierarchy in that regard;
> - The community practice with respect to safeguarding the integrity of its oral history, and stories, legends and traditions.
>
> Information gathered from a particular interview might be divided by those categories, plus:
>
> - His/her own family history
> - His/her version of legends and stories about events from the more distant past, and
> - His/her recollection about specific events.
>
> The following technical points may increase the reliability of the oral histories documented:
>
> - The interview should be videotaped so that the demeanour of the interviewee is seen, and
> - The interviewer should avoid stopping the videotape as such breaks in the recording may raise questions about what was discussed off-camera and whether the discussion influenced the interviewer's account".

[64] *Memorandum Re Oral History in the Courts*. To National Centre for First Nations Governance, by Ratcliffe and Company, September 25, 2009. North Vancouver, BC.

As with other records discussed in this Toolkit, these various types of materials must be captured, filed and preserved so that they will be available for future reference and use. Much of the material in traditional studies and oral histories will be identified for museum and archival collections.

3. Electronic Records Considerations

While the stated principles of records management indicate that all records are managed according to the same principles, the nature of electronic records requires some additional records management considerations. This chapter of the manual covers specific issues and requirements for these record types. In addition to the ISO and Canadian standards already cited as the foundation for the practices in this manual, there are also RIM best practices and standards specifically developed for the management of electronic documents and records.

It is the management of these formats of records that present the most challenging records management dilemmas and most pressing management requirements. Just as organizations in the past have struggled to control the proliferation of paper records, so are they now grappling with the exponential growth of digital information. In 2003, a Berkley School of Information Management study estimated that paper formats grew in the United States at 38 percent per year from 1999 to 2003.[65] This same study found that the digital formats grew at a rate of at 80 percent per year.[66] The findings of this United States study are applicable to formats in British Columbia.

In interviewing First Nations staff for this project, the authors received a common message from everyone: provide basic principles for managing electronic records that are easy to follow, and will ensure that local government records are available in future.

This section provides recommendations about specific electronic records formats and current best practices for their management. A common theme in all of the standards is that electronic records will be considered the best evidence, no matter in what format or data system they are generated or stored, if an organization can demonstrate the reliability and security of the methods and procedures around which these records are managed.

3.1 Electronic Records Defined

The terms “electronic document” and “electronic record” are often used interchangeably. The terms electronic document” and “electronic record” refer to documents or records that have been created, used and stored in a digital medium, using computer hardware and software as well as human intelligence to create, modify, store, access and retrieve the documents. Examples

[65] Peter Lyman, and Hal R. Varian, “How much information?”, *University of California-Berkeley School of Information Management and Science*, 2003, http://www.sims.berkeley.edu/research/projects/how-much-info-2003.
[66] *Ibid*.

include text-based documents, such as word processing and electronic mail, image or graphically– based documents, such as photographs, engineering drawings, maps or numerically-based documents or tables. Hard copy formats can also be converted into digital records by scanning.

In British Columbia, electronic and paper records share the same legal definition. In section 29 of the *Interpretation Act* a "record" is defined as follows:

> "record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise;[67]

Similar definitions are found in Canadian federal legislation. As we can see, the legal definition of paper and electronic documents and records is broad. When British Columbia courts look to interpret what an electronic record is, this is the definition of "record" that the courts will likely consider.

By their nature, electronic documents and records are not as stable, or static, as those in hard copy formats. The software systems used to create electronic records are frequently upgraded or modified. The equipment used to create, access and store the electronic records is also subject to continuous change. Thus, one of the key challenges we face is caused by the dynamic nature of these formats. Moreover, systems for electronic records should be designed so that the records remain accessible, authentic, reliable and usable through any kind of system change, for the entire period of their retention."[68]

Typically, information technology architecture is structured along the lines of applications management. This leads to "silos" of information, disconnected from one another. In addition, the management responsibilities for these systems are frequently assigned to different owners. This assignment creates organizational challenges in planning, strategizing, budgeting, and implementing the records and information management issues. Finally, the custody of electronic records is usually held by individual workers. This custody is usually set behind a series of permissions that are intended to protect the records, but which may lead to inability to share or process information effectively.

[67] R.S.B.C. 1996, c. 238.
[68] ISO/15489, Section 9.6 Storage and Handling, p. 14.

3.2 Hard Copy vs. Digital Formats

The records collections in most First Nations governments are a blend of different formats. While we can talk about the "digital age" that we work in, the reality for most organizations is that they are still in paper-based worlds. What makes this reality challenging is that we have to determine what format of record is the "official" record, and to identify the original as contrasted with the copies of records.

Using the old rules of evidence, the "official" record was almost always determined to be a printed or hard copy document, even if it was first generated as a digital record. Thus, electronic copies were seen as processing records only, viewed as transitory or ignored completely, and could be discarded after all uses were complete. Now, however, we have the possibility of using electronic records as evidence, and so now we have to decide which format to treat as the official record.

In addition, in using multiple formats of information, staff must also contend with duplicate copies in the various formats. Recent research has found that there will be at least 25 percent of duplication caused through retaining documents in both electronic and hard copy formats. Expressed another way, fully one quarter of the costs and labour expended to manage, store and preserve information is wasted on duplicate materials. Most organizations will find significant advantage when reducing this duplication.

3.2.1 Mix of Formats Today

In February, 2006, a survey of the LGMA Records Management Manual Advisory Committee found that the percentage split between electronic and hard copy records ranges from 80 percent digital/ 20 percent paper to 40 percent digital/60 percent paper.[69] So, while the tantalizing digital (i.e. "paperless") future is before us, we must plan and operate for the current reality in most organizations – a mix of hard copy, paper formats, and electronic formats. This mix of formats also tends to split along date lines, with the recent information in digital format, and the older legacy collections of records in paper format. Consequently, this split tends to create at least two separate systems for managing the information, particularly in the retrieval and preservation phases of the life of information. However, in view of the requirements to manage all information according to the same principles, this spilt along format lines must be overcome to ensure a comprehensive approach.

[69] Local Government Management Association of British Columbia, *LGMA Records Manual Project: Committee Survey,* February 2006 (LGMA Survey 2006).

3.2.2 Scanning and Imaging

Scanning of hard copy records is a common technique for converting paper or hard copy documents into a digital format. A digital image is defined as, "a representation of a source record that can be used to generate an intelligible reproduction of that record or the reproduction itself."[70]

Digital images are the most recent version of "pictures" or replicas of source documents. Prior to digital imaging, micrographics was employed for many years as a film-based method of copying (and reducing the size of) original source records. When hard copy or source documents are scanned, the resulting digital images are readily shared within work groups, sent via e-mail as attachments and even distributed via electronic publishing or posting to web sites. For First Nations governments, the use of scanning has greatly enhanced the ability to share historic documents with residents, while retaining and conserving original, fragile documents.

The scanning process requires:

- Good quality source records or documents, sufficiently legible enough to be copied;
- Scanning equipment to create the scanned image, software to process the images and sufficient storage capacity to hold the images in the computing environment; and
- Indexing and describing the images so that they can be retrieved.

The evidentiary value of the images is ensured if, in addition, the processes for controlling the scanning process are also defined and managed. The Canadian General Standards Board *Electronic Records as Documentary Evidence* standard defines the criteria for establishing the electronic imaging program, and also describes the preparation, capture, indexing and quality assurance processes that should be in place.

3.3 Data and Metadata Requirements

"Metadata" is basically data about data. In order to understand the full meaning of an electronic message, which is the content, we also need to know who sent it, on what date, and what the sender described as the subject of the message. This is the metadata that provides the contextual attributes of the data. In some cases we might need to verify the version of a message, or view attachments. All of this descriptive information is called metadata, and, in addition to the actual document or record, the metadata must be saved and associated with an electronic document in order to make it a meaningful record.

[70] CAN/CGSB-72.11.93, p. 6.

The ISO Technical Specification of Metadata[71] identifies six types of metadata that should be designed and applied within records systems:

- Metadata about the record itself – at the point of capture, after records capture, accessibility requirements, security requirements;
- Metadata about the business rules or policies and mandates – at the point of capture and after records capture;
- Metadata about agents – persons involved at records capture and after records capture;
- Metadata about business activities or processes – business functions, processes, activities, transactions, security and accessibility;
- Metadata about records management processes; and
- Metadata about the metadata record.

3.4 "Authentic and Reliable" Electronic Records

The concepts of authenticity and reliability are critical to the validity of electronic records. Electronic records require different measures and controls from those in the paper or conventional hard copy formats.

As earlier described, an "authentic" record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have created or sent it, and to have been created or sent at the time purported. Moreover, "to ensure the authenticity of records, organizations should implement and document policies and procedures to control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alternation, use and concealment."[72]

A reader relies on visual cues when looking at a hard copy document to see who created the record, when it was created, and if there have been alterations. Without specific electronic records management software that effectively locks down electronic documents when they have been declared as records, the reader may not be able to as easily to verify the authenticity of an electronic document.

A reliable record is described as "one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest, and can be depended

[71] ISO, *Information and Documentation – Records Management Processes – Metadata for Records – Part 1: Principles.* (ISO/TS 23081-1), (Geneva, Switzerland: ISO, 2004, http://www.iso.org).
[72] *Ibid*., Section 7.2.2 Authenticity, p. 7.

upon in the course of subsequent transactions or activities."[73] A frequent challenge for readers of digital materials is to locate all of the digital documents associated with a particular matter or project, and to determine which versions of those electronic documents are the documents that should be used.

3.5 Integrity of Electronic Records Management Systems = Electronic Records as Evidence

In Canada, the integrity of electronic records management systems, working in the usual and ordinary course of business, is governed by a mix of statute law and decisions made by courts. A cornerstone of the law of evidence is that only relevant and truthful evidence is admitted into court. That means that hearsay evidence is prohibited.

3.5.1 The Hearsay Rule

In British Columbia, business records are only admissible into evidence in the courts as an exception to the hearsay rule. The hearsay rule is complicated and often misunderstood.

The former Chief Justice of British Columbia explained the hearsay rule this way:

> Witnesses are expected to give evidence about matters of which they have personal knowledge so that an accused, or a party in a civil case, can challenge or confront that evidence head-on in cross-examination. Hearsay evidence cannot be challenged directly because the witness is only testifying as to what he has heard, and therefore cannot speak to the truthfulness of the underlying facts. It may have been a rumour, or hearsay further down the information chain, or it may have been concocted mischievously several minds away from the witness.[74]

The hearsay rule protects evidence to ensure that Canadian courts receive only authentic, relevant and reliable evidence. Having said that, to ensure that all relevant reliable evidence is admitted, Canadian law has recognized specific exceptions to the hearsay rule. One of these exceptions is available for proof of business records as set out in the British Columbia and Canada *Evidence Acts*.

