Digital Records Pathways:
Topics in Digital Preservation

Module 2: Developing Policy and Procedures for Digital Preservation

Table of Contents

Table of Figures

Digital Records Pathways: Topics in Digital Preservation

1 Preface

Digital Records Pathways: Topics in Digital Preservation is an educational initiative developed jointly by the International Council on Archives (ICA) and the International Research on Permanent Authentic Records in Electronic Systems Project (InterPARES). It offers training to archivists and records professionals in the creation, management and preservation of authentic, reliable and usable digital records. The program assumes that the user has a solid grounding in basic concepts of records management and archival theory, and builds on that knowledge.

Consisting of eight independent modules, *Digital Records Pathways* addresses the theoretical and practical knowledge needed to establish the framework, governance structure and systems required to manage and preserve digital records throughout the records' lifecycle.. Each module addresses a specific topic of relevance to the management and preservation of digital records. The program is provided free of charge on the ICA website at www.ica.org/.

1.1 About the ICA and InterPARES

The ICA and InterPARES are committed to establishing educational materials for the continuing education of archivists and records managers, to build upon foundational knowledge, disseminate new findings, and to equip archivists and records professionals with the necessary specialized knowledge and competencies to manage and preserve digital records.

The International Council on Archives (ICA) (www.ica.org) is dedicated to the effective management of records and the preservation, care and use of the world's archival heritage through its representation of records and archives professionals across the globe. Archives are an immense resource. They are the documentary by-product of human activity and as such an irreplaceable witness to past events, underpinning democracy, the identity of individuals and communities, and human rights. But they are also fragile and vulnerable. The ICA strives to protect and ensure access to archives through advocacy, setting standards, professional development, and enabling dialogue between archivists, policy makers, creators and users of archives.

The ICA is a neutral, non-governmental organization, funded by its membership, which operates through the activities of that diverse membership. For over sixty years ICA has united archival institutions and practitioners across the globe to advocate for good archival management and the physical protection of recorded heritage, to produce reputable standards and best practices, and to encourage dialogue, exchange, and transmission of this knowledge and expertise across national borders. With approximately 1500 members in 195 countries and territories the Council's ethos is to harness the cultural

diversity of its membership to deliver effective solutions and a flexible, imaginative profession.

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) (www.interpares.org) aims to develop the knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form and provide the basis for standards, policies, strategies and plans of action capable of ensuring the longevity of such material and the ability of its users to trust its authenticity. The InterPARES project has developed in three phases:

InterPARES 1 (1999-2001) focused on the development of theory and methods ensuring the preservation of the authenticity of records created and/or maintained in databases and document management systems in the course of administrative activities. Its findings present the perspective of the records preserver.

InterPARES 2 (2002-2007) continued to research issues of authenticity, and examined the issues of reliability and accuracy during the entire lifecycle of records, from creation to permanent preservation. It focused on records produced in dynamic and interactive digital environments in the course of artistic, scientific and governmental activities.

InterPARES 3 (2007-2012) built upon the findings of InterPARES 1 and 2, as well as other digital preservation projects worldwide. It put theory into practice, working with archives and archival / records units within organizations of limited financial and / or human resources to implement sound records management and preservation programs.

1.2   Audience

The audience for this program includes archivists and records and information professionals interested in expanding their competencies in the management of digital records. Taken as a whole, the modules form a suite of resource materials for continuing professional education with particular focus on issues influencing the preservation of reliable, accurate and authentic digital records.

1.3   How to Use the Modules

Each module consists of theoretical and methodological knowledge and its practical application, illustrated through case studies and model scenarios. While the modules have been developed by InterPARES Team Canada, and are therefore illustrated with examples from the Canadian context, each module is customizable for a specific domain or juridical context. For wider applicability, they have been translated into the languages of the ICA partners.

The modules can be studied individually according to need and interest, or as a set, covering the range of competencies required. They can be self-administered by individuals, or offered through professional associations or workplace training. The modules also contain a number of templates that allow universities and professional associations to adapt and to

develop specific course curricula, on-site training materials for students and professionals on digital recordkeeping and preservation issues. Universities and professional associations are free to adapt the materials and develop their own context-specific course curricula and training kits.

1.4   Objectives

The modules have the following objectives:

- To provide educational resources based on cutting edge research in digital records issues to professional archival and records management associations for the benefit of their members;
- To provide archivists and records managers with the necessary theoretical knowledge as well as procedural and strategic skills to develop, implement and monitor a digital recordkeeping and/or a preservation program;
- To illuminate theoretical concepts with practical applications through real life examples drawn from case studies, anchored in specific administrative and technological contexts;
- To provide university programs with content and structure for courses on digital records management and preservation.

1.5   Scope

Digital Records Pathways: Topics in Digital Preservation consists of the following modules:

Module 1:   Introduction – A Framework for Digital Preservation
Module 2:   Developing Policy and Procedures for Digital Preservation
Module 3:   Organizational Culture and its Effects on Records Management Selection and Appraisal of Digital Records
Module 4:   An Overview of Metadata
Module 5:   From *Ad Hoc* to Governed – Appraisal Strategies for Gaining Control of Digital Records in Network Drives
Module 6:   E-mail Management and Preservation
Module 7:   Management and Preservation of Records in Web Environments
Module 8:   Cloud Computing Primer

Each module consists of some or all of the following components as appropriate:

- **Overview** of the topic and scope of the module;
- **Learning objectives** and expected level of knowledge upon completion;
- **Methodology** or the procedures to follow in order to apply the module;
- **Templates (where appropriate)** to facilitate the implementation of the module;
- **Case Study(ies)/Scenarios (where appropriate)** that provide real-world examples of module topic
- **Exercises** covering key learning points;

- **Review questions** to enhance comprehension and understanding of the topic;
- Additional **Resources** for the topic, including **readings, standards** and other **templates** for reference

Overview of the set			
1. A Framework for Digital Preservation 2. Developing Policy and Procedures for Digital Preservation			Foundational
3. Organizational Culture	4. An Overview of Metadata	5. Appraisal Strategies	General purpose
6. E-mail	7. Websites	8. Cloud Computing	Specific purpose
International Terminology Database			Foundational

1.6   International Terminology Database

The terminology used in the modules reflects common usage in archival and records management communities of practice. To ensure common understanding, and minimize potential confusion that may arise from regional or jurisdictional practice, all modules are supported by the International Terminology Database, available at http://www.web-denizen.com/. As well, certain specific terms are included in short glossaries in each module.

Module 2: Developing Policy and Procedures for Digital Preservation

2 Introduction

Every individual and organization creates records in the course of daily affairs. Records document transactions and provide the basis for future decision-making. We rely on the records we create to provide proof of our decisions and transactions, rights and responsibilities. In addition to being instruments of accountability, well managed, authentic, reliable records can also serve as important and trusted sources of information for memory and future decision-making. However, records that are not well managed may not withstand scrutiny when they are required as evidence of transactions or for accountability. To meet these goals, records must be created, maintained and preserved to be trustworthy, that is, reliable, accurate, and authentic, and they must remain accessible and usable over time and across technological change.

A digital preservation policy provides the framework for action and planning to ensure the long-term maintenance and preservation of an organization's records. Following a digital preservation policy through the records' active life will facilitate preservation over the long-term for inactive records; whether it is the creator who preserves the records, or a trusted third party.

2.1 Scope

Depending upon the policy framework within an organization, policy requirements pertaining to preservation may be incorporated into an existing records management policy, the policies governing the organization's programs and/or systems, or reflected in a stand-alone digital preservation policy. This module outlines policy development at a high level and can be utilized by both the record creating organization and, if different, the records' preserver.

2.2 Aims and Objectives

The objective of this module is to explain the purpose and benefits of a digital preservation policy and provide the knowledge and tools necessary to create such a policy. This module guides you in developing, writing and implementing an effective digital preservation policy within your organization and includes methodology for the development of policies in general, practical tools to aid in policy development, examples of existing digital preservation policies, and links to further resources to assist you in policy and procedure development.

2.3 Learning Outcomes

Upon completion of this module, you will be able to:

- Understand the purpose and benefits of a digital preservation policy and accompanying procedures;
- Distinguish between policy and procedures;
- Understand the fundamentals of digital preservation policy development – identify what needs to be included in (and excluded from) a digital preservation policy;
- Understand the issues that need to be considered when implementing a digital preservation policy;
- Have the foundational tools to carry out digital preservation policy development within your organization;
- Know where to locate additional information and resources that will aid in policy development and implementation.

2.4   What is policy?

A policy is a set of rules and/or principles that guide decision-making and actions in order to achieve desired outcomes for a particular topic or goal. Policy should be approved at a high level within an organization and:

- Be non-prescriptive;
- Technologically neutral;
- Support the governing structure and organizational culture of an organization.

Policy provides a framework that dictates the scope and requirements of procedures. It is situated within the broader context of the organization and aids in carrying out the organization's mandate. Policy does not outline particular actions; this is the role of procedures.

2.5   What are procedures?

Procedures are prescriptive actions or operations which, when performed, result in a prescribed result or outcome. Procedures are the implementable actions that enable policy to be put into practice. Procedures should be established and outlined for all stakeholders within an organization and reflect the policy's stated goals and requirements. Because procedures are context specific, they change more frequently than policy and are thus easier to change as required. Organizations often incorporate elements of procedures into policy; this module recommends that policy be kept at a high level. Procedures can then be developed within an organization to support policy and reflect the organization's specific needs and requirements.

2.6   What is Digital Preservation?

Organizations are creating an ever-increasing number of digital records. Unlike traditional records (e.g. on paper, film), digital records are vulnerable to loss and corruption. Because of the

Digital preservation is the process of maintaining digital materials across different generations of technology over time, irrespective of where they reside. (InterPARES)

9

speed of technological change, organizations have to consider issues of preservation of their digital records even while they are still in active use. In order to ensure records' authenticity, reliability and accessibility over time, organizations need to take into consideration issues of preservation at the time of creation. This means addressing the issue of preservation at the planning stage of program or system design - even before the records are created.

2.7   The purpose of a digital preservation policy

Several international research projects are currently researching solutions and building technological tools for digital preservation, however, technology is only part of the solution. In order to be effective, digital preservation should support an organization's goals and objectives through institutional frameworks and policies.

Fundamental requirements

A digital preservation policy should ensure that:

- Digital records are created and maintained authentic, and reliable;
- Digital records remain usable over time;
- Recordkeeping practices adhere to relevant standards and best practices;
- Records are maintained and preserved in accordance with any relevant regulatory requirements;
- Records identified for long-term preservation are capable of being preserved.

A digital preservation policy facilitates the effective management of digital records ensuring the organization is able to carry out its mandated functions. Continuing effective management of and access to digital records ensures they are available within an organization to support operations and decision-making.

Research into digital records has shown that it is not possible to preserve digital records, but only to maintain the ability to reproduce them. Records' authenticity, reliability and accuracy depend on a framework of specific requirements, and the capacity to maintain records' authenticity over time must be considered as the records are being created. InterPARES 2 developed a framework of principles guiding the creation of policies, strategies and standards that is flexible enough to be implemented in different national environments and balance cultural, social and juridical perspectives, and yet robust enough to serve as a solid foundation for any resultant policy document.

See Appendix A in Module 1: Introduction – A Framework for Digital Preservation for the complete Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records

These InterPARES principles should be situated within the context of an overarching policy objective that establishes the link between records and the business of the organization.[1] They apply to policy development whether your organization's primary focus is records creation or records preservation:

- Digital records must have fixed form and stable content,
- Digital components of records should be created so that they can be separately maintained and reassembled over time,
- Records should be created and maintained according to the purposes they must fulfill, and preserved according to the purpose and desired outcome of preservation, rather than in terms of available technologies,
- Records policies should address the issues of record reliability, accuracy and authenticity expressly and separately,
- A trusted record-making system (integrated business and documentary procedures and technology) should be used to generate records that can be presumed reliable,
- A trusted recordkeeping system should be used to maintain records that can be presumed accurate and authentic,
- Appraisal and preservation decisions should be embedded in all record-creating and recordkeeping activities,
- A trusted custodian should be designated as the preserver of a creator's records,
- All business processes that contribute to the creation and/or use of the records should be explicitly documented,
- Third-party intellectual property rights attached to the records should be explicitly identified and managed in the record-creating and recordkeeping systems,
- Privacy rights and obligations attached to the records should be explicitly identified and managed in the record-creating and recordkeeping systems,
- Procedures for sharing records across jurisdictions should be established on the basis of legal requirements,
- Reproductions made in the usual and ordinary course of business, or for purposes of preservation, have the same effect as the record's first manifestation and are considered authentic copies.

These principles are embedded in the methodology and template that follow.

---

[1] ISO 15489 (Management Statement: 2007) sets out the following objectives linking records with the business of the organization: 1) strategies, including effective conduct of business through informed decision-making; performance management; productivity improvement; consistency, continuity and quality assurance in management and operations; 2) operations, including responsive and accurate service delivery, resource management and cost control; 3) regulatory compliance, and legal protection and support; 4) accountability, corporate governance, financial and practice audits; 5) risk management, including security, reputation management, business continuity planning and implementation; 6) corporate values, including openness, safety, quality, integrity, respect and meeting expectations of external stakeholders; 7) corporate memory, including innovation through capture and reuse of organizational knowledge, and use of strategic knowledge to support business.

3   Methodology

3.1   Development of policy

The development of policy for the management and long-term preservation of digital records in an organization is guided by an action research methodology. This methodology is based on an iterative application of practices including data gathering, collaborative dialogue, and participatory decision-making.

Although this module focuses on the development of a digital preservation policy, the methodology that follows can be applied successfully to the development of a broader strategic plan for preservation, or adapted to any policy or procedure development. The workflow of data collection and analysis provides rich data about the organization (agency or office) and the records that it creates and maintains, and/or preserves. In the context of the discussion that follows, the workflow is presented primarily as a policy development tool, distinguishing between policies and procedures where appropriate or necessary.

The process for developing policy is established for each organization at the level of senior management or other administrative or regulatory body. There needs to be a process in place through which the policy can be developed and approved. Without this in place, even the best efforts at developing and implementing policy are likely to fail. Identification of the need for records management policy in general (and procedures governing digital records in particular) may come from the records manager or records management office, the business manager, or from senior management. Successful policy creation results from a collaborative team effort – records managers will have the greatest success if their business managers represent the need for policy to senior management.

Once the person or office seeking to initiate development of the policy has received approval from the necessary senior body, the following workflow will lead to development of a policy that ensures that:

- Digital records are created reliable and accurate, and maintained authentic,
- Digital records remain usable over time,
- Recordkeeping practices adhere to relevant standards and best practices,
- Records are maintained and preserved in accordance with any relevant regulatory requirements, and
- Records identified for long-term preservation are capable of being preserved.

More specifically, digital records governed by such a policy will be capable of fulfilling their business function regardless of the technology used to create, maintain and store them. They will have stable content and fixed form; they can be presumed reliable, authentic and

accurate throughout their life cycle; privacy and intellectual property rights will be explicitly identified and managed; and their use and continuing access will be assured.

Exercise:

- Identify the level at which policy development and approval occurs in your organization.

- What existing policies cover records management? If your organization has a records management policy, does it explicitly cover digital preservation?

The following workflow diagram outlines the process of development for a digital preservation policy.

```
                    ┌──────────────────┐
                    │  Initiate Policy │
                    │   Development    │
                    └──────────────────┘
                             │
   ┌──────────────┐   ┌──────────────┐
   │  Contextual  │◄──│   Conduct    │
   │ Analysis     │   │  Contextual  │
   │ Report       │   │   Analysis   │
   └──────────────┘   └──────────────┘
                             │
              ┌──────────────┴──────────────┐
       ┌──────────────┐           ┌──────────────┐   ┌──────────────┐
       │Review Current│           │Review Relevant│  │  Report on   │
       │ Policies and │           │ Standards &  │   │ Standards &  │
       │  Practices   │           │  Practices   │   │  Best        │
       └──────────────┘           └──────────────┘   │ Practices    │
                             │                        └──────────────┘
                    ┌──────────────┐
                    │ Conduct Gap  │     ┌──────────────┐
                    │Analysis betw.│────►│ Gap Analysis │
                    │Current & Best│     │   Report     │
                    │  Practices   │     └──────────────┘
                    └──────────────┘
                             │
            Yes      ◇ Need more  ◇
          ◄──────────   information?
                             │ No
                    ┌──────────────┐
                    │  Establish   │
                    │ required     │
                    │ policy       │
                    │ elements     │
                    └──────────────┘
                             │
                    ┌──────────────┐
                    │ Draft policy │
                    └──────────────┘
                             │
                    ┌──────────────┐
                    │Measure against│
                    │ requirements │
                    └──────────────┘
                             │
           No        ◇ Does it meet  ◇
          ◄──────────   the          
                         requirements?
                             │ Yes
                    ┌──────────────┐
                    │ Review with  │
                    │ stakeholders │
                    └──────────────┘
                             │
           No        ◇ Does it meet  ◇
          ◄──────────   the
                         requirements?
                             │ Yes
                    ┌──────────────┐
                    │ Present to   │
                    │ appropriate  │
                    │ authority for│
                    │  approval    │
                    └──────────────┘
                             │
           No        ◇ Is it         ◇
          ◄──────────   approved?
                             │ Yes
                    ┌──────────────┐
                    │    Policy    │
                    └──────────────┘
                             │
                    ┌──────────────┐
                    │    Policy    │
                    │ development  │
                    │  complete    │
                    └──────────────┘
```

Figure 1: Workflow for policy development

3.2   Workflow Diagram Narrative

The process of creating policy begins by identifying a need to govern conduct and practice through formal instruments. The responsible person or department will build a case for policy development that articulates that need, and positions the proposed policy in its organizational context. The case is then presented to the appropriate authorities. It is critical when developing policy to secure the commitment of all stakeholders. If the people who develop, apply, or monitor the policy are not committed to its implementation, the policy will not achieve its intended results, and be a continuing source of frustration.

The triggers that lead to the recognition and expression of the need for policy should come from a recognized business issue. This may involve multiple business functions or a single, perhaps central, business function. But the need, even if expressed generally, should always reflect a business perspective (e.g. the systems supporting an organization's major business purpose are generating digital records that need to be retained for legal and organizational reasons for extensive periods of time, and the organization wishes to develop policy to guide the process of retention and preservation.)

Once approval to develop the policy is received, the drafters begin by conducting research, identifying required policy outcomes, interviewing stakeholders, drafting, submitting for review, and revising the policy until it is ready for final approval and implementation.

1. Initiate Policy Development
The first step in developing policy is to conduct research that will allow the drafters to clearly state the goals and outcomes of the policy, embed it in a network of existing policies as necessary, and be contextually relevant in the organization. Research consists of conducting a contextual analysis, reviewing and researching current practice and industry best practices, and conducting a gap analysis to identify what must be included in the policy.

2. Conduct Contextual Analysis
A contextual analysis gathers information about the organization or department that will influence the policy or procedures being developed: its administrative structure; its legal and regulatory obligations with respect to its records; norms and standards which influence record creation; maintenance and use; its record creating and recordkeeping requirements and constraints, including the business culture of the organization, personnel constraints and technological constraints.
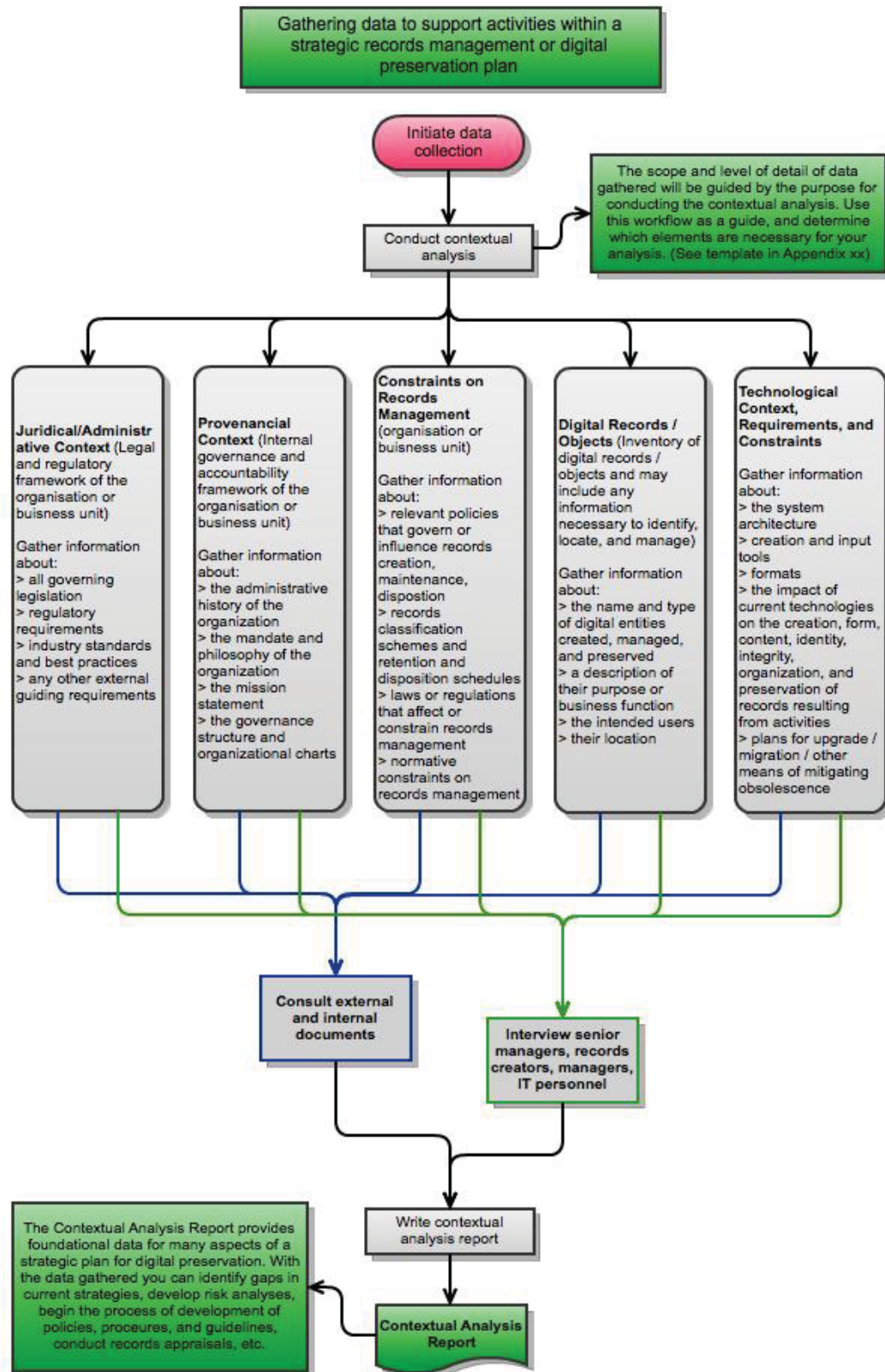
Gathering data to support activities within a strategic records management or digital preservation plan