[73] *Ibid*., Section 7.2.3 Reliability, p. 7.
[74] The Honourable Chief Justice of British Columbia Allan McEachern (as he then was), "Chapter 10, Legal Compendium", *Legal Compendium*, 1999, www.courts.gov.bc.ca/legal_compendium/Chapter10.asp.

3.5.2 British Columbia *Evidence Act*

In British Columbia, section 42 of the *Evidence Act* sets out the rules for admissibility for business records.[75] Section 42 provides that if a fact is recorded in the ordinary course of business within a reasonable time, it may usually be given in evidence without proof by personal knowledge.

Section 42 defines "business" broadly, to include "every kind of business, profession, occupation, calling, operation or activity, whether carried on for profit or otherwise". That means that "business" include such organizations as: companies, local governments, non-governmental organizations, including non-profit associations.

While section 42 does not cite electronic records, by virtue of use of "record", use of electronic records is implied.

3.5.3 British Columbia *Electronic Transactions Act*

In British Columbia, the *Electronic Transactions Act* gives electronic signatures and electronic records the same legal weight as signatures and records created in paper.[76] The *Electronic Transactions Act* applies to both the public and the private sectors, but does not take priority over any current statute that specifies whether electronic means of communication can be used or not.[77] That would include the British Columbia *Evidence Act*. Persons or organizations are not required to use the *Electronic Transactions Act*..[78]

Section 8 of the *Electronic Transactions Act* provides that an electronic record may function as an original if there are sufficient assurances of integrity of the information in it. This is similar to the standards for meeting the best evidence rule in section 31.2 of the *Canada Evidence Act*, noted below.

Section 10 of the *Electronic Transactions Act* provides that a requirement to retain a record is satisfied by the retention of the record in electronic form if the record is retained in the format in which it was created, the record will be accessible in the future and if the electronic record is transmitted, then any information available about the time of its transmission be retained. The *Electronic Transactions Act* does not require a person or organization using it to retain the

[75] R.S.B.C. 1996, c. 124.
[76] S.B.C. 2001 c. 10.
[77] *Ibid*., Section 2.
[78] *Ibid*., Section 4.

metadata, except that, if the electronic record is transmitted, then information about its origin and destination should be retained.

The *Electronic Transactions Act* does not state a specific retention period for which to retain electronic records. Nor does it prescribe the specific computer hardware/software to be used. In this way, the *Electronic Transactions Act* is technology neutral.

The *Electronic Transactions Act* does not operate as an admissibility of evidence statute. It operates as a legal structure that removes any uncertainty about the legality and enforceability of electronic transactions in British Columbia.

3.5.4. Canada *Evidence Act*

In Canada, for those businesses subject to Canadian federal law, the *Canada Evidence Act* applies.

Like British Columbia, section 30(1) of the *Canada Evidence Act* provides that "a record made in the usual and ordinary course of business that contains information in respect of that matter is admissible in evidence under this section in the legal proceeding on production of the record."[79]

The *Canada Evidence Act* goes further than British Columbia to provide for admissibility of electronic records. The *Canada Evidence Act* in sections 31.1-31.8 lists the components needed to admit electronic records as evidence in court:

31.1 Authentication of electronic documents;
31.2 Application of best evidence rule — electronic documents;
31.3 Presumption of integrity;
31.4 Presumptions regarding secure electronic signatures;
31.5 Standards may be considered;
31.6 Proof by affidavit;
31.7 Application; and
31.8 Definitions.

[79] R.S.C. 1985, c. C-5.

Section 31.1 provides that a person intending to rely on an electronic record has the burden of proving its authenticity by evidence that the electronic document is that which it is purported to be. This is important for persons and organizations to remember since they must take concrete steps to prove to the court that their electronic records should be admitted into evidence.

Section 31.2 provides that where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored. The best evidence rule is used by courts to ensure the integrity of the record, since modifications are more likely to be identified on the original record. The best evidence rule requires that the person claiming that a record is what it says it is, should produce the original record or the closest thing available to an original. For electronic records, the "original" record is not as easy to determine as with paper records. Section 31.2 adapts the best evidence rule for electronic records. Instead of looking to the actual original record for reliability, section 31.2 looks to system reliability. In this way, section 31.2 provides the legal basis for admitting electronic records in court. So that, if an organization destroys paper originals in the ordinary course of business under a records retention schedule, then that organization is not prejudiced in using reliable electronic versions of those records.

Section 31.3 sets out a series of legal presumptions that a person or organization can use to prove the integrity of the electronic records system. In the absence of evidence to the contrary, the integrity of an electronic documents system may be proven in one or more of three ways.

First, the integrity of the electronic records system is proved by evidence that the computer system was operating properly. If the computer system was not operating properly, evidence can be lead that, the fact that it was not working properly does not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system. This legal presumption is technology neutral, so that there is no advantage to using a more sophisticated computer system than a simpler one.

Second, the integrity of the electronic records system is proven if the electronic record was recorded or stored by a party who is adverse in interest to the party seeking to introduce it. This applies when a party receives electronic documents from an adverse party as the result of the litigation process. In the litigation process, parties in a lawsuit exchange records prior to trial as part of pre-trial discovery of facts and evidence. Here, the record is presumed reliable since the party adverse in interest knows his or her own computer records system.

Third, the integrity of the electronic records system is proven if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it. This creates a presumption of reliability for the business records of a person who is not a party to the legal proceeding, where the person claiming the record as evidence did not control the making of the record. This prevents organizations from contracting out their computer data processing or record management program, then claiming that what are in fact their own records are someone else's records.

Section 31.4 permits the federal government to make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures. To date, the federal government has not passed any of these regulations.

Section 31.5 provides that, to determine if an electronic record is admissible in court, evidence of the use of standards may be considered by a court. Section 31.5 does not make it mandatory for an organization to use recognized standards but it makes them relevant to the question of admissibility in court. Section 31.5 does not specify any specific standards to be considered. The test in section 31.5 is that the court may consider "any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document." It is up to the person or organization to prove these elements to the court. Some common industry standards are those released by the Canadian General Standards Board. For example for records, the Canadian General Standards Board has issued the following standards: *Microfilm and Electronic Imaging as Documentary Evidence*[80] and *Electronic Documents As Documentary Evidence*[81]. As previously discussed, other relevant standards include the ISO standard for records, *Information And Documentation (Records Management)*.[82]

Section 31.6 provides that the presumptions and other specified matters in sections 31.2-31.5 may be proven by a written affidavit. Section 31.6 does not specify who should give the affidavit. The person or organization seeking to admit the evidence will need to determine who is the most reliable and persuasive witness to give the affidavit. That person may be the records manager or other management personnel. This is especially important since section 31.6 also gives the opposing party the chance to cross-examine in court, the person giving the affidavit. The purpose of cross-examination is to test the truthfulness of the evidence.

[80] CAN/CGSB-72.11-93.
[81] CAN/CGSB-72.34.
[82] ISO/15489-1 and ISO/15489-2.

Section 31.7 provides that sections 31.1 to 31.4 do not affect any rule of law relating to the admissibility of evidence, except the rules relating to authentication and best evidence.

Section 31.8 sets out specified definitions for use in sections 31.1-31.6.

3.5.5. Judicial Interpretation of Electronic Records

In the Canadian legal system, decisions of the Supreme Court of Canada are binding on all courts across Canada, including the provincial courts of appeal.

Unlike other types of litigation, like criminal law, there are not as many judicial decisions interpreting the application of electronic records, RIM or records retention.

Overviews of seven recent cases that have interpreted electronic records, records management or records retention are provided below for your information.

1. In the Supreme Court of Canada leading case of *Dagg v. (Minister of Finance*) (1997), an applicant sought access to employment information held by the federal government. The Supreme Court of Canada held that, in the definition of "record" under the *Privacy Act*, "records" should not be interpreted as meaning only an entire particular document.[83] Under any practical, contextualized definition, "record" would refer to a specific piece of information under the control of a government institution, regardless of whether that piece is located within a large "document".[84]

2. Recently, in *R. v. Owen* (2003), the Supreme Court of Canada affirmed this practical, contextualized approach taken in the *Dagg* case.[85] The Supreme Court of Canada reflected in the wording of the evidence statutes. In the *Owen* case, in the context of hospital records, the Supreme Court of Canada held that:

> Nursing notes and hospital records have routinely been admitted for more than 30 years as *prima facie* proof of the truth of their contents under the hearsay exception for business records: *Ares v. Venner*, [1970] S.C.R. 608, *per* Hall J., at p. 626:

[83] [1997] 2 S.C.R. 403, http://scc.lexum.umontreal.ca/en/1997/1997rcs2-403/1997rcs2-403.html.
[84] *Ibid*., Para. 80.
[85] [2003] 1 S.C.R. 779, http://scc.lexum.umontreal.ca/en/2003/2003scc33/2003scc33.html.

> Hospital records, including nurses' notes, made contemporaneously by someone having a personal knowledge of the matters then being recorded and under a duty to make the entry or record should be received in evidence as *prima facie* proof of the facts stated therein.[86]

3. In BC, *British Columbia (Superintendent of Family and Child Services) v. Hughes,* (1995), the British Columbia Supreme Court found that the definition of "record" was broadly defined in section 29 of the British Columbia *Interpretation Act* and affirmed that the contents of section 29 should be interpreted in their ordinary usage.[87]

4. In *Her Majesty the Queen v. Rojas* (2003), consistent with the Supreme Court of Canada's holding in the *Dagg* case, the British Columbia Supreme Court held that a map qualifies as a business record such that it is admissible pursuant to section 30 of the *Canada Evidence Act*.[88] One of the reasons for this, the court found, was that in section 30 of that Act, the definition of "record" includes the whole or any part of any book, document, paper, card type or any other thing on or in which information is written, recorded, stored or reproduced.[89]

5. In *R. v. Hall* (1998), the British Columbia Supreme Court held that copies of computer printouts qualify as business records such that they are admissible pursuant to section 30 of the *Canada Evidence Act*.[90]

To date, the provisions of the *Canada Evidence Act* for electronic records have had some judicial interpretation in the lower courts in Canada.