Initiate data collection

Conduct contextual analysis

The scope and level of detail of data gathered will be guided by the purpose for conducting the contextual analysis. Use this workflow as a guide, and determine which elements are necessary for your analysis. (See template in Appendix xx)

Juridical/Administrative Context (Legal and regulatory framework of the organisation or buisness unit)

Gather information about:
> all governing legislation
> regulatory requirements
> industry standards and best practices
> any other external guiding requirements

Provenancial Context (Internal governance and accountability framework of the organisation or business unit)

Gather information about:
> the administrative history of the organization
> the mandate and philosophy of the organization
> the mission statement
> the governance structure and organizational charts

Constraints on Records Management (organisation or buisness unit)

Gather information about:
> relevant policies that govern or influence records creation, maintenance, dispostion
> records classification schemes and retention and disposition schedules
> laws or regulations that affect or constrain records management
> normative constraints on records management

Digital Records / Objects (Inventory of digital records / objects and may include any information necessary to identify, locate, and manage)

Gather information about:
> the name and type of digital entities created, managed, and preserved
> a description of their purpose or business function
> the intended users
> their location

Technological Context, Requirements, and Constraints

Gather information about:
> the system architecture
> creation and input tools
> formats
> the impact of current technologies on the creation, form, content, identity, integrity, organization, and preservation of records resulting from activities
> plans for upgrade / migration / other means of mitigating obsolescence

Consult external and internal documents

Interview senior managers, records creators, managers, IT personnel

Write contextual analysis report

The Contextual Analysis Report provides foundational data for many aspects of a strategic plan for digital preservation. With the data gathered you can identify gaps in current strategies, develop risk analyses, begin the process of development of policies, proceures, and guidelines, conduct records appraisals, etc.

Contextual Analysis Report

Figure 2: Conduct contextual analysis

17

See also Appendix A: Contextual Analysis

You will gather information through interviews and analysis of your organization's literature. Interview administrators and decision-makers, records managers and/or others responsible for the management of records. Read annual reports, work and strategic plans, legal documentation and legislation, and any other material that will help you best understand the framework within which the policy and procedures under development will function.

> Exercise:
>
> • Who are the key decision-makers you will interview first and what is the impact of their role in the organization on records management requirements? Consider managers in IT and legal departments.
>
> • What is the relationship between IT and records management personnel in your organization?

3. Conduct Review of Current Practices

Reviewing current practices will give you a comprehensive understanding of how records are created and managed currently in your organization. You will interview records creators and analyze any existing policies that govern and constrain records management.
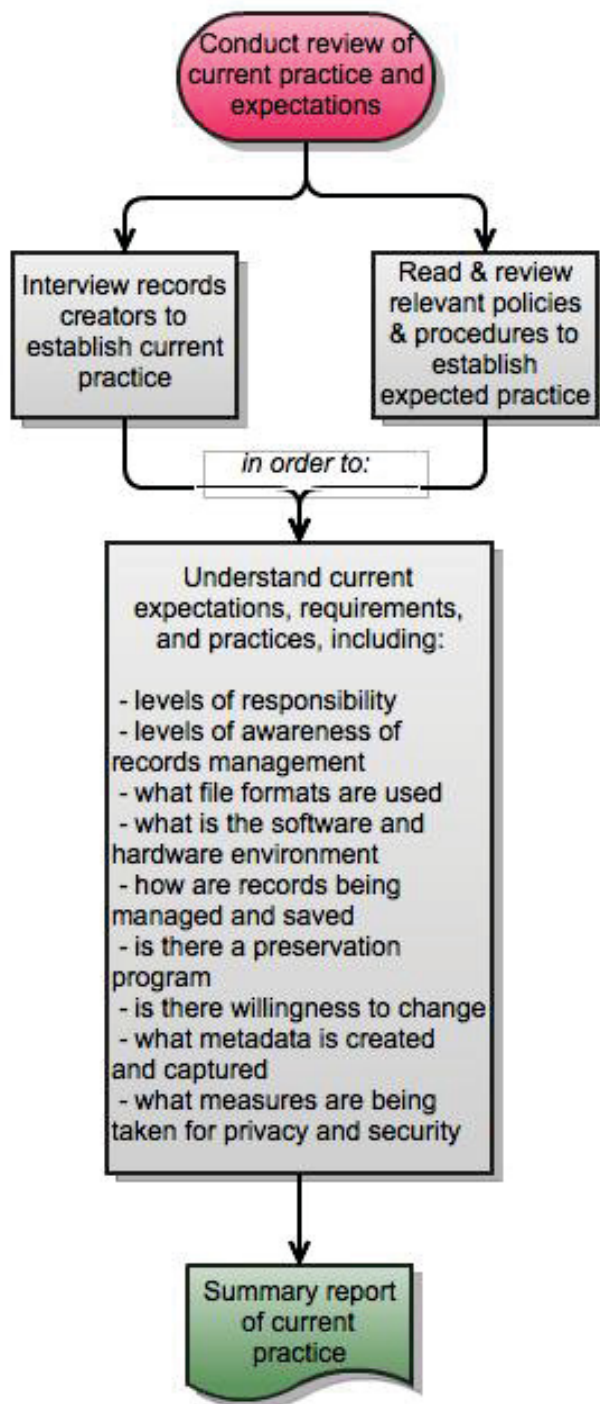
Figure 3: Review of current practice

See Appendix B for an outline of information you should have

4. Conduct Review of Relevant Standards / Best Practices

Examine all standards and best practices relevant to your organizational context. Identify the key points that are relevant for your organization and for which you wish to account in the policy or procedures under development. Digital preservation policy should account for key management strategies protecting records' authenticity, reliability, usability and accessibility, for as long as they are needed, either explicitly or implicitly (see point 5 below).

> Exercise:
>
> - What existing policies cover records management in your organization? Do any existing policies explicitly cover digital preservation?

5. Conduct Gap Analysis – Compare Existing Practices with Standards / Best Practices

Map your existing practices to best practice as outlined in the InterPARES 2 Creator and Preserver Guidelines and relevant standards under which your organization operates. This will help you identify gaps that can be remedied through policy and procedure development. If after conducting this step you need more information or clarification, return to previous steps.

Conduct gap analysis between existing practice & standards/best practice

List standards/best practices relevant to your organization/ jurisdiction

List current practices of your organization (summary report of current practice review)

in order to:

Identify gaps in the practices of your organization. Consider the following, including:

- ensure fixed form and stable content of digital objects to be preserved
- focus on the purpose of the records rather than the technology
- consider reliability, accuracy, and authenticity expressly and separately
- generate records within a trusted record making system
- use a trusted recordkeeping system
- consider preservation requirements
- designate a trusted custodian to preserve the records
- keep explicit documentation of all business processes
- identify and manage third-party intellectual property rights and obligations
- identify and manage privacy rights and obligations
- establish procedures for sharing records across jurisdictions
- establish procedures for managing copies

Gap analysis report

Figure 4: Gap analysis

See Appendices C and D for complete versions of the InterPARES 2 Creator and Preserver Guidelines

Your comparison should consider the following areas *(Note: the level of granularity is applicable to procedures rather than policy, however these elements must be considered when crafting broad policy statements)*:

Accessibility

- Choose software and hardware for interoperability,
- Choose software that is backwards compatible,
- Adopt official or *de facto* software standards,
- Fully document all choices and any customization,
- Choose widely used, non-proprietary, platform independent, uncompressed formats with freely available specifications where possible,
- Choose lossless compression when compression is required.

Fixity

- Digital records should have fixed form and stable content,
- Endow records with bounded variability (established fixed rules for the selection of content and documentary form that allow known, stable variations);
- Establish the elements of documentary presentation or form that are essential to the meaning of the records.

Identity

- Ensure the completeness of identity metadata:
  - Names of persons (author, writer, originator, addressee, recipient);
  - Title/subject (action or matter);
  - Documentary form (letter, report, etc.);
  - Digital presentation (format, wrapper, encoding, etc.);
  - Dates of creation and transmission;
  - Expression of documentary context (e.g., classification code, folder or directory, etc.);
  - Indication of attachments (if applicable);
  - Indication of copyright or other intellectual rights (if applicable);
  - Indication of the presence or removal of digital signatures;
  - Indication of other forms of authentication (e.g., corroboration, attestation, etc.)
  - Draft or version number (if applicable);
  - Existence and location of duplicate materials outside of the system (indicate which is the authoritative copy).

Integrity

- Ensure that digital materials carry information that will help verify their integrity,
- Integrity metadata:
  - Name of handling persons/office;
  - Name of office/person w/ primary responsibility for keeping (may be same as handling);
  - Indication of annotations;
  - Indication of technical changes to either material or application;
  - Access restrictions (if applicable);
  - Access privileges (if applicable);
  - Vital record (if applicable);
  - Planned disposition.

Organization

- Organize digital materials into logical groupings (classification scheme, identity metadata).

Authentication

- Use authentication techniques that foster maintenance and preservation of digital materials,
- Technology-independent vs. technology-dependent.

Protection

- Protect digital materials from unauthorized action.

Backup

- Protect digital materials from accidental loss and corruption,
- Develop a rigorous policy or routine that ensures your system is backed up daily,
- Choose and install the best backup technology for your situation.

Obsolescence

- Take steps against hardware and software obsolescence.

Awareness

- Consider issues around long-term preservation.

Exercise:

- Use the template provided in Appendix E to begin to map the required elements for digital preservation to your existing policies.

Exercise:

- Use the template provided in Appendix E to begin to identify required elements that must be addressed in new policy.

6. Establish Required Elements that Policy Must Cover

Decide how your policy will ensure that the elements necessary to enable creation, maintenance and preservation of authentic, reliable, accurate and accessible records are to be included. Outline the roles and responsibilities for personnel at all levels of accountability for records. Detail issues of training, risk assessment and compliance.

Establish required elements that policy must cover

Required policy elements including but not limited to:

- roles and responsibilities for personnel at all levels of accountability
- cooperation between RM and IT
- support of senior management
- adherence to legislation, regulations, professional associations requirements
- compliance
- risk assessment and risk management

Figure 5: Required elements of policy

7. Draft Policy for Review

Use the policy template (section 4) as a guide.

8. Measure Draft Policy against Requirements

Check the policy statements you have drafted against the requirements you have identified. If your policy does not meet all the requirements, return to previous steps as necessary and make changes as required.

9. Review with Relevant Stakeholders

Get feedback from relevant stakeholders to ensure the draft policy can be implemented as intended. Incorporate feedback as appropriate, or gather more data as needed.

10. Present for Approval to Appropriate Authority

4   Policy Template

4.1   Principles

A digital records preservation policy establishes the general principles that guide the implementation of a digital records management and preservation programme, ensuring the reliability, authenticity and accessibility of records across space and over time. A Digital preservation policy provides guidance on the management of digital records that need to be retained for periods of time that could exceed the life span of the technology that originally created the records. It prescribes the roles and responsibilities of everyone in the organization who creates and uses digital records. It must use language that is clear and concise. In the event that records management and archival terminology are used, users of the policy will be directed to a glossary. It should be monitored and audited to ensure its effectiveness and reviewed on a regular basis.

4.2   Policy Elements

The policy should address the following:

- Purpose/objectives
- Scope
- Mandate
- Policy statement
- Roles and responsibilities
- Definitions
- Related sources
- Version control
- Policy review

4.2.1 Purpose/Objectives

The policy should begin with an introductory section that aligns the goals and objectives of the policy with the goals and objectives of the organization. Policies governing the creation, maintenance and/or preservation of digital records should address issues of record reliability, accuracy and authenticity.

The examples that follow are taken from case studies in InterPARES 3. Many of the small and medium-sized organizations that participated as testbed partners in InterPARES 3 sought to develop policies and procedures to help manage their digital records. The examples are offered to help start the process of policy development initiatives, and support the learning experience of this module. While they reflect the principles and guidelines developed through the InterPARES research, they are not necessarily intended to be viewed as templates of best practice. Every organization is different and must be approached with a pragmatic view of implementation of the principles.

Examples

Example #1. cIRcle: University of British Columbia Digital Repository (cIRcle), Digital Preservation Policy

The purpose of the cIRcle Digital Preservation Policy is to make certain that action is taken to ensure the long-term preservation of the digital content in cIRcle. This policy acts as an authoritative guide for the long-term preservation of cIRcle's contents and provides a framework to guide preservation practices.

Example #2. British Columbia Institute of Technology (BCIT), Digital Preservation Policy

This policy acts as an authoritative guide on the long-term preservation of digital records at BCIT and to provide a comprehensive overview of the long-term digital preservation function.

The objectives of this policy are:

- *to support the identification of the significant characteristics of digital records that need to be protected to maintain their accuracy, reliability and authenticity;*
- *to ensure that BCIT digital records creators and custodians are informed of their roles and responsibilities in the creation, maintenance and disposition of digital records identified for long-term and permanent preservation; and*
- *to support the ongoing accessibility and continuing preservation of digital records that will be considered trustworthy for legal, administrative and historical purposes over the long term.*

4.2.2 Scope

The scope of a policy should indicate the digital objects that are covered by the policy, and the individuals or department(s) to whom the policy applies.

Examples

Example #1. cIRcle, Digital Preservation Policy.

This policy covers all digital objects submitted to cIRcle.

Example #2. BCIT, Digital Preservation Policy.

To Whom Does This Policy Apply?
　　This policy applies to all BCIT employees (including faculty, staff and administrators) and all schools and departments that generate digital records.

Scope of Digital Records Preservation Policy
　　The BCIT policy for digital records preservation provides the institutional framework necessary to carry out the procedures that will ensure such preservation. Based on the infrastructure outlined in the InterPARES 2 Policy Framework,[i] policy and procedures together constitute a Digital Records Preservation Program that encompasses the disposition of all BCIT digital records appraised for long-term maintenance and of those appraised for permanent preservation in the Archives.

4.2.3 Mandate

The mandate of the organization, agency or department issuing the policy should be stated. The inclusion of a mandate will indicate that the governing body issuing the policy has the authority to do so, and, the policy supports the department and/or organization's business needs.

Example

cIRcle, Acquisition Policy

cIRcle is the University of British Columbia's digital repository for research and teaching materials created by the *UBC* community and its partners. Materials in *cIRcle* are openly accessible to anyone on the Web, have persistent *URLs,* and will be

---

preserved for future generations.

4.2.4   Policy Statement

The policy statement provides a framework that affords for the accountability of records creators and ensures that records are created reliable, and maintained authentic and accurate. It should be based on the business needs of the organization, not on the technology used to achieve those needs. Policies will be reviewed periodically and amended as business needs evolve.

Example

Vancouver School of Theology (VST), Records Management Policy

VST recognizes that efficient management of its records, regardless of form or medium, is essential to support the work of the School, to facilitate governance and management, and to enable the School to comply with legal and regulatory obligations. VST is committed to developing an effective records management program that will promote record accessibility and support VST in meeting its obligations for accountability and protection of privacy, reducing risk and maximizing efficiency.

This policy provides a framework for the creation, management and ongoing preservation of VST's records on any medium that are authentic, reliable and accessible for current and future use.

4.2.5   Roles and Responsibilities

This section ties the responsibility for implementing the policy into the overall organizational structure. It identifies stakeholders and assigns ongoing responsibilities for assuring that the policy is adhered to at all organizational levels. It is in this section of the policy that the accountability framework is examined and defined, maintaining and clarifying the difference, where applicable, between being responsible for actions regarding digital records, and being accountable to others for carrying out actions regarding digital records.

Vancouver School of Theology, Records Management Policy

Director—Records Management and Privacy (or designate)

- *Raise awareness of records management issues with staff and administrators;*

> *administrators, a records classification scheme, and retention and disposition schedules for all records, regardless of their medium;*
> - Identify, with input from and in consultation with administrators, existing digital records, ensure their *trustworthiness according to the InterPARES 1 Project's "Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records," and determine and maintain their relationships with corresponding paper records;*
> - *Advise, train and support staff in implementing records management procedures;*
> - *Work with the IT Director to select hardware, software and file formats that offer the best likelihood of interoperability and continuing accessibility over time; and*
>
> Monitor progress in implementation of procedures, providing support
>
> Develop, with input from and in consultation with as necessary.

4.2.6   Definitions

This section should provide a glossary of domain- or organization-specific terms used in the policy, especially if the use of those terms differs from usage in the *lingua franca* of the organization.

> **Examples**
>
> **Example #1. BCIT, Digital Preservation Policy**
>
> *Active Records: Active records are those in current use, meaning that they are referred to at least once a month per records series. They are stored in office areas and on information technology servers that are immediately accessible.*
>
> **Example #2. cIRcle, Acquisition Policy**
>
> *Bit Preservation: Ensuring that the bits comprising a digital object remain the same over time, preventing corruption, data loss and other damage.*
> *Community: Institution, faculty, department or identified group that creates or generates material.*

4.2.7   Related Sources

Policies must adhere to relevant national and/or regional legislation and may follow relevant standards and best practices. These laws, policies, standards and best practices should be referenced in the policy. The policy should also reference related organizational polices.

Example

BCIT, Digital Preservation Policy

BCIT Policies:
- *6700, Freedom of Information and Protection of Privacy*
- *6701, Records Management*
- *6702, Archives and Special Collections*

Legislation:
- *BC Evidence Act*
- *BC Freedom of Information and Protection of Privacy Act*
- *Canada Copyright Act*
- *Canadian Patent Act*
- *Canadian Trade-Marks Act*

Guidelines and Standards:
- *Canadian Digital Information Strategy (October 2008)*
- *Electronic Records as Documentary Evidence (CAN/CGSB-72.34-2005)*
- *Canadian General Standards Board Microfilm Standard*

4.2.8   Version Control

Each policy should contain version control information to ensure that stakeholders follow the most up-to-date policies. Information needed to support version control include:

- Version number of the policy;
- Date the policy is effective;
- If policy has been superseded, date policy has been superseded;
- Each policy should reference policies it supersedes (has been superseded, reference to updated version).

4.2.9   Policy Review

Policies should be approved by the highest level of management that reflects the importance of their subject matter. Because records bear witness to the activities of an

organization and hold it accountable for its actions, the top levels of management should approve a digital preservation policy. If necessary, policy review should also be sought from legal counsel to ensure that the policy adheres to relevant legislation, and harmonizes with related organizational policies governing records, access to information and privacy.

Policies should be reviewed periodically, to ensure that they continue to provide the best guidance in support of the organization's goals. The policy should identify who, how, when, an by whom the policy itself will be reviewed (for example, there should also be a policy requirement that business managers be responsible for reviewing the implementation of the policy within their own areas.) As distinct from this periodic review, this section should also identify who, how, when and by whom audits and evaluations of the implementation of the policy will be conducted.

This section should contain the following information:

- The individual(s) and/or department(s) responsible for approving the policy;
- Length of time between reviews;
- Date the policy was last reviewed;
- Date the policy was approved by the relevant individual(s) and/or department(s); and
- Date of the next review.

Example

cIRcle, Acquisition Policy

This policy is subject to approval by the UBC Library and will be reviewed every three years. As part of the review, all specific references to legislation, policies, or other documents should be updated to reflect the latest iteration of all materials.

---

5   Case Study: Development of Policy at a Post-Secondary Technical Institution

As with the examples, this case study is offered to illustrate the methodology presented in this module applied in a real-life situation. It is intended to help start the process of policy development, and support the learning experience of this module. Because every organization is different and must be approached with a pragmatic view of implementation of the principles, it is in actual practice that the challenges to the methodology are revealed and solved.

5.1   Background on Institute

The Institute joined InterPARES3 (IP3) as a test-bed partner in order to develop policy and procedures that would be informed by and reflect cutting edge research into the creation and maintenance of digital records.

The Institute is a large post-secondary institution, with an annual enrollment of 16,000 FT & 32,000 PT students. The school offers certificates, diplomas and applied bachelor's degrees and employs over 2,000 full-time and part-time faculty and staff. Education is delivered in six schools (faculties) with classrooms and offices on five campuses. There is one Associate Director, Privacy and Records Management.

Records are created in all departments and are subject to the school's classification system, the Directory of Records. Classification is linked to retention schedules, and while records administrators are designated in each department, the Associate Director, Privacy and Records Management has broad oversight over all records management functions. This system works well for records in traditional formats (paper, microfilm, etc.), but is challenged by the increasing use of computers and other digital technologies to create records.

There are several records creation and storage systems in place for specific types of structured records, but unstructured records are kept in digital document libraries that are created by the Information Technology department by request of individual departments, generally without consulting the Associate Director, Privacy and Records Management.

Traditional records were well managed under several inter-related policies and procedures. While in principal these governed all records regardless of medium, in reality the time had come to update the policies and procedures to cover digital records so that these important assets would be subject to the same accountability as their traditional counterparts.