6. Section 31.1 has been interpreted by the Alberta provincial court in *R. v. Bellingham* (2002).[91] In the *Bellingham* case, the Crown prosecutor sought to introduce lottery printouts as evidence to support the charge of theft of lottery tickets. The Alberta provincial court found that, while section 31.1 applied, the Crown had not fulfilled its burden of proof under section 31.1 because there was no evidence from anyone connected with the Lottery Authority to prove that the computer printouts were what the Crown purported them to be.[92]

---

[86] *Ibid*., Para. 58.
[87] 1995 CanLII 1746, http://www.canlii.org/bc/cas/bcsc/1995/1995bcsc11636.html.
[88] 2003 BCSC 1072 (CanLII), http://www.canlii.org/bc/cas/bcsc/2003/2003bcsc1072.html.
[89] *Ibid*., Para. 4.
[90] 1998 CanLII 3955, http://www.courts.gov.bc.ca/jdb-txt/sc/98/16/s98-1603.txt.
[91] 2002 ABPC 41 (CanLII), http://www.canlii.org/ab/cas/abpc/2002/2002abpc41.html.
[92] *Ibid*., Para. 26.

7. Section 31.5 has been interpreted by another Alberta provincial court in *R. v. Gratton* (2003).[93] In the *Gratton* case, the Crown prosecutor sought to introduce the data results from a piece of technology, a sensing diagnostic module located inside the defendant's vehicle. The Crown wanted to admit the results of this technology in order to prove that the defendant was speeding. The defendant was charge with several motor vehicle offenses under the *Criminal Code of Canada*. The Alberta provincial court found that this technology evidence was inadmissible. The Alberta court found that this technology evidence required expert opinion to establish "the nature, proper operation, and evaluation of this technology and its reliability, including a method for falsification of erroneous information provided".[94] The Alberta court found that since the police officer was not such an expert, the evidence did not meet the requirements set out in sections 31.1 to 31.8 of the *Canada Evidence Act* and the technology evidence was inadmissible.

3.5.6 Canadian General Standards Board *Electronic Documents As Documentary Evidence*

As noted above, the Canadian General Standards Board standard, *Electronic Documents As Documentary Evidence*, is a standard that organizations may choose to follow in implementing their records management program for electronic records.

Section 31.5 of the *Canada Evidence Act* gives legal recognition that the use of a standard by a person or organization is relevant to determine if an electronic record is admissible in court. Where section 31.5 applies, the *Electronic Documents As Documentary Evidence* standard may be used by an organization.

While the *Electronic Documents As Documentary Evidence* standard has not yet been recognized in Canadian statutes, the Canadian General Standards Board's standard, the *Microfilm and Electronic Imaging as Documentary Evidence*, has.[95]

The *Electronic Documents As Documentary Evidence* standard reflects the principles contained in sections 31.1-31.8 of the *Canada Evidence Act*. The *Canada Evidence Act* provides a statutory exception from the hearsay rule to admit business records, including electronic records, into evidence.

[93] ABQB 728 (CanLII), http://www.canlii.org/ab/cas/abqb/2003/2003abqb728.html.
[94] *Ibid*., Para 121.
[95] See regulations under the Canadian *Custom Act* [R.S., 1985, c. 1 (2nd Supp.)]: Customs Brokers Licensing Regulations (SOR/86-1067) (s.17(4)), Imported Goods Records Regulations (SOR/86-1011) (s.5) and the Persons Authorized to Account for Casual Goods Regulations (SOR/95-418) (s. 8).

The *Electronic Documents As Documentary Evidence* standard provides that a procedures manual required by a by-law or policy of the organization should be used by an organization to meet the evidentiary standards for admissibility of electronic records. Recall that in the *Bellingham* and *Gratton* cases reviewed earlier, the court refused to admit electronic records because there was a lack of expert or other witness evidence to support the electronic records system. Having the procedures manual standing as an "eyewitness" can be used by an organization to prove that the organization has a reliable, authentic and trustworthy electronic records system and that electronic records should be admitted in evidence in a court of law.

Further, the manual can be an "eyewitness" to prove that the organization has created records in the usual and ordinary course of business and followed its records management policies. This includes implementing its record retention schedule, which results in the destruction of electronic records in the usual and ordinary course of business.

3.6 Partnership with Information Technology

As a result of the blended world of hard copy and digital record formats, the best strategies for managing records include building alliances and partnerships with the staff responsible for computing and information technology. Records and information technology staff share common problems that may have solutions through records management best practices. For example, the government IT staff may be struggling with storage or capacity issues, such as having to store and maintain too many e-mail messages. At the same time, the records management staff require retention schedules to be applied to e-mail messages in the same way as with hard copy documents. How do the two groups get together to manage these common problems?

An American attorney and writer, Randolph A. Kahn, has described the new reality for information management compliance as "a battle between the way we did things yesterday and the way that the courts, regulators, boards expect us to do things today, a battle between emerging technology tools and burgeoning compliance criteria".[96] He makes the analogy that information management is like boot camp. He describes "information warriors" as having four quadrants of battlefield concern: information technology, legal, business and records management. Within the IT quadrant, he suggests that policy should drive technology, and that information warriors, as he describes them, should be involved throughout the IT management processes, including evaluation, acquisition, configuration, management and decommissioning.

[96] Randolph Kahn, and Barclay T. Blair, *Information Nation Warrior: Information Management Compliance Boot Camp*, (Association for Information and Image Management, 2005), p. 4.

Whether one agrees with this "warrior" vision or not, it is now a reality of business practice that the two groups work together with management to resolve these matters of common concern. Joint efforts will ensure fully compliant recorded information management systems. How this cooperation comes about will depend to a large extent on the working relationship and line of responsibility for these functions. As mentioned earlier, frequently the records and IT staff report to the different managers. A reorganization to bring the two groups together will help with the coordination and communication. If not, a team-based approach is ideal, where any new technology purchases are selected with representatives or advocates for the records management requirements. Likewise, when implementing or revising records management foundation practices, representation from the IT group will ensure that information technology management perspectives will also be considered.

3.7 Life Cycle Management of Electronic Records

The most practical way to highlight the specific requirements of electronic records is to take the principles of life cycle management, as outlined in the standards, and speak directly to the issues associated with electronic records at each phase.[97] As one of the Information Management Manual Advisory Committee members has stated, "take baby steps to ensure that there is a coherent set of practices".[98] If we examine each of the stages, the additional requirements for electronic records are evident. As with paper records, preservation of the life cycle metadata of electronic records must be retained to ensure future interpretation and trustworthiness of the electronic records, despite changes in technology over time.

3.7.1 Creation Phase

Individual workers create records as part of their specific duties. This practice now takes place in a digital environment, generally in programs on all desk tops, or within specific applications such as financial or mapping software. Whatever the application, the creation phase is where the record keeping activities are undertaken under the custody and control of the creator. So, two challenges are present. First, the worker must name and save the document ("file") so that it can be retrieved later. Second, this method must be intuitive and clear enough so that, long after the time the document has been created, another worker can find the document. Most electronic systems will automatically generate a number or some other identifier. However, the identifier is usually not clear enough for us to be certain about the content of the document. Therefore, for

[97] CAN/CGSB-72.34, see Section 6 Establishing a Records management system (RMS) program, p. 16 which outlines the full requirements of managing electronic records through the life cycle.
[98] LGMA Survey 2006.

later retrieval, document naming practices are necessary to create a uniform approach, and ensure that all staff follow the same logic or method. The document name will include not only the subject or function of the document but some other elements to provide a precise identifier, such as a form number. Using a common naming convention means that later, when a document is required, it can be readily retrieved and the name will help to ascertain the relevance of the retrieved document. Recommended document naming practices are included as Appendix C. In addition, the data about the document or file (metadata) are also important elements that ensure we have retrieved the correct item.

First Nations governments should ensure that, where possible, staff use electronic forms and templates. Templates and electronic forms provide organizations with tools for standardizing the design of business processes and the collection of data. These tools enable the automation of processes that were formerly labour intensive and error prone. Electronic forms will also facilitate the processing of information and the maintenance of privacy or confidentiality of personal information.

3.7.2 Registration/Capture

When an electronic document is complete, and ready to be saved as a record, it is declared ready by the creator, and captured in some way into the record keeping system. This capture process, unlike the "to be filed" basket where we place our hard copy records for processing, involves several other decisions:

- is this a valid record, created by an authorized person, and required for saving?
- is it the complete (correct, current) version?
- are there attachments that need to be incorporated as part of the whole record?
- are there non-records associated with this, e.g. drafts, and where do these non-records go?
- where does this record get saved? What other records are related to this one?

Electronic records management software applications provide tools at this stage, as most of the products operate with the "secure electronic repository" feature. This feature will take a declared record and "lock it". This means that any future actions are both authorized and audited. Such software applications often "auto populate" or automatically fill in key fields. These fields include author, date and system application, without effort from the creator to add these extra fields of information.

For organizations without a records management application, business rules will assist users. The rules should define what are records, when to save electronic documents and where to place the documents in the directory structure. See the section below describing the organization of directories for filing and saving electronic records.

3.7.3 Use/Maintenance/Retrieval

At this stage, when organizational staff are retrieving and using records, the key challenge with digital records is finding them. (This may also be true with hard copy records, but the additional challenge with digital forms is that they are invisible!) The greatest benefit for controlled processes at the creation and capture phases is that staff can later find the requisite documents, and be certain that they are the correct versions of the documents required.

All digital records and metadata are searchable. So, for many staff, using a search term such as subject or author will find records. At this stage, the staff benefit from the precision of work in the first phases above. Documents having file names will be easier for staff to identify. Documents placed in the correct directories of topics that match the classification structure will have a context that enables searchers to evaluate the relevance of the documents they find against the search criteria they were using.

We can see with relative ease the difference between versions of hard copy documents, and we can also see when modifications have taken place. These distinctions are not so easy to discern with electronic documents. The integrity of the electronic record must be protected, and most electronic records applications will provide this assurance. Integrity means the reliability and trustworthiness of records. Where there is no software application, staff can ensure that documents are saved as "read only" versions. This removes the risk of unauthorized modifications once the record has been registered.

The greatest challenge for use of electronic records lies with the security and permission structures that most network architecture imposes. If a record is assigned to a creator's own workspace as a storage location, this situation will frustrate use, as another searcher with different permissions will be unable to find or access the required document. Shared directories that are available for work groups or staff across the organization ensure that information is readily accessible after the fact. Consequently, business rules that create "open" access to electronic records in First Nations government, with very specific exceptions for the classes of records ("land, labour, legal") that must be treated as confidential, will enable use and sharing of information when it is required for business functions.

Routine back up of active electronic information is a best practice to protect IT systems from loss of data. This routine backup process requires copies to be made at planned intervals. This backup process creates a second set of records which ideally are copied, stored offsite, and recopied as need be for the sole purpose of protecting the content of the IT records. When duplicate sets of back up data are retained, more redundancy is built into the system.

3.7.4 Disposition/Deletion

How do we dispose of electronic records? Generally, users hit a "delete" key and there will be a series of system processes to delete the pointers to the data. In some cases, the metadata is deleted but the data remains or vice versa. In other cases, there are processes for overwriting, which will obliterate the data and metadata. One method described by IT staff is to remove data from a server onto CD storage platters, then break the platters, obliterating the storage media as well as the data.

The challenge with disposition is that staff must follow authorized procedures to ensure that approved disposal will happen according to records retention and disposition processes. Complex retention schedules may make the retention and disposal process for electronic records difficult. As a result, some IT staff may fall back to the principle of keeping information until the longest retention period expires. Ideally, a streamlined retention process will enable the logical storage of digital records by retention date.

When electronic records must be retained as archival records or for longer time periods, a physical transfer or "migration" of data is required. Like boxing and storing paper records offsite, this transfer of custody or format must happen in a manner that still enables retrieval or recopying of the record when a future need arises. Also, plans and strategies to protect stored electronic records should include backup systems and maintenance procedures.[99]

3.7.5 Preservation

According to professional archivists, the concept of digital archives is an oxymoron, a contradiction of terms, as digital media and the means to create digital media are constantly upgrading, changing and not stable. There is currently a large body of research being conducted around the world to determine the means and mechanisms by which digital records may be retained to ensure their accessibility and retrieval over time.[100]

[99] ISO/TR15489-2, Section 4.3.7.3 Digital Storage, p. 19.
[100] See, The University of British Columbia, Inter PARES (International Research on Permanent Authentic Electronic Records in Electronic Systems Project), http://www.interpares.org.

The lack of standardized languages in which to create archival documents, for example, XML or PDFA, leaves digital records vulnerable to obsolescence, unable to be read in the future when new languages are created. Storage media, including CDs and DVDs, are also perishable when new formats are created, despite claims by manufacturers. While the recording surfaces are more stable than magnetic media and have a longer life expectancy, these storage devices are still no prescription for long term storage.

Archival advice[101] at the time of this writing is to watch for announcements from the research community but at this time, no definitive standards have yet been developed to ensure availability of electronic records over time. As a further caution, it is recommended that if source documents are converted to another media, for example, scanned into PDF format, the original documents be saved and stored. Microfilm continues to be recommended as a secure storage medium over the long term. Archivists recommend that when converting source materials to a digital format, organizations should also create a microfilm version of the materials. Microfilm, stored in the proper conditions, is considered an archivally secure media, and is readily converted back to hard copy, or migrated to another media format.

3.7.6 Quality Assurance and Audit Trails

An additional program requirement in the information life cycle of electronic records is the requirement for Quality Assurance and Audit Trails. The Quality Assurance Program (QAP) "monitors and judges the records management system, including the quality control operations."[102] Audit trails provide details "of the storage date of the information, the movement of information from medium to medium, and the evidence of the controlled operation of the records management system."[103]

3.8 Managing Records in Directories

Organizing electronic information is similar to that of organizing paper records. For First Nations governments who are beginning to assert control over electronic records, this can be the first step to improve practices by providing a set of directories on a network that mirror the classification structure included in this manual.

[101] LGMA Survey 2006.
[102] CAN/CGSB-72.34, Section 7 Quality Assurance Program, p. 28.
[103] *Ibid*., Section 8 Audit Trail, p. 29.

Usually, within a computer's storage system (hard drive or network), files are organized into directories that are created and managed by the computer application that created them. Examples include My Documents in MS Office, which uses different extensions to denote Word, Excel, Power Point and Outlook. A directory is really like a table of contents for the application, and depending upon the storage capacity, may have the opportunity for various subdirectories, each storing files of a particular type. For individual staff members, this hierarchical arrangement provides an opportunity to create individual subject folders and sub-folders to match the primary and secondary subjects from the records classification.

In a shared network environment, a filing hierarchy or tree structure can be set up along the same lines. Then, staff are able to electronically "drop and drag" their completed documents into designated folders, labeled according to the shared primary subjects they require.

Coordination between work groups and individual staff training are required to ensure that staff understand their responsibilities in this shared environment. In addition, business rules covering the following elements are necessary:

- document naming standards, so that all staff label electronic records in meaningful ways;
- "open" permissions, with limited exceptions, to enable staff to view, access and retrieve information;
- work group procedures to ensure staff understand when "completed" documents or files must be saved in the shared files;
- assigned responsibility to a "gate keeper" or records management staff member for the creation, modification, transfer or removal of records categories;
- periodic review or audit of the shared drives to ensure that electronic records are being saved according to business rules; and
- controlled procedures for the deletion or removal of records, apply retention practices as with paper records.

Staff who have implemented electronic records management software applications will attest that this work to set up shared filing in common directories is excellent preparation for the change management required when electronic records management ("ERM") systems are installed in organizations.[104]

[104] Greater Vancouver Regional District staff describing the preliminary work before they installed their electronic document system, Vancouver ARMA seminar, October 2004.

While directory management will work at the beginning stages of electronic records management, most network software will not have the capability to provide the security to ensure records integrity, nor the ability to audit the actions to "records" once saved.

3.9 Managing Electronic Mail

The use of e-mail represents one of the biggest changes in the way staff in today's organizations conduct business. In the survey of government staff, e-mail is identified as the number one electronic record format, and is generally the format causing the most difficulties. [105] The difficulties range from the misunderstandings about the record value of the messages to the variety of practices that staff may use to manage (or not) their messages. Generally, these will range from one extreme of keeping every message ever received or sent to the opposite extreme of deleting every message. In cautious organizations, staff are printing and filing copies of significant e-mail messages.

Best practices and standards for electronic mail management have now been developed that will be useful tools for municipal organizations to develop policies and procedures to manage this electronic tool and provide solutions to the difficulties with e-mail.[106]

3.9.1 Electronic Mail is a Record

Although it was intended to be a replacement for the facilitative inter-office memorandum, electronic mail has evolved into the primary vehicle by which business decisions are now made and communicated. Consequently, e-mail messages are records. E-mail messages include metadata about the messages, the attachments, the links and the threaded discussions.

Most organizations have a policy statement or business rule mandating that electronic mail messages and attachments created or received in the usual and ordinary course of business are the property of the organization and must be managed as business records. This mandate may also be an explicit statement within a records management policy, or it may be embedded in an employee code of conduct.

[105] LGMA Survey 2006. As one participant stated, "if the new LGMA manual does nothing more than incorporate good practices for managing e-mail, many problems will be resolved".
[106] Sources for best practices and standards include provincial and federal government information management standards, and ARMA/ANSI standards, including ARMA *Managing Electronic Messages as Records.* See also the list of resources in Appendix G of this manual.

Equally helpful to staff however, are the lists of the types of messages they will receive that are not business records, and that can be discarded as soon as their useful life is over. Examples of messages that are not business records include:

- transitory or fleeting messages;
- attachments that are duplicates;
- administrative or facilitative messages**,** for example, booking appointments, meeting rooms;
- messages included in the complete text of a subsequent message;
- copies received for information only; and
- personal messages.

3.9.2 Electronic Mail Responsibilities

Electronic mail records should be saved and filed in the same way as other electronic formats, and according to the subject or function of the message. Where there is no electronic records management software application in use, staff should be encouraged to organize their e-mail directories with the same folder and subfolder arrangements as the records classification. If common or shared drives and directories are available, then staff should follow the same practices as with other electronic records formats.

Other general principles to follow include:

- an author is responsible for managing e-mail messages that are sent internally;
- an originating author is responsible for managing a threaded internal e-mail message;
- a recipient is responsible for managing externally generated e-mail messages;
- a first person on a list of multiple recipients is responsible for managing an externally generated e-mail message; and
- workgroups of staff may designate an e-mail gatekeeper to save and file group messages.

Where staff use lap top computers, portable digital assistants or other portable devices to transmit or receive electronic messages, an important procedure should be observed. This procedure requires staff to include the regular removal or uploading to a central storage device, both to protect the content of messages, as well as to ensure that no information is lost if the device is misplaced or damaged.

3.10 Managing Digital Photographs

When collections of digital photographs have substantive records value, records management staff must ensure that processes are present to manage their integration into the records management systems.

In addition to the general factors for electronic records management already described, digital photographs pose several records management requirements. These include:

- Ensuring that adequate naming or coding of individual images is completed to facilitate retrieval;
- Ensuring that adequate compression or storage techniques are used that will retain the technical quality of the images, but will also reduce the storage capacity requirements.

Typically, most digital cameras will embed automatic metadata for images, including date taken. A unique identifying number is also assigned to each photograph as it is taken. When the images are uploaded from the camera to a computer, the processing software will usually create a folder, often again automatically dated, to "file" these photographs. Inside the date folder, the image names are generally in numeric sequence ("img7021.jpeg, img7022.jpeg", and so on). When no further indexing takes place, staff members must retrieve by date, opening and examining the images individually to find the specific photograph they are seeking. This exercise is very time consuming, especially if the search happens a long time after the photographs were taken. If a person other than the photographer is searching for the photographs, they may be unable to find any images.

To facilitate retrieval, a records management clerk or responsible staff member must move these images from the temporary date folder to their appropriate subject or topic file folder as soon as the uploading is complete. As well, the individual images should be renamed to be fully indexed, adding project names, permit names or other relevant data to facilitate staff retrieval and use of the images.

Digital images are much larger electronic documents than text documents. Compression of the images will "shrink" the size of the electronic image, and enable more storage on the server. The amount and type of compression should be reviewed with the information services staff to ensure that the image quality is not diminished. Generally speaking, less compression should be used with archival or permanent images to maintain clarity and quality of the images.

3.11 Managing Database Records

First Nations governments use electronic systems to support of many organizational functions. Consequently, many electronic records are created from structured tables or data elements within databases or electronic systems, such as financial information systems or geographic information systems. The data elements are retained in the database, and are updated or changed as required. For example, an employee record in a payroll system is maintained for the purpose of issuing employee pay every pay period. The database elements include employee name, employee number, date of hire and a variety of other data elements. These elements will change when conditions around the employee's pay change, such as when the employee moves from one pay grade to another, or enrolls in benefits.

The records associated with databases are usually:

- the input or source records. In our example, these will be the source documents such as employee enrollment forms that are required to enroll an employee into the payroll system, and
- the outputs or reports from the system. In the payroll system, these reports may be the pay advice statement given each pay period, the payroll register of all payroll issued for a pay period, and the annual T4 statement issued to the employee.

The input and output records are usually filed by subject or function with the records classification system. In addition, most organizations treat the entire database as one record, and assign a file code that is associated with the specific computer system application. The retention period is usually a conditional retention, e.g. retain until [number of years] after system is discontinued. The file description includes all of the documentation about the system.