The Institute wanted to develop policy and procedures for the preservation of their digital records. This policy would complement the existing records management policy, and the associated procedures would expand the procedures for records management and replace the outdated section on electronic records in the existing procedures. This was to be presented as a policy to preserve digital records – this did not, nor was it intended to, address archival preservation, but the ability to create, maintain and use authentic, reliable, and accurate digital records over their entire life cycle while still in the custody of the creator.

5.2   The Challenges

The Institute has two existing records management policies (Records Management, Archives & Special Collections) and has established procedures to assure long-term preservation of analog records. The Institute has 100 million digital records and counting, however, no policy or procedures for long-term preservation of digital records is in place.

The Institute's digital records are subject to classification and retention, but these are not fully implemented for digital records as they are with their analogue and film counterparts. The Institute's records are at risk of loss due to technological obsolescence. Additionally, Freedom of Information (FOI) legislation and privacy requirements require that the Institute be aware of the digital records in its possession and their contents in order to protect personal information and make relevant records available for FOI upon request. The Institute currently has an organizational culture that is not uniformly aware of or sympathetic to digital records management issues.

Case study methodology, using semi-structured interviews and participatory and iterative analysis between researchers and subjects.
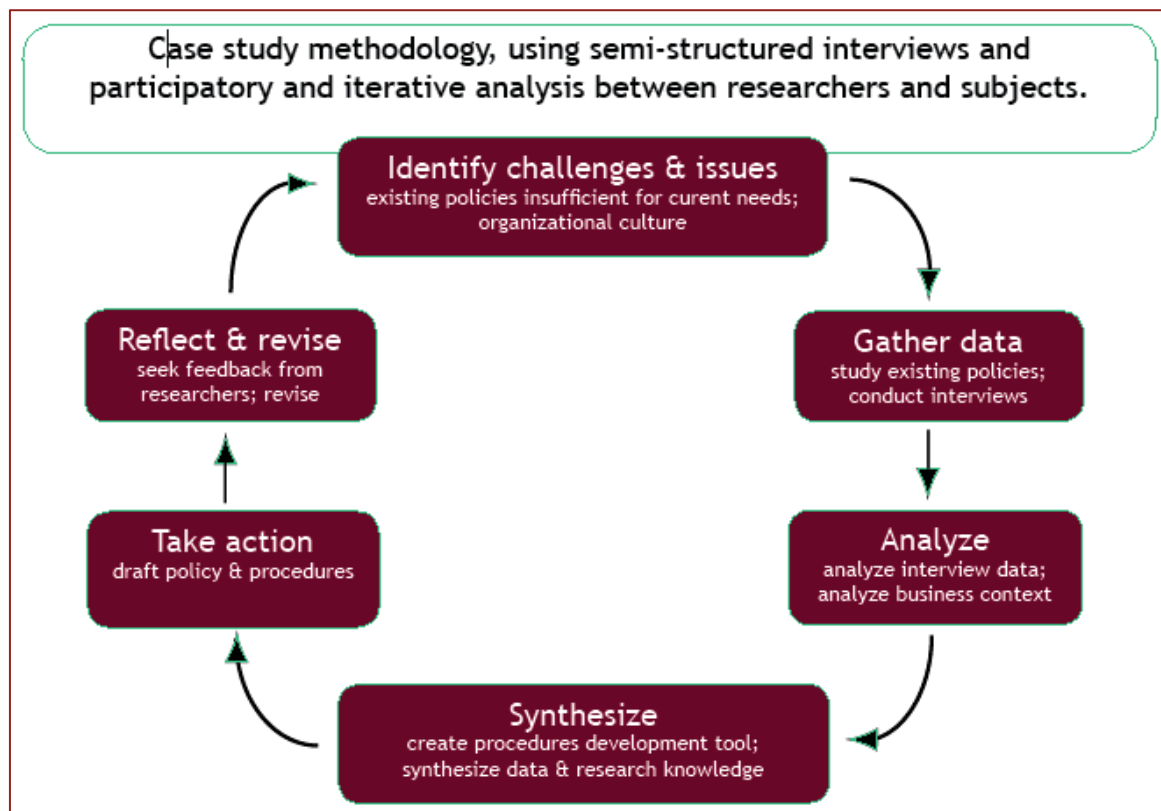
5.3 The Process of Policy Development

- **Gathering data – the contextual analysis and research questions** — The researchers interviewed key management and administrative personnel to build the contextual analysis and answer questions about the records, the record-keeping systems, and the policy development process at the Institute. This was conducted at a high level rather than at the level of individual records creation processes in individual departments.

- **Reviewing existing policies** – The researchers analyzed existing policies and records management materials in order to understand the records management practices and culture of the Institute.
- The researchers **identified the relevant standards and best practices** that needed to be considered.
- The researchers **identified gaps in the existing policy** that needed to be addressed.
- The researchers **drafted a policy that harmonized with the existing records management policy** (as well as other relevant policies, such as, the Institutions Freedom of Information and Archives policies) and added responsibilities to the various levels of records creators and those with authority for the records to ensure that the challenges posed by digital technology were met. The researchers and the Institute's Associate Director, Privacy and Records Management explored the business-related issues that were driving this policy development to identify gaps that needed to be addressed.

It is important to note that this process was not linear. Through discussion and analysis by the Associate Director, Privacy and Records Management and the researchers, an iterative process led to generation of the final draft policy, which was then presented to the authorizing body at the Institute. Once that policy was approved, the researchers began the process of developing procedures that would support the policy.

Procedures were developed in the same model. The difference in the process was in the level of granularity of detail. Where policy articulates high-level concepts that outline and guide accountability, procedures give records creators concrete activities and responsibilities to ensure the creation of authentic, reliable, accurate and usable records.

The researchers interviewed records administrators with direct responsibility for the records of their departments. In the process of conducting interviews, many issues arose that alerted the records administrators to the risks inherent in continuing with "business as usual." Examples include raising awareness about the risk of maintaining and storing records in formats that are not fixed; and the risks of emailing sensitive records to members of external governing bodies who might not exercise the same level of control as was applied internally.

The researchers mapped current practice as gleaned from the interview data to current written procedures, and then mapped this data to best practices and the new policy. With that mapping they were able to write procedures that closed gaps and, if followed, would ensure the creation and maintenance of authentic, reliable, accurate and usable records.

6   Review Questions

The following questions are designed to provide the opportunity for readers of this module to examine some of the concepts and issues presented more closely and evaluate how the concepts presented apply to their organization.

- Describe the key differences between policies and procedures.

- Identify the purpose and key components of a digital recordkeeping and/or digital preservation policy.

- What are the advantages and disadvantages of including preservation in a general records management policy versus having a separate digital preservation policy?

- Identify the main principles in developing a digital preservation policy.

- What is the role of policy in compliance?

- What role does digital preservation policy play in freedom of information, access and privacy, litigation/e-discovery, and organizational accountability?

7   Exercises

7.1   Exercise #1: Policy Analysis – University Electronic Records Disposal Policy[2]

Using what you have learned about designing effective policies, identify the strengths and weaknesses of the following sample policies.

In particular, note:

- What information required of a policy do you find missing?; and
- What information is included in this policy that may better be situated in other control instruments (i.e., guidelines, procedures, etc.)?

University Electronic Records Disposal Policy

1. Purpose

   1.1. The purpose of this policy is to ensure that all electronic records of the University are created, maintained, accessed and disposed of in a controlled manner for the following reasons:
   1.1.1. Support the business functions of the University and its stakeholders;
   1.1.2.   Maintain evidence for possible litigation, mediation, arbitration or disciplinary hearings;
   1.1.3. Adherence to the University Records Management Policy;
   1.1.4. Adherence to the University Records Retention Schedule;

---

[2] See Appendix G for suggested discussion points.

1.1.5.Adherence to the *Provincial Universities Act*; and

1.1.6.Adherence to the *Access to Information Act.*

2. Scope

2.1. This policy applies to all electronic records created, received and maintained by the University.

3. Policy Statement

3.1. The disposal of electronic records must adhere to the University Records Retention Schedule.

3.2. Electronic records that are scheduled for destruction may, upon the date of destruction, be:

3.2.1.Deleted, including all copies maintained across all media (including the University intranet, personal workstation, flash drives, CDs, DVDs and any other external media)

3.3. All paper copies of electronic records scheduled for destruction shall be:

3.3.1.Shredded, if records contain sensitive or confidential information; or

3.3.2.Recycled, if records do not contain sensitive or confidential information.

3.4. Records that are scheduled for permanent retention by the archives shall, upon the date of transfer, be transferred in one of the following methods:

3.4.1.Placed in the "University Archives Drop Box" on the University intranet;

3.4.2.E-mailed to the University Archivist; or

3.4.3. Delivered via external storage media, including flash drives, CDs or DVDs.

4. Roles and Responsibilities

4.1. University Archivist

4.1.1. The University Archivist oversees the University Records Management Program.

4.1.2. The University Archivist, in accordance to this and other applicable policies, shall:

4.1.2.1. Develop and periodically review and update the University Records Retention Schedule;

4.1.2.2. Assist University departments, faculty and staff with the management and disposal of their records, through the provision of guidance documents and training; and

4.1.2.3.   Create procedures as detailed in this policy.

4.2. University Employees

    4.2.1.1.   All University employees shall create and maintain full and accurate records to support the business functions of the University.

    4.2.1.2.   All University employees will ensure the proper disposal of electronic records in accordance with this policy and all procedures relating to this policy.

5. Related University Policies and Documents

5.1. University Records Management Policy

5.2. University Records Retention Schedule

6. Related Legislation

6.1. Provincial Universities Act

6.2. Access to Information Act

7. Review

7.1. This policy will be reviewed every five years and must be approved by the University Board of Regents and the University Legal Counsel.

7.2. Date Approved: 5 March 2010

7.3. Date of Next Review: March 2012

7.2   Exercise #2: Policy Analysis and Review[3]

Using what you have learned about designing effective policies, identify the strengths and weaknesses of the following sample policy governing the management, appraisal and disposition of digital records for a regional archives mandated to preserve records of local government. Within the region, there are different government organizations with varying systems and levels of competencies to manage and preserve digital records. The archives provides advice and sets standards on the creation, management and preservation of digital records of the government agencies; determines the archival value of digital records; issues disposition authorities for digital records when they no longer serve the legal, administrative and business requirements of the agencies; and provides public access to digital records transferred to the archives.

In particular, consider the following of:

- What are the strengths and weaknesses of the policy? Why?
- What is missing from the policy?
- What are the implications of missing elements in terms of implementation of the policy?
- Discuss the adequacy or inadequacy of:
    - The roles and responsibilities section of this policy,
    - The definitions section of the policy,
    - The statement of scope of this policy.

Policy on the Management, Appraisal and Disposition of Digital Records

1. **Objective**
    1.1. The objective of this policy is to provide an integrated framework and strategy for the management, appraisal and disposition of reliable, accurate and authentic digital records generated from business information systems of public agencies. It applies to records owners, IT managers and action officers/users in public agencies.

2. **Definitions**
    2.1. For the purpose of this policy, the following definitions apply:
        2.1.1.   "Digital records" refers to records created, received, processed and stored in electronic or digital form as the official public records of the public agency in the course of official business transactions by the agency's officers.
        2.1.2.   "Data" refers to the electronic representations of information (such as facts, figures or instructions) used for the communication and processing by a computer system.

---

[3] See Appendix G for suggested discussion points.

3. **Roles and responsibilities of staff in recordkeeping**
   3.1. The management of digital records is a shared responsibility and requires various stakeholders to work in partnership to ensure that the infrastructure, systems and procedures are in place to comply with good recordkeeping and preservation practices.
   3.2. Records owners and IT managers are responsible for:
      3.2.1. Developing business rules and processes for creating and capturing digital records onto business information systems and linking metadata with the records;
      3.2.2. Aligning IT processes with recordkeeping procedures including ensuring the proper use, retention, disposal, conversion and migration of digital records;
      3.2.3. Implementing access controls and security measures;
      3.2.4. Determining how long the records should be kept (i.e. retention period) based on business processes, legislative framework and financial requirements;
      3.2.5. Managing changes in recordkeeping system in relation to changes in business processes and needs, software upgrades and new technologies.

4. **Good practices in recordkeeping**

   4.1. Have in place a reliable recordkeeping system:
        In managing digital records, of which emails make up a large proportion, it would be advisable for an organization to invest in a reliable recordkeeping system which helps to ensure that important government decisions captured on emails and digital formats are effectively managed and safeguarded to ensure their accountability, trustworthiness and reliability, as well as long term accessibility.
   4.2. Ensure that digital records and their metadata are integrated into the system:
        Metadata provides contextual information to understand how, when, why and by whom a record was created and transmitted and is an essential component of good recordkeeping. Metadata should be first captured at the point where a record is created and also periodically be captured as more actions on the records take place. Audit trails are a type of metadata and provide contextual information and history on the creation and use of the records within the system—such as when the record was created, accessed, edited and by whom.

5. **Appraisal of digital records**
   5.1. Objective of Appraisal:
        Timely appraisal of digital records ensures the proper identification, safeguarding and protection of records deemed to have continuing business value, identified for long-term preservation, or having archival value.

   5.2. When to Appraise:

      5.2.1.   Ideally, the need for digital preservation should be identified at the planning stage and the digital records themselves should be appraised during the system design and implementation stage so as to facilitate the process of integrating recordkeeping and preservation functionalities and to ensure that appraisal and disposal actions are built into the system.

      5.2.2.   Appraisal decisions should be reviewed periodically, as over time, the business processes may change and recordkeeping systems may evolve. As such, both the creating/transferring agency and the archives need to monitor and review previous appraisal decisions.

6. **Destruction of digital records of short-term/transitory value**
   6.1. Digital records that are of short-term and transitory value such as records meant to support internal housekeeping activities - for example, leave application and financial payment can be routinely destroyed in accordance with the *General Electronic Records Retention Schedule*

7. **Transfer of appraised digital records to the provincial archives for long-term preservation**
   7.1. Agencies are responsible for the authenticity and reliability of the digital records they create and transfer to the regional archives for permanent preservation.
   7.2. Agencies should **decrypt, decompress and unzip** digital records before sending records that are of archival value to the provincial archives. The use of authentication technologies like digital signatures ensures data integrity and confirms the identity of the sender at a specific point of time, but it is not sufficient to ensure the long-term integrity and preservation of e-records over time.

8   Resources

There are many excellent resources available for the development of policy governing digital records maintenance and preservation. The following list is not, nor is it intended to be exhaustive, but is intended to offer a selection of available resources. They are chosen because they are seminal works in the field, offer the results of influential original research, and reflect collective "best-practice" knowledge from a particular area of discipline or community of practice. Many of the sources listed here also include bibliographies that will lead the reader to a broader network of resources.

Author: ARMA International and Society of American Archivists
Title: Sample Forms for Archival & Records Management Programs
Publication Details: 2002
Publisher: Lenexa, KS: ARMA International

This resource contains approximately 200 sample forms and policies users can customize to suite their organization's needs. Forms included cover records management and archival functions including inventory and scheduling; records destruction and disposition; auditing; appraisal; arrangement and description among others. The forms are included in the resource in hard copy and users are also given access to electronic versions of the forms that can be downloaded and customized to suit the organization's needs. There is a cost for this resource.

Author: Shepherd, Elizabeth and Geoffrey Yeo
Title: Managing Records: A Handbook of Principles and Practice (Chapter 8: Implementing records management: Practical and managerial issues)
Publication Details: 2003
Publisher: London: Facet Publishing

This book is a comprehensive text outlining the principles of records management and its practical implementation in organizations. It is comprehensive in its coverage of records management concepts, practices and issues. Useful to both newcomers to the profession and more experienced records managers, issues covered include organizational context; classification; creation and capture of records; appraisal, retention and disposition; access and implementation. The book includes a comprehensive bibliography of records management resources as well as lists of national and international records management standards and professional organizations for records managers.

Author: International Organization for Standardization (ISO)
Title: Information and documentation – Records management
Publication Details: ISO 15489-1: 2001 Part 1: Section 6; Part 2: Sections 2 and 3.2.6
Publisher: ISO

The ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies that prepare and issue International Standards. ISO technical

committees comprised of representatives from member bodies as well as international organizations, and governmental and non-governmental prepare the standards. ISO 15489 consists of the following parts, under the general title *Information and documentation — Records management: Part 1: General and Part 2: Guidelines* [Technical Report]. ISO 15489 was developed in response to consensus among participating ISO member countries to standardize international best practice in records management using the Australian Standards AS 4390, *Records management* as its starting point. ISO 15489 provides guidance on effectively managing records within organizations to ensure that appropriate attention and protection is given to all records, and that the evidence and information they contain can be retrieved more efficiently and effectively, using standard practices and procedures.

Author: The National Archives (TNA)
Title: How to Produce a Corporate Policy on Electronic Records
Publication Details: September 2000 Version 1
Publisher: Crown, Public Records Office
URL: http://www.nationalarchives.gov.uk/documents/rm_corp_pol.pdf

This report, developed by The National Archives of the UK is intended to facilitate the development of a policy by Departmental Record Officers (DROs) within their own departments and agencies. While aimed at DROs, it is a useful resource for any personnel charged with records management responsibilities, including policy development. The report provides guidance on planning, what a policy should cover, importance and incorporation of a policy framework, implementation and auditing. It outlines the various components essential to an effective organizational policy on electronic records, outlining generic principles that can be applied to the management of electronic records.

Author: The National Archives (TNA)
Title: Digital Preservation Policies: Guidance for Archives
Publication Details: 2011
Publisher: Crown, Public Records Office
URL: http://www.nationalarchives.gov.uk/documents/digital-preservation-policies-guidance-draft-v4.2.pdf

This guide was developed by The National Archives of the UK to provide guidance for publicly funded archives in developing digital preservation policies. The guide outlines the key characteristics of a digital preservation policy and discusses why it is necessary and how a policy supports digital preservation. The guide is intended to aid organizations in improving governance of digital preservation via the development of a digital preservation policy. While this guide is directed at publicly funded archives, other archives may find this guide useful in the development of a digital preservation policy.

Author: Beagrie, Najla Semple, Peter Williams, Richard Wright
Title: Digital Preservation Policies Study
Prepared by: Charles Beagrie Limited
Publication Details: HEFCE 2008, Part 1: Final Report October 2008
Publisher: Joint Information Systems Committee (JISC)

URL:
http://www.jisc.ac.uk/media/documents/programmes/preservation/jiscpolicy_p1finalreport.pdf

This report is the result of a JISC funded study that aimed to both provide knowledge into the role of digital preservation in supporting key strategies in the UK Higher Learning environment and create a model for digital preservation policies for UK Higher Education institutions. The publication consists of two tools: 1) a model/framework for digital preservation policy and implementation clauses based on examination of existing digital preservation policies; 2) a series of mappings of digital preservation links to other key institutional strategies in UK universities and colleges. The report serves as a practical guide for developing an institutional digital preservation policy. It contains strategic policy advice supported by further reading sections which select and provide brief descriptions of key existing resources to assist implementation using specific strategies and tools.

Author: The State Records Authority, New South Wales (SRNSW)
Title: Examples of policy, procedure and planning
Prepared by: State Archives
Publication Details: 2010
Publisher: Department of Services, Technology & Administration
URL: http://www.records.nsw.gov.au/recordkeeping/useful-resources/examples-of-policy-procedure-and-planning/examples-of-policy-procedure-and-planning

The State Records Authority of New South Wales manages the NSW archives, and sets the rules and provides guidance on the management of official records. It manages a framework of policy, legislation, standards, codes of best practice and guidelines governing creation, maintenance, preservation of, and access to, public sector records and archives holdings. Among its many useful and informative webpages is the resource page offering examples of policy, procedures and planning. The examples include policies on records management, communication devices, disposal of imaged records, and strategic and operational plans.

Author: Electronic Resource Preservation and Access Network
Title: Digital Preservation Policy Tool
Publication Details: September 2003
Publisher: Information Society Technologies
URL: http://www.erpanet.org/guidance/docs/ERPANETPolicyTool.pdf

This tool sets out the reasons for developing a policy for digital preservation, the advantages of having one, the elements to be included in it, and problems and other specific and relevant aspects. It examines policies in use or under development for preserving and maintaining digital materials, dwelling in particular on specific aspects such as costs, requirements, roles, responsibilities, monitoring and review. It includes a bibliography of resources on digital preservation policy, with particular focus on university libraries and archives, and public records in the United Kingdom, Australia, and the United States.

Author: The InterPARES 2 Project, Luciana Duranti and Randy Preston, eds.

Writers: Luciana Duranti, Jim Suderman, Malcolm Todd
Title: "A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records" in International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records
Publication Details: Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008
URL: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_19.pdf

The *InterPARES Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records* is predicated on the research findings that the ability to preserve trustworthy digital records depends on actions undertaken at the time of their creation. The InterPARES Framework establishes principles to guide policy, strategy and standards development that are flexible enough to be useful in different national environments, but consistent enough to be adopted in their entirety. It consists of thirteen principle statements for records creators, listed in order of relative importance and indicated as required or recommended, and thirteen principle statements for records preservers, similarly listed. Creator and Preserver statements are cross-referenced.

Author: The Northeast Document Conservation Center (NEDCC)
Title: Digital Preservation Template
Publication Details: January 2007 (last revised October 2007)
Publisher: *Interuniversity Consortium for Political and Social Research* (ICPSR)
URL: http://www.nedcc.org/resources/soda/downloads/SoDAExerciseToolkit.pdf

Author: Cornell University Library
Title: Cornell University Library Digital Preservation Policy Framework
Publication Date: December 2004
URL: http://commondepository.library.cornell.edu/cul-dp-framework.pdf

This document formalizes the framework in which digital assets are identified and secured for long-term preservation and ongoing access. The preservation program governed by this framework complies with the Open Archival Information System (OAIS) Reference Model. It includes the operating principles, roles and responsibilities, scope and challenges.