The government of British Columbia uses an "Information System Overview" or ISO to fully describe an electronic system, and the comprehensive description includes the following elements:

- title of system
- ownership of system – department or workgroup responsible for the system
- purpose of the system – description of what it is used for
- system details – application, version, producer, upgrades or modifications
- data description – elements of the data, input records, system processes, out put records
- personal information banks
- legislation or specific mandate for which the information is collected or generated.

Further information about this method of filing and describing information systems can be seen in the *Recorded Information Management Manual (RIM)* of the government of British Columbia.[107]

3.12 Managing Web Content and Links

The creation and use of Internet websites by First Nations governments creates web publications as another electronic record format to be managed. The processes by which information is prepared, routed, posted and removed from web sites involves collaboration and work flow across all organization units. Consequently, issues such as privacy protection of web content, copyright ownership of web content and related matters may require organizations to issue specific policy statements or codes of acceptable conduct for web content and links.

Current management practices from the Government of Alberta focus on two specific aspects of web content management for records management issues: the metadata about the information being published, and the capture of any dynamic information as it is obtained through a web site.[108] These Alberta management practices are applicable to British Columbia. The metadata elements that all web documents should include, at minimum, are the following items:

- **Title** – a descriptive title for the document;
- **Description** – a metatag that is a short summary of web page content;
- **Keywords** – the topic of the resource, typically expressed as keywords or phrases that describe the subject or content of the resource;
- **Author** – the author and/or business unit; and
- **Key Dates** – the dates the document was created and revised.

It is recommended that staff regularly review their web sites from a records management perspective, to ensure that full and accurate records are captured and maintained. The capture of a record of web-based activity, together with the metadata, should occur at the time the resource is posted to the web site and the record created. However, it is also acknowledged that the extent of maintenance required to preserve the functionality of electronic records will need to be determined on an individual basis, as the underlying technologies vary, and change constantly.

---

[107] Policy #5-13-03 *The Information System Overview.* Policies and Procedures of the Corporate Information Management Branch, Ministry of Labour and Citizens' Services are found at http://www.mser.gov.bc.ca/CIMB.policy/default.htm.

[108] Alberta, Information Management Branch, "Managing Web Content," *Information Management*, March 2004, http://www.im.gov.ab.ca.

Staff should regularly monitor research being undertaken by various standards organizations. In the future, this research may provide records management standards to manage web content management that local governments can adopt for their web content.

3.13 Electronic Records Management Applications

Electronic records management applications (RMAs) are software applications designed to provide various types of computer-assisted control and management of many records management functions. Recent developments in technology have seen these products add functionality beyond the traditional records management functions. These traditional records management functions are: indexing, labeling, tracking active records, managing life cycles through retention schedules, and transferring and tracking of stored records. Industry convergence has resulted in integrated document management software capable of managing electronic, paper and other records format through single software interfaces. The term "content management" is now used to describe the ability to create, capture, manage and distribute information content of records.

3.13.1 Better, More Functional Tools

Whatever the terminology, these software tools are capable of integrating the management of diverse information formats and applying the records management principles to all types of records, whether paper, electronic or other formats. For records managers, these new tools represent a giant step forward in functionality, as most of these tools can work within the broad spectrum of required activities. Formerly, software applications might have strengths in certain records management functions, but be deficient in others, creating additional costs and implementation time. For example, the two separate worlds of electronic document management and electronic records management meant that an organization would be required to buy two separate software tools. One software tool would ensure the creation, security and capturing of electronic documents. The second software tool would apply life cycle management to the documents as records. Thankfully, those days are now past, and First Nations government staff will be able to select better tools as a result.

The records management functions of these products are varied. Although the changes in computer architecture and processing technology have an impact on the capabilities of the programs, the following is a brief listing of typical software features:

- Indexing of records on all media in active, inactive and archival systems;
- Maintaining on-line inventories of records;

- Developing retention schedules and maintenance programs, including tracking legal and regulatory requirements;
- Maintaining on-line retention schedules for flagging and processing of retention actions;
- Incorporating bar coding to track movement and use of hard copy records in all media;
- Generating of labels;
- Managing electronic images;
- Managing electronic documents; and
- Producing reports on diverse program activities.[109]

One of the greatest challenges now is to locate, evaluate, select and implement the "right" product for your environment. As one of the Toolkit Advisory Committee has advised, currently the development of a business case and review of the selection of software applications creates a lot of wasted effort between First Nations government organizations. However, since the range of capabilities and requirements for the successful implementation are so broad, that makes it difficult to identify one "best" application.

The intent here is to provide a set of guiding principles for First Nations governments considering or actively pursuing an electronic document and records management system. First Nations governments can incorporate these principles into their specific checklists for evaluation and consideration in any purchasing process.

3.13.2 Standards for Selecting Records Management Applications

As the products have evolved, offering more and different capabilities, First Nations governments are faced with the dilemma of what product to choose. At various times, the Canadian federal and provincial governments have reviewed products and these respective governments have recommended a single product for ministries to purchase. Other government agencies outside Canada have chosen to develop functional product standards.

Two of these government agencies that have developed influential functional product standards are the United States Department of Defense[110], and the European Commission.[111] Both of these

[109] Mark Langemo, *Winning Strategies for Successful Records Management Programs,* (Englewood, CO: Information Requirements Clearinghouse, 2002), pp. 56-59.
[110] United States, Dept. of Defense, "Design Criteria Standard for Electronic Records Management Software Applications," DoD 5015.2-STD Records Management Application Design Criteria Standard, *Defense Information Systems Agency, Joint Interoperability Test Command Records Management Application,* June 2002, http://jitc.fhu.disa.mil/recmgt/standards.html. The Joint Interoperablity Test Site provides a list of all products currently certified.
[111] European Commission, "Model Requirements For The Management Of Electronic Records: MoReq Specification," *Electronic Document and Records Management,* March 2001, http://www.cornwell.co.uk/moreq.html.

agencies have these functional product standards that define operating requirements. Software vendors who meet these requirements are certified by either the United States Department of Defense or the European Commission. In practice, these standards permit software purchasers to be guided to those vendors bearing the certification stamp from either the United States Department of Defense or the European Commission. While these two government agencies have no relationship to business practices in British Columbia, their standards have driven the RIM marketplace to develop products that meet their acceptable records management requirements.

3.13.3 How to Select the "Right" Application

At the beginning of any process to select software applications, the first step is to review organizational requirements. Purchasing rules may require staff to build a business case, developing the cost justification and requirements for the organization. In developing the justification, staff must answer the question "why do we need this product?" The answer is that the product needs to facilitate the required processes and controls to ensure that records are reliable, have integrity, will be available over time, secure and protected, and admitted as evidence in court. However, there may be other specific records management business processes to be established. A team comprising various users, IT and records staff is most effective for developing the requirements and business case, since this team will be able to represent all the organization's requirements.

Organizational readiness is crucial. These applications are not substitutes for sound records management practices. As preparation, and at the beginning of a records management program, the local government should have adopted the classification scheme and retention schedule. All records management applications will require these fundamental program elements to be configured within the application. Without these, a records management application cannot be implemented. Policies and processes for records management should already be in place, with staff trained and all users knowledgeable in records management requirements.

Visits to peers and successful program installations will identify what other local government organizations are using, successfully and also with difficulty. A list of requirements created by the local government should cover all aspects of the RIM program requirements.

3.13.3.1 The Request for Proposals

Generally, there are least three sets of requirements that have to be defined in any request for quotations or proposals that a local government may release into the marketplace:

- The general operating environment, including the number of users and the reporting structure;
- The records management requirements, including the functions that this system must perform, and any specific considerations such as compliance with freedom of information legislation; and
- The computing environment, including the network, architecture and system components, as well as other large enterprise systems will need to communicate with the records management application.

As part of the selection process, proponent vendors should provide detailed information, including, but not limited to:

- Proof of their performance to meet the specific needs of the local government;
- History and financial structure;
- Customers for references, and possible site visits;
- Local representation and post sales support; and
- Detailed pricing of all of the elements that their system will require to meet performance requirements, including licensing costs, installation costs, modules or components, extra hardware or servers required, training costs, documentation costs, and on-going help and support.

A site visit by vendors to the local government offices is good practice. This enables vendors to show their system using in-house records. Organizations may require vendors to sign a non-disclosure agreement, if confidential information may be seen as part of the sales process.

The request for proposals should be directed to the key vendors as well as to other prospective purchasers that are usually provided with requests for proposals.

An evaluation process that covers these elements, as well as specific reviews by the First Nations government team, will ensure that the local government will have a comprehensive evaluation and fair ranking for each of the vendors who submit proposals.

By following these recommendations, it is hoped that a successful purchase is accomplished, with a vendor prepared to work with the local government for a successful implementation.

3.13.4 Implementation and Operational Issues

The challenging part of the purchase of software begins with the implementation of the product. The most successful implementations are phased in, using a pilot or test group to work through the specific issues that will arise.

Many software applications are designed with specific functionality and distinctly different training for key groups. These key groups include: information technology administration, records administration, and end users.

Training and change management strategies for staff are crucial. Consequently, from the outset, it is better to take time, and work with groups to resolve installation and work related issues. Implementation issues generally will include questions about legacy records in paper form, templates or in older applications.

4. Summary

The purpose of a recorded information management program is to:

- Provide the right information to the right person at the right time at the lowest possible cost to the organization;
- Facilitate compliance with current legislation;
- Systematically control records from creation to final disposition;
- Ensure that records can be admissible in court as evidence; and
- Protect the organization from risk.

RIM programs in First Nations government will provide a strong foundation for the work of staff in all areas of responsibility. When implemented according to the standards and best practices of RIM, the records within the custody of the government will be available when needed for staff work. In addition, the records within the records management system will meet all standards of authenticity, reliability and trustworthiness, so that the records will be available for users as long as the records have value to the organization.

The RIM program requires continued support from senior management, as well as continued management of operating activities. These continued efforts will ensure that the program is dynamic and that it matches the First Nation government responsibilities and requirements for its recorded information.