Author: Library of Congress National Digital Information Infrastructure and Information Preservation Program
Title: *Sustainability for Digital Formats: Planning for Library of Congress Collections*.
Publication Date: 2007
URL: http://www.digitalpreservation.gov/formats/sustain/sustain.shtml

This article outlines seven sustainability factors to be considered when choosing digital formats for any category of information for the purpose of preserving digital information as an authentic resource for future generations. They influence the feasibility and cost of preservation and are significant regardless of preservation strategies chosen.

Author: National Library of Australia
Title: *Digital Preservation Policy*
Publication Date: October 2007
URL: http://www.nla.gov.au/policy/digpres.html

This policy reflects the commitment of the National Library of Australia to prioritize ongoing accessibility of its digital resources, participate in research into digital preservation and standards development, and work with national and international partners to foster digital preservation.

Author: University of Illinois at Champaign-Urbana
Title: *IDEALS Digital Preservation Policy*
Publication Date: October 2007
URL: https://services.ideals.uiuc.edu/wiki/bin/view/IDEALS/IDEALSDigitalPreservationPolicy

The IDEALS initiative seeks to comply with the Open Archival Information System Reference Model standard and with certification requirements for a Trusted Digital Repository. The digital preservation policy ensures collection, preservation and sustainable access to the University's scholarly and research output. The policy commits the University to preservation within a flexible framework that accommodates technology development.

Author: Yale University Library
Title: *Policy for Digital Preservation*
Publication Date: November 2005, updated February 2007
URL: http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf

This is an example of a policy for digital preservation in the context of a major research library. The Yale University Library digital preservation policy supports the physical and intellectual preservation and technical stabilization of digital resources through time in order to ensure ongoing access and maintain authenticity. Key elements of the policy recognize that the ability to preserve digital resources and the costs involved depend on decisions taken at all stages of records' life cycle.

Appendix A: Contextual Analysis

A contextual analysis gathers data about the organization that will influence the creation of policy and procedures. It includes information about the organization's administrative structure; its legal and regulatory obligations with respect to its records; norms and standards which influence record creation, maintenance and use; its record creating and recordkeeping requirements and constraints, including the business culture of the organization, personnel constraints and technological constraints. A contextual analysis provides the following information.

Legal and Regulatory Position

Identify and provide information about all laws and regulations, and legally required standards or codes of conduct that govern or affect your organization's records creation and recordkeeping, including requirements for retention and disposition.

Norms

Identify and provide information about any non-legally required standards, methodologies, codes or regulations that govern or affect your organization's records creation and recordkeeping, including requirements for retention and disposition.

Resources (Physical)

Summarize information about the physical context in which your organization operates, including relevant information about equipment and infrastructure.

Governance

Document the governance structure of your organization and the decision-making process as it relates to records management.

Provide the mission statement(s), which may have evolved over time.

Policies

Identify and provide information about all existing policies that pertain to records, their creation, maintenance, retention and disposition and long-term preservation.

Functions

List all of the major functions that your organization undertakes that result in the creation of records.

Appendix B: Records Analysis – Current Practices

Activities that generate documents and records

- List the general types of activities within your organization's functions that result in the production of documents or records.
- Identify the records creators.

Documents and records resulting from activities

- List the main types of documents and records resulting from these activities.

Existence of a records management program

- Describe activities currently undertaken that relate to records management.
- Analyze any policies that the creator might have that govern the creation and management of records.

Individuals responsible for records maintenance

- Identify the individuals(s) responsible for keeping the records after their creation (records maintenance). This might be designated records personnel, or may be the creators of the records, or both.

Existence of maintenance strategies

- Identify the complex of practical means, either formally articulated or informally implemented, that constitute the management of records. This includes:
- The location in which the records are kept,
- The medium/media in which records are kept,
- A description of how records are organized,
- A brief description of any methods used to maintain records,
- A brief description of any methods used to attempt to avoid technological obsolescence while the records are still active or semi-active.

Technological Requirements and Constraints

- Identify and describe the equipment used in your organization:
- Architecture (e.g., network topology, infrastructure, hardware),
- Creation or input tools (e.g., software, camera, microphone),
- Processing tools (e.g., for example software, console).
- Identify and describe the types of media created (e.g., graphic, textual, audio).
- List the formats created (e.g., .pdf, .doc, .jpg) and identify any particular challenges related to their maintenance and preservation.

- Identify and describe how relevant technological requirements/constraints impact upon the creation, form, content, identity, integrity, organization and preservation of the records.

If applicable:

Scientific requirements and constraints

Scientific foundations of the discipline with which your organization identifies that require, influence or prohibit certain behaviors.

- Identify and describe how relevant scientific requirements/constraints impact upon the policies and procedures by which activities are carried out.
- Identify and describe how relevant scientific requirements/constraints impact upon the creation, form, content, identity, integrity, organization and preservation of the records resulting from those activities.

Artistic requirements and constraints

Artistic foundations or schools of thought which your organization identifies that require, influence, or prohibit certain behaviors.

- Identify and describe how relevant artistic requirements/constraints impact upon the policies and procedures by which activities are carried out.
- Identify and describe how relevant artistic requirements/constraints impact upon the creation, form, content, identity, integrity, organization and preservation of the records resulting from those activities.

Appendix C: Creator Guidelines – Making and Maintaining Digital Materials: Guidelines for Individuals[4]

Introduction

Most information today is created and stored in digital form. The advantages of the digital medium are by now familiar to everyone. Documents can be created quickly and edited and revised with ease. Thanks to the Internet, they can be distributed globally with lightning-like speed. They can be manipulated in ways that allow them to be used for multiple purposes. The digital medium also solves the longstanding storage problems associated with large files of paper records.

The blessings of the digital era, however, are not without their costs. Only in recent years have people begun to fully grasp the many problems inherent in the digital medium. For example, there is the fact that digital information can only be accessed using a computer. Furthermore, the computer must be equipped with the necessary software to be able to read the bit strings contained on the disc or tape. Ease of reproduction and the proliferation of copies make it more difficult to identify a complete or final version of a digital document. Easy distribution of information on the Internet makes the preservation of intellectual property rights difficult. Finally, all digital materials are vulnerable to viruses and simple technology failure, as well as to the rapid developments in software and hardware that risk making them inaccessible very quickly.

With all of these problems, it is little wonder that some people yearn for the comforting tangibility of paper. Yet although our systems for creating and maintaining information will likely continue for some time to be hybrid systems—that is, containing both paper and digital materials—there is clearly no turning back from the digital revolution. Consequently, everyone should be aware of the risks faced by digital materials and know how best to minimize these risks.

These guidelines have been developed for individuals who create digital materials in the course of their professional and personal activities to help them make informed decisions about making and maintaining these materials in ways that will help ensure their preservation for as long as they are needed. They may also be useful for small organizations or groups of individuals, such as medical offices, consulting groups or teams of research scientists.

---

[4] These Guidelines have also been issued in an illustrated booklet form that is freely available at http://www.interpares.org/display_file.cfm?doc=ip2(pub)creator_guidelines_booklet.pdf. [Please note that these guidelines have been included here directly from the InterPARES website – appendices referenced in these Guidelines refer to the IP2 book – this will be clarified and fixed when the final delivery method and content are approved]

Although these guidelines can be applied to various kinds of digital publications, documents and data, they are especially important for digital records. Records are the documents that you make, receive and use in your activities, and that you keep because you may need them later or because you want to have reliable evidence of what you have done. Therefore, you need to be especially careful in maintaining and preserving them. These guidelines are applicable to records that need to be maintained for only a short period of time as well as to those that require long-term maintenance. Adherence to these guidelines will help ensure that records that merit long-term preservation in an archival repository will be accessible when they are turned over to the care of a trusted custodian.

Definitions

Before presenting recommendations to guide you in making and maintaining digital materials, it will be both necessary and helpful to clarify the meaning of some of the terms used in this document.

For the purposes of these guidelines, a record is defined as any document created (i.e., made or received and saved for further action or reference) by a physical or corporate person in the course of a practical activity as an instrument and by-product of that activity. A publication is defined as a document intended for dissemination or distribution to the public at large. All records and publications are documents and contain data. A document is information affixed to a medium in a fixed form; information is an assemblage of data intended for communication over time or space; and data are the smallest meaningful and indivisible pieces of information.

These guidelines aim at providing recommendations for the creation and maintenance of reliable digital materials in general, and records in particular, that can be accurately and authentically maintained and preserved over time. To facilitate their application, however, the terms "reliability," "accuracy," "authenticity" and "authentication" need to be defined.

For the purposes of these guidelines, *reliability* is the trustworthiness of digital materials as statements of fact or as content. It is the responsibility of the author of the materials, be that author an individual or the corporate person in whose name an individual is writing, and is assessed on the basis of the material's completeness and accuracy and of the degree of control exercised on the process of its creation.

Accuracy is the degree to which the data in the materials are precise, correct, truthful and free of error or distortion. To ensure accuracy, one must exercise control on the processes of creation, transmission, maintenance and preservation of the materials. Over time, the responsibility for accuracy shifts from the author to the keeper of the materials and later to the long-term preserver of the materials (if applicable).

Authenticity refers to the fact that the materials are what they purport to be and have not been tampered with or otherwise corrupted. Thus, with respect to records in particular, authenticity refers to the trustworthiness of records as records. To ensure that authenticity can be presumed and maintained over time, one must define and maintain the identity of

the materials and protect their integrity. Authenticity is at risk whenever materials are transmitted across space and time. Over time, the responsibility for authenticity moves from the keeper to the long-term preserver of the materials.

Authentication is a declaration of authenticity, resulting either from the insertion or the addition of elements or statements to the materials in question, and the rules governing it are established by legislation. Thus, it is a means of proving that materials are what they purport to be at a given moment in time. Digital authentication measures, like the use of digital signatures, only ensure that the materials are authentic when received and cannot be repudiated, but not that they will stay authentic afterwards.

Recommendations

1. Select hardware, software and file formats that offer the best hope for ensuring that digital materials will remain easily accessible over time.

Accessing digital materials depends on having the appropriate software. Software that is not compatible with previous versions (backward compatibility) or with future versions (forward compatibility) makes it difficult to access records over time. Software for one application also needs to work well with that of other applications and systems (interoperability). Paying attention to the following factors can help ensure that your software and hardware maintain accessibility.

Choose software that presents materials as they originally appeared. Ideally, materials should keep the same look over time to be fully intelligible and accessible. Be sure that new software will be able to read your older materials in the software format in which you kept it and display it on the screen in the same documentary form in which it was originally displayed. In other words, new software should be backward compatible with older software.

Choose software and hardware that allow you to share digital materials easily. Software should be able to accept and output files in a number of different formats. The ability to interact easily with other technology is called *interoperability*. It will make it easier to access your materials and also to move them to other systems.