Index

Note: References are to manual page numbers

Appendices:

- **A – Model Records Management Bylaw**
- **B – Forms and Samples**
    1. **Information Survey Form**
    2. **Sample Filing Procedures**
    3. **Transitory Records**
    4. **Filing Equipment Standards**
    5. **Sample File Closing, Storage and Destruction Procedures**
- **C. – Document Naming Conventions**
- **D – Glossary**
- **E – References and Links**

Volume 2:

- **F – Records Classification and Retention Schedule**
- **G – Legal Citation Listing**

Appendix A – Model Bylaw

MODEL RECORDS MANAGEMENT BYLAW

INTRODUCTION

This Model Records Management Bylaw is offered as a model bylaw for governments who choose to use it. Use of this model bylaw is voluntary. This model bylaw is for general information purposes only and is not intended to provide legal advice or opinion of any kind. The law referred to in this model bylaw is current as at the date of this writing. First Nations governments intending to rely on this information, should use the relevant official paper versions of the statutes and regulations. Prior to using this model bylaw, First Nations governments should seek competent legal advice to ensure that the information contained in the model bylaw and relevant law applicable to it are current and applicable to the specific needs of the local government.

An explanation of each provision of this model bylaw is provided.

LEGISLATIVE FRAMEWORK

Respecting the duty to keep records, local governments may come under the jurisdiction of one or more of these British Columbia statutes:

- *Community Charter*, S.B.C. 2003, c. 26;
- *Local Government Act*, R.S.B.C. 1996, c. 323;
- *Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c. 165;
- *Mountain Resort Municipality of Whistler Act*, R.S.B.C. 1996, c. 407;
- *Society Act*, R.S.B.C. 1996, c. 433; or
- *Vancouver Charter*, S.B.C. 1953, c. 55.

Community Charter

Section 148 of the *Community Charter*, S.B.C. 2003, c. 26 requires that a municipal officer must be assigned the responsibility to ensure that accurate minutes of the meetings of the council and council committees are prepared. Further this officer must ensure that the minutes, bylaws and other records of the business of the council and council committees are maintained and kept safe and that access is provided to records of the council and council committees, as required by law or authorized by the council.

Section 149 of the *Community Charter* requires that a municipal officer must be assigned the responsibility of financial administration, ensuring that accurate records and full accounts of the financial affairs of the municipality are prepared, maintained and kept safe.

Local Government Act

Section 196 of the *Local Government Act*, R.S.B.C. 1996, c. 323 requires a regional district board to pass a bylaw establishing officer positions regarding the powers set out in section 198 and 199 of this Act.

Section 198 of the *Local Government Act* requires that an officer must be assigned the responsibility to ensure that accurate minutes of the meetings of the board and board committees are prepared. Further, this officer must ensure that the minutes, bylaws and other records of the business of the board and board committees are maintained and kept safe and that access is provided to records of the board and board committees, as required by law or authorized by the board.

Section 199 of the *Local Government Act* requires that an officer must be assigned the responsibility of financial administration, ensuring that accurate records and full accounts of the financial affairs of the regional district are prepared, maintained and kept safe.

Freedom of Information and Protection of Privacy Act
Section 6(1) of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 requires that the head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

In addition, section 6(2) of the *Freedom of Information and Protection of Privacy Act* further requires the head of a public body to create a record for an applicant if the record can be created from a machine readable record in the custody or under the control of the public body using its normal computer hardware and software and technical expertise and creating the record would not unreasonably interfere with the operations of the public body.

Section 30 of the *Freedom of Information and Protection of Privacy Act* requires that a public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Section 77(a) of the *Freedom of Information and Protection of Privacy Act* requires a local public body to pass a bylaw or other legal instrument by which the local public body acts to designate a person or group of persons as the head of the local public body for the purposes of this Act.

Section 77(b) of the *Freedom of Information and Protection of Privacy Act* permits a local public body to authorize any person to perform any duty or exercise any function under this Act of the person or group of persons designated as the head of the local public body.

Section 77(c) of the *Freedom of Information and Protection of Privacy Act* permits a local public body to set any fees the local public body requires to be paid under section 75.

Mountain Resort Municipality of Whistler Act
Section 3 of the *Mountain Resort Municipality of Whistler Act*, R.S.B.C. 1996, c. 407 provides that, subject to the *Resort Municipality of Whistler Act,* the *Community Charter* and the *Local Government Act* apply to the Resort Municipality of Whistler unless they are inconsistent with the *Resort Municipality of Whistler Act* or regulations made under the *Resort Municipality of Whistler Act*.

Society Act
Section 11(1) of the *Society Act*, R.S.B.C. 1996, c. 433 provides that a society must ensure that all of its documents, including its financial records, are kept at the address of the society. Section 11(2) of that Act provides an exception to this requirement. Section 11(2) of that Act provides that, despite subsection (1), the directors of a society may by resolution permit some of the documents, including its financial records, to be kept at places in British Columbia other than the address of the society. Section 11(3) of that Act requires that a resolution passed under subsection (2) must describe the documents to which it applies and the place they are to be kept. Section 11(4) of the *Society Act* provides that any such resolution has no effect until a copy of it is filed with the registrar.

From time to time, organizations registered under the *Society Act* may request that local governments take custody and control over the organization's records. Section 11(2) of that Act does not permit a society to cede to local governments the custody and control of all of its records. Section 11 requires all records, wherever located, to be kept in British Columbia.

Vancouver Charter
Section 221 of the *Vancouver Charter*, S.B.C. 1953, c. 55 requires that the City Clerk must ensure that an accurate record of all resolutions, transactions, and other business and proceedings of the Council and its committees are prepared, and must safely preserve and keep custody of all such records.

RELEVANT STANDARDS
The following standards were considered in developing this model bylaw:

- International Standards Organization ("ISO"), International Standard Information And Documentation — Records Management -Part 1 15489-1 (2001);

- ISO, Information And Documentation — Records Management —Part 2 Guidelines TR15489-2 (2001); and

- Canadian General Standards Board, *Electronic Documents As Documentary Evidence* (CAN/CGSB-72.34-2005).

RELEVANT STATUTES
In addition to the statutes noted above, the following statutes were considered in developing this model bylaw:

- *Canada Evidence Act*, R.S.C. 1985, c. C-5;
- *Document Disposal Act*, R.S.B.C. 1996, c. 99;
- *Electronic Transactions Act,* S.B.C. 2001 c. 10;
- *Evidence Act*, R.S.B.C. 1996, c. 124;
- *Interpretation Act*, RS.B.C. 1996, c. 238; and
- Uniform Law Conference of Canada *Uniform Electronic Evidence Act*.

MODEL RECORDS MANAGEMENT BYLAW

Contents

Title
1. This bylaw may be cited as the Records Management Bylaw.

Interpretation
2. Interpretation
In this bylaw:

"Designated Officer" means the person designated and authorized to act on behalf of the organization to manage and maintain the records management system;

"record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

"records management system" includes a system used by the [Name of local government] to manage the records of the [Name of local government] from record creation through to records disposal;

EXPLANATION:
The definition of "Designated Officer" is used to ensure that the records management system is duly designated and authorized by the local government and properly managed and maintained. Local governments may wish to add a designated occupational title—for example, "City Clerk" or "Records Officer" in place of "Designated Officer", wherever "Designated Officer" appears in the Model Records Management Bylaw.

The definition of "record" used is the same one used by the *Freedom of Information and Protection of Privacy Act* as set out in Schedule 1 to that Act. This definition of "record" includes both paper and electronic records. Most, if not all, local governments must comply with the *Freedom of Information and Protection of Privacy Act*, including its definition of "record". Some local governments may see fit to adopt "record" as defined by the *Freedom of Information and Protection of Privacy Act*. Some local governments may set fit to adopt definitions other than the legal definition of "record" to reflect other operational values and uses made of their respective records in the usual and ordinary course of business.

The definition of "records management system" permits use of a paper based or electronic record-keeping system or a combination of the two. Under the definition of "records management system", the records management system used by a local government must use a life-cycle approach to records management.

Records Management System Established
3. The records management system of the [Name of local government] is established and authorized.

OR THE ALTERNATIVE

The records management system currently used by the [Name of local government] is authorized.

EXPLANATION:
In order to comply with applicable legislation, the records management system must be authorized by the governing body of the local government. If an existing records management system is employed, then the alternative provision should be used so that the existing system in use is authorized by the governing body of the local government.

Compliance with Records Management System
4. All records in the custody and control of the employees of the [Name of local government] are the property of the [Name of local government]. All records of the [Name of local government] must comply with this records management system and this bylaw. All employees and management of the [Name of local government] must comply with this bylaw.

EXPLANATION:
Once authorized by the governing body of the local government, both records and staff of the local government must comply with the records management system and this compliance is recognized by the bylaw. That records are the property of the local government clarifies that the organization as a whole is owner of the property of the records, not specific departments or groups within the organization.

Designated Officer
5. The Designated Officer is responsible for the management and maintenance of the records management system. The Designated Officer is authorized to manage and maintain the records management system.

EXPLANATION:
In order to comply with applicable legislation in the *Community Charter*, *Local Government Act*, or the *Freedom of Information and Protection of Privacy Act,* the local government must designate a specific person, with express authority, to take responsibility to manage and maintain the records management system.

Manual of Procedures and Policy
6. The Designated Officer is authorized to create and maintain a manual of procedures and policy (the "Manual"). Records of the [Name of local government] are created, accessed, maintained and disposed of only as provided by the Manual.

[ADDITIONAL PROVISION]

The Manual must provide for management of the records of the [Name of local government] and include provisions regarding:

- **the creation and organization of records, including records not authorized for creation;**
- **the collection of records (including records not authorized for collection);**
- **access to records;**
- **disclosure of records;**
- **maintenance of records;**
- **retention of records;**
- **security of records;**
- **storage of records;**
- **preservation of records;**
- **disposal of records; and**
- **any other matter(s) the Designated Officer authorizes to be included in the Manual.**

EXPLANATION:
The manual of procedures and policy functions as evidence to prove the integrity and authoritativeness of the records made in the usual and ordinary course of business and in the records management system. This evidence may be submitted as evidence admissible in a court of law or other legal proceedings in order for the local government to defend or prosecute a legal claim. Applicable law, evidentiary rules and records management standards require that the following elements are necessary in order for records to be admitted as evidence and to prove facts in court or other legal proceedings:

- integrity;
- authoritativeness; and
- records made or kept in the usual and ordinary course of business.

Integrity of the records management system is required to prove that the system is operating properly. Integrity is also necessary to prove that records from the records management system were made in the usual and ordinary course of business and capable of being retrieved from the records management system. Integrity of the system also proves that this system is trustworthy and reliable and it produces true copies of original records.

Authoritativeness proves that the records generated by the records management system are what they purport to be: a true record of authorized data coming from the organization.

Under the evidence statutes, records must be made or kept in the usual and ordinary course of business in order to qualify as an exception to the rule that makes hearsay inadmissible in court and other legal proceedings.

The additional provision in the Model Records Management Bylaw that recommends what must be in the manual of procedures and policy, may be of assistance to local governments who wish to enshrine in the bylaw specific mandatory components for this manual. The list of components in this additional provision is consistent with the life cycle of records approach to records management. Annex C of the Canadian General Standards Board, *Electronic Documents As Documentary Evidence* (CAN/CGSB-72.34-2005) provides an example of necessary components that may be placed in a manual of procedures and policy.

Integrity and Authenticity Maintained
7. The records management system must maintain the integrity and authenticity of records made or kept in the usual and ordinary course of business.

EXPLANATION:
See Explanation for section 6 for the explanation regarding integrity, authenticity of the records of the local government made or kept in the usual and ordinary course of business.

Authorization to Amend Manual
8. The Designated Officer is authorized to amend the Manual.

EXPLANATION:
To ensure that the manual of procedures and policy proves that the records management system complies with applicable laws, this manual must be keep up to date and complete. As a result, this manual must be amended from time to time. This provision authorizes the designated officer of the local government to amend this manual to ensure it is current and complete.

Compliance with Law
9. The records management system must comply with the Manual, applicable laws and any provincial, national or international standards adopted for use and contained in the Manual.

EXPLANATION:
This provision is necessary in order for the local government to prove that it complies with law so it can produce its records as evidence in legal proceedings. Further, this provision expressly provides that any relevant provincial, national or international standards may be adopted for use and be contained in the manual of procedures and policy.

Severability
10. If any section, subsection, paragraph, subparagraph or clause of the Records Management Bylaw is for any reason held to be invalid by the decision of any court of competent jurisdiction, such decision does not affect the validity of the remaining portions of the Records Management Bylaw.

EXPLANATION:
In the event of a court order striking down a part of the Records Management Bylaw as invalid, this provision provides that such a court order does not invalidate the entire Records Management Bylaw.

Coming into Effect
11. The Records Management Bylaw comes into effect upon adoption.

EXPLANATION:
The Records Management Bylaw comes into effect upon adoption by the local government.

MODEL RECORDS MANAGEMENT BYLAW

SHORT VERSION:
RECORDS RETENTION AND DISPOSAL PROVISIONS ONLY

INTRODUCTION

Instead of enacting the Model Records Management Bylaw, local governments may choose to use this Short Version of the Model Records Management Bylaw to only govern records retention and disposal. As such, specific provisions for records retention and disposal contained in this Short Version may be used as a stand alone bylaw.

Local governments may also integrate these Short Version records retention and disposal provisions as separate provisions into the Model Records Management Bylaw. Sections 1 to 3 and sections 7 and 8 in this Short Version are the same as those corresponding sections in the Model Records Management Bylaw. To integrate these Short Version records retention and disposal provisions, sections 4 to 6 below can be renumbered and added after section 9 in the Model Records Management Bylaw.

Section
1. Title
2. Interpretation
3. Records Management System Established
4. Records Retention Schedule
5. Designated Officer
6. Disposal Ordered by Designated Officer
7. Coming into Effect

Title
1. This bylaw may be cited as the Records Retention and Disposal Bylaw.

Interpretation
2. Interpretation
In this bylaw:

"Designated Officer" means the person designated and authorized to act on behalf of the organization to manage and maintain the records management system;

"record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

"records management system" includes a system used by the [Name of local government] to manage the records of the [Name of local government] from record creation through to records disposal;

EXPLANATION:
The definition of "record" used is the same one used by the Records Retention and Disposal Bylaw and the *Freedom of Information and Protection of Privacy Act* as set out in Schedule 1 to that Act.

As with the definition in the Model Records Management Bylaw, the definition of "records management system" permits use of a paper based or electronic record-keeping system or a combination of the two. Under the definition of "records management system", the records management system used by a local government must use a life-cycle approach to records management.

Records Management System Established
3. The records management system of the [Name of local government] is established and authorized.

OR THE ALTERNATIVE

The records management system currently used by the [Name of local government] is authorized.

EXPLANATION:
In order to comply with applicable legislation, the records management system must be authorized by the governing body of the local government. If an existing records management system is employed, then the alternative provision should be used so that the existing system in use is authorized by the governing body of the local government.

Records Retention Schedule
4. The records retention schedule must prescribe the period of time that records are kept to meet the operational, legal, regulatory, financial or other requirements of the [Name of local government] (the "Records Retention Schedule"). The Records Retention Schedule must also provide instructions as to the manner and time of the disposition of a record.

EXPLANATION:
This provision sets out the required components of the records retention schedule.

Designated Officer
5. The Designated Officer is designated and authorised to prepare, review, amend and manage the Records Retention Schedule.

EXPLANATION:
In order to comply with applicable legislation in the *Community Charter*, *Local Government Act*, or the *Freedom of Information and Protection of Privacy Act,* the local government must designate a specific person, with express authority, to take responsibility to manage and maintain the records management system, including the records retention schedule. This provision provides the designated officer with power to prepare, review, amend and manage the records retention schedule.

Disposal Ordered by Designated Officer
6. When the Designated Officer determines that the retention period for a given record described in the Records Retention Schedule has ended, the Designated Officer may order the record to be destroyed or otherwise disposed of in accordance with the instructions in the Records Retention Schedule.

EXPLANATION:
This provision provides the designated officer with the authority to destroy of dispose of given records according to the terms of the records retention schedule.

Coming into Effect
7. The Records Management Bylaw comes into effect upon adoption.

EXPLANATION:
The Records Management Bylaw comes into effect upon adoption by the local government.

Appendix D: – Glossary

GLOSSARY OF TERMS

As with any area of specialized professional work, records management employs terminology that requires explanation. The following terms are used frequently in describing program activities and are derived from ISO 15489 – 1, ISO/TR 15489 – 2 *Information and Documentation – Records Management – Part 1 General, and Part 2 Guidelines,* and CGSB 72.34-2005 *Electronic Records as Documentary Evidence.*

Authenticity – authenticity of a record, so that it can be proven to be what it purports to be, to have been created or sent by the person purported to have created or sent it, and at the time purported to have been created or sent

Classification – systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system

Conversion – process of changing records from one medium to another or from one format to another

Destruction – process of eliminating or deleting records, beyond any possible reconstruction

Disposition – range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities and other instruments

Document – record information or object which can be treated as a unit

Integrity – Integrity of the records management system means that this system is operating properly, is trustworthy and reliable and it produces true copies of original records; integrity of records proves that records from the records management system were made in the usual and ordinary course of business and capable of being retrieved from the records management system

Life cycle – stages of life for a record, including to ensure the capture, filing and availability of records for business purposes, the systematic and controlled disposal of records once their value

to the organization has ceased, and the preservation and continued availability over time of those records with enduring value to the organization

Metadata – data describing context, content and structure of records and their management through time

Migration – act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability

Procedures manual – reference source for staff responsible for creating, receiving, preparing, processing, storing and disposing of records

Records – information created, received or maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business

Retention schedule – provides a timetable and consistent procedures for maintaining the organizations records, moving the records to inactive storage when appropriate and destroying records when they are no longer valuable to the organization

Appendix E: – References and links

Records and Information Management (RIM)
Best Practices
References and Standards
Current to July 1, 2006 (including dates of access for Internet links)

RIM Program Content:

ARMA International. *Information Management: A Business Imperative – FAQs for Corporate Executives and Decision-Makers*. Lenexa, KS: ARMA International, 2005. http://www.arma.org.

---. *RIM Industry Competency Requirements: A Baseline for Education*. Lenexa, KS: ARMA International, 2000.

Hofman, Hans. "Standards: Not 'One Size Fits All." *Information Management Journal,* May-June, 2006.

International Standards Organization (ISO). *Information and Documentation – Records Management – Part 1: General* (ISO/15489-1). First Edition. Geneva, Switzerland: ISO, 2001. http://www.iso.org.

---. *Information and Documentation – Records Management – Part 2: Guidelines* (ISO/TR15489-2). Geneva, Switzerland: ISO, 2001. http://www.iso.org.

---. *Information and Documentation – Records Management Processes – Metadata for Records – Part 1: Principles* (ISO/TS 23081-1). First Edition. Geneva, Switzerland: ISO, 2004. http://www.iso.org.

Library and Archives of Canada. "Information Management Capacity Check: Tools and Methodology." *Information Management*. July 2003. http://www.collectionscanada.ca/information-management/002/007002-2003-e.html.

National Archives of Australia. "DIRKS – A Strategic Approach to Managing Business Information. Step G – Implementation of a Recordkeeping System." *Recordkeeping.* September 2001 (Revised July 2003). http://www.naa.gov.au/recordkeeping/dirks/dirksman/dirks.html.

Saffady, William. *Records and Information Management: Fundamentals of Professional Practice*. Lenexa, KS: ARMA International, 2004.

Active Records Management:

ARMA International. *"What is Records Management? Why Should I Care?"* Lenexa, Kansas: ARMA International, 2005.

ARMA International Standards Task Force. *Establishing Alphabetic, Numeric and Subject Filing Systems.* ANSI/ARMA 12-2005. Lenexa, KS: ARMA International, 2005. http://www.arma.org.

Bennick, Ann. *Active Filing for Business Records*. Lenexa, KS: ARMA International, 2000.

British Columbia. Ministry of Labour and Citizens' Services. Corporate Information Management Branch. *ARCS Online (Administrative Records Classification) 2003 Edition. (ARCS On-line Version 1.4.* http://www.mser.gov.bc.ca/CIMB.

Canadian Standards Association. *A Model Code for the Protection of Personal Information,* (embedded in *Personal Information Protection and Electronic Documents Act* (PIPEDA)). CAN/CSA-Q830-96. Mississauga, Ontario: Canadian Standards Council, 1996. http://www.csa.ca.

Hofman, Hans. "Standards: Not 'One Size Fits All'." *Information Management Journal,* May-June, 2006: 40.

Langemo, Mark. *Winning Strategies for Successful Records Management Programs*. Englewood, CO: Information Requirements Clearinghouse, 2002.

Lyman, Peter and Hal R. Varian. "How much information?" *University of California-Berkeley School of Information Management and Science*. 2003. http://www.sims.berkeley.edu/research/projects/how-much-info-2003.

Swartz, Nikki. "Dealing with Disaster." *Information Management Journal*, July-August, 2006: 29 – 34.

Records Retention And Scheduling:

Anson-Cartwright, Ronald M., Robert T. Hollingshead and J. Timothy Kennish. *Records Retention: Law and Practice*. 3rd ed. Toronto: Thomson Carswell, 2005.

ARMA International Standards Task Force. *Retention Management for Records and Information.* ANSI/ARMA 8-2005. Lenexa, Kansas: Association for Records Managers and Administrators, 2005. http://www.arma.org.

Canada Revenue Agency. "Books and Records Retention/Destruction." Income Tax Information Circular #IC78-0R41. *Forms and Publications*. June 2005. http://www.cra-arc.gc.ca/E/pub/tp/ic78-10r4/ic78-10r4-e.html.

---. "Electronic Record Keeping." Income Tax Information Circular #IC05-1. *Forms and Publications*. June 2005. http://www.cra-arc.gc.ca/E/pub/tp/ic05-1/ic05-1-05e.pdf.

---. "GST/GST Memorandum: 15.1 General Requirements for Books and Records." *Forms and Publications*. Revised June 2005. http://www.cra-arc.gc.ca/E/pub/gm/15-1/15-1-e.pdf.

---. "GST/GST Memorandum: 15.2 Computerized Records." *Forms and Publications*. Revised June 2005. http://www.cra-arc.gc.ca/E/pub/gm/15-2/15-2-e.pdf.

Electronic Records Management:

Alberta. Information Management Branch, "Naming Conventions for Electronic Documents." *Electronic Information Management*. August 2005. http://www.im.gov.ab.ca/index.cfm?page=imtopics/eim.html.

ARMA International. *Requirements for Managing Electronic Messages as Records.* Lenexa, KS: ARMA International, 2004. http://www.arma.org.

British Columbia. Corporate Information Management Branch, Ministry of Labour and Citizens' Services. Policy #5-13-03 *The Information System Overview.* http://www.mser.gov.bc.ca/CIMB.policy/default.htm.

Canada Revenue Agency. "Electronic Record Keeping." Income Tax Information Circular #IC05-1. *Forms and Publications*. June 2005. http://www.cra-arc.gc.ca/E/pub/tp/ic05-1/ic05-1-e.html.

Canadian General Standards Board. *Micrographics and Electronic Images as Documentary Evidence* (including Amendment 1, April 2000). CAN/CGSB-72.11-93. Ottawa: Canadian General Standards Board, 2000. http://www.techstreet.com.

Canadian General Standards Board. *Electronic Records as Documentary Evidence.* CAN/CGSB-72.34. Ottawa: Canadian General Standards Board, 2005. http://www.techstreet.com.

European Commission. "Model Requirements For The Management Of Electronic Records: MoReq Specification." *Electronic Document and Records Management*. March 2001. http://www.cornwell.co.uk/moreq.html.

United States. Dept. of Defense. "Design Criteria Standard for Electronic Records Management Software Applications." DoD 5015.2-STD Records Management Application Design Criteria Standard. *Defense Information Systems Agency, Joint Interoperability Test Command Records Management Application*. June 2002. http://jitc.fhu.disa.mil/recmgt/standards.html.

Freedom of Information and Privacy:

British Columbia. Ministry of Labour and Citizens' Services of British Columbia. Information Policy and Privacy Branch. "Guidelines for Determination of Fee Estimates." n.d. http://www.lcs.gov.bc.ca/privacyaccess/main/fee_estimates.htm.

Office of the Information and Privacy Commissioner for British Columbia. "A decision by the Insurance Corporation of British Columbia (ICBC) to withhold records from an applicant and the adequacy of ICBC's search for records." Order No. 170-1997. *Orders*. http://www.oipcbc.org/orders/1997/Order170.html.

---. "A decision by the Ministry of Attorney General to refuse an individual access to some of his Human Resources records." Order No. 218-1998. *Orders*. http://www.oipcbc.org/orders/1998/Order218.html.

---. "Annual Report 2004/2005." *Annual Reports*. http://www.oipcbc.org/publications/annual_reports/2005AR/OIPC_Annual_Report_web.pdf.

---. "Faxing And Emailing Personal Information." (February 2005). http://www.oipcbc.org/pdfs/public/fax-emailguidelines(Feb2005).pdf.

---. "Public Surveillance System Privacy Guidelines (OIPC Reference Document 00-01 January 26, 2001)." *Advice*. http:// www.oipcbc.org/advice/VID-SURV(2006).pdf.

---. *Ministry Of Children And Family Development*, [2002] B.C.I.P.C.D. No. 53. *Orders*. http://www.oipc.bc.ca/orders/Order02-52.pdf.

---. "Public Surveillance System Privacy Guidelines (OIPC Reference Document 00-01 January 26, 2001)." *Advice.* http:// www.oipcbc.org/advice/VID-SURV(2006).pdf.

---. “Request for Access to Records of the Insurance Corporation of British Columbia.” Order No. 12-1994. *Orders*. http://www.oipcbc.org/orders/1994/Order12.html.

Select Legal Resources:

British Columbia Legislation

Community Charter, S.B.C. 2003, c. 26.

Document Disposal Act, R.S.B.C. 1996, c. 99.

Electronic Transactions Act, S.B.C. 2001 c. 10.

Evidence Act, R.S.B.C. 1996, c. 124.

Interpretation Act, RS.B.C. 1996, c. 238.

Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.

Local Government Act, R.S.B.C. 1996, c. 323.

Mountain Resort Municipality of Whistler Act, R.S.B.C. 1996, c. 407.

Society Act, R.S.B.C. 1996, c. 433.

Vancouver Charter, S.B.C. 1953, c. 55.

Canadian Legislation

Canada Evidence Act, R.S.C. 1985, c. C-5.

Custom Act, [R.S., 1985, c. 1 (2nd Supp.)

Custom Act Regulations. Customs Brokers Licensing Regulations (SOR/86-1067). Imported Goods Records Regulations (SOR/86-1011). Persons Authorized to Account for Casual Goods Regulations (SOR/95-418).

Personal Information Protection and Electronic Documents Act, 2000, c. 5 (PIPEDA).

Privacy Act (R.S., 1985, c. P-21).

Uniform Electronic Evidence Act of the Uniform Law Conference of Canada

General Law and Case Law

British Columbia (Superintendent of Family and Child Services) v. Hughes, 1995 CanLII 1746 (B.C S.C.). http://www.canlii.org/bc/cas/bcsc/1995/1995bcsc11636.html.

Dagg v. (Minister of Finance) (1997), [1997] 2 S.C.R. 403. http://scc.lexum.umontreal.ca/en/1997/1997rcs2-403/1997rcs2-403.html.

Her Majesty the Queen v. Rojas (2003), 2003 BCSC 1072 (CanLII). http://www.canlii.org/bc/cas/bcsc/2003/2003bcsc1072.html.

R. v. Bellingham, 2002 ABPC 41 (CanLII). http://www.canlii.org/ab/cas/abpc/2002/2002abpc41.html.

R. v. Gratton, 2003 ABQB 728 (CanLII). http://www.canlii.org/ab/cas/abqb/2003/2003abqb728.html.

R. v. Hall (1998), 1998 CanLII 3955. http://www.courts.gov.bc.ca/jdb-txt/sc/98/16/s98-1603.txt.

R. v. Owen (2003), [2003] 1 S.C.R. 779. http://scc.lexum.umontreal.ca/en/2003/2003scc33/2003scc33.html.

The Honourable Chief Justice of British Columbia McEachern, Allan (as he then was). "Chapter 10." In Legal Compendium." *Legal Compendium*. 1999. www.courts.gov.bc.ca/legal_compendium/Chapter10.asp.

References for Records and Information Management on the Internet, including Links

General Records Management Information

- Association for Records Managers and Administrators (ARMA), http://www.arma.org.
- ARMA, Vancouver Chapter, http://www.armavancouver.org. See "hot topics" on member side of portal, including information protection and disaster management.
- Institute of Certified Records Managers, http://www.icrm.org.
- Alan S. Zaben's Records Information Management Resource List, http://www.infomgmt.homestead.com.

Information Policy/Management Sources

- Alberta Information Management Branch, http://www.im.gov.ab.ca.
- Archives Canada, http:www.archivescanada.ca.
- British Columbia Ministry of Labour and Citizens' Services, Corporate Information Management Branch, http://www.mser.gov.bc.ca/CIMB.
- Library and Archives of Canada, http://www.collectionscanada.ca.
- National Archives and Records Administration of the United States, http://www.archives.gov/records-mgmt.
- National Archives of Australia, http://www.naa.gov.au.
- The National Archives of the United Kingdom, http:www.nationalarchives.gov.uk.
- Treasury Board of Canada, Chief Information Officer Branch, http://www.tbs-sct.gc.ca/cio-dpi/pols_e.asp?who=/cio-dpi.

Electronic Records Management

- Cohasset Associates, http://www.cohasset.com. See annual conference, "Managing Electronic Records".
- International Congress of Archives. See http://www.wien2004.ica.org.
- The Sedona Conference, http://www.thesedonaconference.org.

Access to Information and Protection of Privacy

- British Columbia Ministry of Labour and Citizens' Services, Corporate Information Management Branch, http://www.mser.gov.bc.ca/privacyaccess/.
- British Columbia Freedom of Information and Privacy Association, http://www.fipa.bc.ca.

- Office of the Information and Privacy Commissioner for British Columbia, http://www.oipcbc.org.
- Office of the Information Commissioner of Canada, http://www.infocom.gc.ca.
- Office of the Privacy Commissioner of Canada, http://www.privcom.gc.ca.

Legal Resources

Canadian Department of Justice Laws (for Laws of Canada), http://laws.justice.gc.ca/en/index.html.

Canadian Legal Information Institute (CANLII), http://www.canlii.org.

Courts of British Columbia, http://www.courts.gov.bc.ca.

Federal Court of Canada, http://www.fct-cf.gc.ca/index_e.shtml.

Revised Statutes and Consolidated Regulations of British Columbia, http://www.qp.gov.bc.ca/statreg.

Supreme Court of Canada, http://scc.lexum.umontreal.ca/en/index.html.

Uniform Law Conference of Canada, http://ulcc.ca.

Related Professional Associations

- Archives Association of British Columbia (AABC), http://www.aabc.bc.ca.
- Association for Information and Image Management (AIIM), http://www.aiim.org.
- Association of Canadian Archivists (ACA), http://archivists.ca.

Research Sites

- The University of British Columbia, Inter PARES (International Research on Permanent Authentic Electronic Records in Electronic Systems Project), http://www.interpares.org.

Vital Records and Disaster Management

- British Columbia Ministry of Public Safety and Solicitor General, Provincial Emergency Program, http://www.pep.bc.ca.
- DRI International (Disaster Recovery Institute), http//:www.drii.org.
- Disaster Recovery Journal, http://www.rothstein.com/drjbooks.
- Public Safety and Emergency Preparedness Canada (PSEPC), http://www.psepc.gc.ca.

Manual continues with Volume 2:

Appendix F – Classification and Retention Schedule
Appendix G – Legal Citation Listing

End of Volume 1