Use software that adheres to standards. This is one of the best things you can do to ensure your material will last. Standards endorsed by national and international organizations are best. These are called *de jure* standards.[5] If these do not exist for your material, you can help ensure longevity by adopting software that is very widely used. In the absence of an official

---

[5] Defined as: A standard adopted by an official standards-setting body, whether national (e.g., ANSI), multi-national (e.g., CEN) or international (e.g., ISO). For computer file formats, two recent de jure standards are PDF/A (PDF standard for archiving) and ODF (OASIS OpenDocument Format).

standard, such software is often referred to as a *de facto* standard.[6] Open source software; that is, freely available non-proprietary software, is preferable (see subsection G).

Keep the specifications of software. This kind of documentation (e.g. the owner's manuals or any other more detailed description of the software you might have) will be essential in the future to access the materials or to migrate them to a new computer environment as technology advances. It is particularly important to fully document any software that you build yourself.

If you customize software, make sure you document the changes you make. Give detailed information about the changes and describe clearly the characteristics and features of the material these changes produce, as well as the outcomes you are trying to achieve by customizing the software. A good way to do this is to include the information as comments in the software code. The information will not get lost, as it is part of the file, and it will be very helpful to those who need to make adjustments later, as technology advances.

Document the construction of your system as a whole to help ensure its accessibility. You should document your system's structure and functions. This means identifying its hardware and software components, including peripherals, its operating system and software packages. Such documentation will identify how the software packages represent information, and how they process it and communicate it to each other and to users. These basic specifications will ensure that those who come after you understand the context in which you are working now. They will provide the information necessary to update the system as hardware and software evolve.

Choose widely-used, non-proprietary, platform-independent, uncompressed formats with freely available specifications where possible. These are often called "open formats," which means that their specification is published and freely available. However, it may also mean that the format is free of patent or royalty fees or the possibility of such fees being applied in the future, and/or that it is widely adopted. It should be noted that "open" formats are not necessarily the same as formats produced by *open source software*, as the latter term describes software for which the code is made freely available and can be modified. Open source software does not always produce non-proprietary formats. Distinguish between file formats, wrapper (or container) formats and tagged formats such as XML-tagged files, and ensure that version, encoding and other characteristics are clear and fully specified. For XML files, make sure that the files are well-formed and valid and accompanied by the relevant DTDs or schemas. If it is not convenient for you to follow this recommendation, consult with an archives that accepts digital materials and choose among the formats that it recommends for long-term preservation. You should not compress your digital materials, if

---

[6] Defined as: A standard not adopted by any official standards-setting body, but nevertheless widely used and recognized by its users as a standard. Well known and widely used computer file formats that are considered de facto standards include PDF, TIFF, DOC and ZIP.

at all possible, since this can lead to problems for their long-term preservation. If you need to compress them, choose lossless compression techniques that conform to accepted international standards.

2. Ensure that digital materials maintained as records are stable and fixed both in their content and in their form.

One of the great advantages of digital materials is the ease with which information can be edited, revised or updated. But this also means that important information can be changed or even lost, accidentally or on purpose. This is a particularly important problem for records, because one of the characteristics of a record is that its content is unchanged and unchangeable. This implies that the information and the data in the record cannot be overwritten, altered, deleted or expanded. A system that contains fluid, ever-changing information or data does not really contain records until someone decides to make them and save them with *fixed form*[7] and *stable content.*[8]

Although the idea of stable content is fairly simple, the concept of fixed form is more complex. Essentially, it means that the message conveyed by a digital record (or other digital object) can be rendered with the same documentary presentation it had on the screen when it was made or received and first saved. The bit streams that compose the digital record and determine its digital presentation (i.e., its file format) may change, but its documentary presentation must not change. A simple example is when a document created in Microsoft Word is later saved as an Adobe PDF file. Although the document's digital presentation has changed—from a Microsoft Word .doc file format to an Adobe .pdf file format—the documentary presentation of the document—also called its *documentary form*[9]—has not changed, and therefore we can say that the document has a fixed form.

In some cases, digital materials can be presented in several different ways—in other words, the information they convey can take different documentary forms. For example, statistical data can be presented as a pie chart, a bar chart or a table. However, the possible variations of these displays are usually limited by the system. In such cases, we can regard each documentary presentation as having stable content and fixed form, since the information is selected from a fixed store of data within the system and the system's rules govern the form of its documentary presentation(s).

A similar situation occurs when the selection of both content and form is from a large store of fixed information that is only partially accessed every time a user queries the system. If

---

[7] Defined as: The quality of a record that ensures the documentary appearance or presentation is the same each time the record is retrieved.
[8] Defined as: The quality of a record that makes the information and data contained in it immutable, and requires changes to be made by appending an update or creating a new version.
[9] Defined as: The rules of representation according to which the content of a record, its administrative and documentary context and its authority are communicated. Documentary form possesses both extrinsic and intrinsic elements.

the same query always produces the same output as to content and documentary form, the output can be regarded as having stable content and fixed form. Thus, if you, as the author of the record, establish fixed rules for the selection of its content and of its documentary form that only allow for a known and stable range of variability— that is, endow it with *bounded variability*[10]—then you can claim that your material has stable content and fixed form.

The concern for the documentary presentation of digital materials is particularly important for maintaining and assessing the reliability and accuracy of records. Future upgrades, conversions or migrations of data may result in changes to the documentary form. Therefore, you would be wise to first establish the documentary form of records associated with each activity or procedure and then identify the essential characteristics (i.e., the essential *intrinsic* and *extrinsic* elements[11]) of each documentary presentation or form. This will help alert you to any changes in the future that would imply a loss of identity and integrity of the record, especially if you are active in the sphere of digital art, where a certified description of those essential characteristics by the artist would help support the recognition of the intellectual property rights linked to work so described.

3. Ensure that digital materials are properly identified.

Giving a meaningful name to a computer file helps identify its content and makes it easier to find. The full identification of records is more complex than just naming files, however. Full identification is essential in distinguishing records from each other, in distinguishing different versions of a single record and in providing evidence of the identity of a record from the moment of its creation through its long-term preservation.[12]

The information about digital materials that supports their identification and retrieval is commonly referred to as *metadata*.[13] Most software applications automatically tag all digital materials with some data about their identity because this information is necessary to

---

[10] Defined as: The quality of a record that ensures that its documentary presentations are limited and controlled by fixed rules and a stable store of content data, form data and composition data, so that the same user activity, query, request or interaction always generates the same result.

[11] 8 *Intrinsic Elements* are defined as: The elements of a record that convey the action in which the record participates and its immediate context, including the names of the persons involved in its creation, the name and description of the action or matter to which it pertains, the date(s) of creation and transmission, etc. *Extrinsic Elements* are defined as: The elements of a record that constitute its external appearance, including presentation features such as font, graphics, images, sounds, layouts, hyperlinks, image resolutions, etc., as well as digital signatures, seals, and time stamps and special signs (digital watermarks, logos, crests, etc.).

[12] In this context, *identity* is defined as: The whole of the characteristics of a document or a record that uniquely identify it and distinguish it from any other document or record. With integrity, a component of authenticity. (See also Recommendation 4.)

[13] Defined as: Information that characterizes another information resource, especially for purposes of documenting, describing, preserving or managing that resource.

locate documents effectively. Without metadata, it would be nearly impossible to find a document without opening and reading through a folder or several directories. Metadata describe the properties or attributes of digital materials. In the case of records, however, these properties or attributes are also necessary to maintain and assess their authenticity, and that is why it is important to ensure that all the essential ones are recorded and that they are correct.

The properties or attributes conveying the identity of digital materials are referred to as identity *metadata*.[14] These include:

- Names of the persons involved in the creation of the digital materials. These include:
    - the author—the physical or corporate person(s) responsible for issuing the materials;
    - the writer—the physical person(s) or position(s) responsible for articulating the content of the materials;
    - the originator—the physical person, position or office responsible for the electronic account or technical environment where the materials are generated and/or from which it is transmitted;[15]
    - the addressee—the physical or corporate person(s) for whom the materials are intended; and
    - the recipient—the physical or corporate person(s) to whom the materials may be copied or blind copied.
    - *Name of the action or matter*—in other words, the title or subject.
    - *Documentary form*—in other words, whether it is a report, a letter, a contract, a table, a list, etc.
    - *Digital presentation*—in other words, format, wrapper, encoding, etc.

- Date(s) of creation and transmission. These include:
    - the *chronological date* written on the materials or on which the materials were compiled;
    - the *dates of transmission and/or receipt;* and

---

[14] Defined as: The properties or attributes conveying the identity of a digital object that is to be kept as a record. (See also Recommendation 5.)

[15] Identification of the originator is only important in cases where the person, position or office responsible for physically creating and/or transmitting the materials is neither the author nor the writer, and when the presence of the originator's name appearing on, or in association with, the materials calls into question the actual author and/or writer of the materials. This is most commonly associated with e-mails in instances where the name of the originator appears in the header of an e-mail and/or its attachments that were in fact authored and/or written by another person, but physically manifested and/or transmitted on behalf of that person by the originator.

- the *archival or filing date*—in other words, the date when the materials were associated with a computer folder or directory, or other classification scheme or filing plan (see Recommendation 5).

- *Expression of documentary context*—for example, a classification code, or the name of the computer folder or directory, or comparable filing unit within the classification scheme or filing plan to which the materials are associated, and the name of the broader group of records in which the materials belong (see also Recommendation 5).
  - Indication of attachments, if applicable.
  - Indication of copyright or other intellectual rights, if applicable.
  - Indication of the presence or removal of a digital signature, if applicable (see Recommendation 6, Technology-dependent Authentication section).
  - Indication of other forms of authentication, if applicable. This could include, for example, the presence of a corroboration (i.e., an explicit mention of the means used to validate the record); an attestation (i.e., the validation of a record by those who took part in the issuing of it, and by witnesses to the action or to the 'signing' of the record); a subscription (i.e., the name of the author or writer appearing at the bottom of the document), or a qualification of signature (i.e., the mention of the title, capacity and/or address of the person or persons signing the record).
  - Indication of the draft or version number, if applicable.
  - Existence and location of duplicate materials outside the digital system, if applicable. If multiple copies of a document exist, you should indicate which one is the official or authoritative copy.[16] If the document is certified by the author as an "approved reproduction" of a work (for example, a digital work of art), indication of the existence of such certification is required. If the document comprises material copyrighted by different author(s), indication of copyright clearance (or lack thereof) with related dates is necessary.

4. Ensure that digital materials carry information that will help verify their integrity.

Although the identity metadata help distinguish digital materials from one another, another set of metadata allows users to infer that the materials are the same as when they were created (although not to verify or demonstrate it, because this would require comparison with a copy of the materials kept elsewhere). These metadata can be referred to as *integrity*

---

[16] Defined as: The instance of a record that is considered by the creator to be its official record and is usually subject to procedural controls that are not required for other instances.

metadata (see below). Digital materials have *integrity*[17] if they are intact and uncorrupted, that is, if the messages that they are meant to communicate to achieve their purposes are unaltered. This means that the physical integrity of digital materials, such as the proper number of bit strings, may be compromised, provided that the articulation of the content and its required elements of *documentary form* (see Recommendation 2) remain the same. The content and the data in it are considered to be unaltered if they are identical as to the value and presentation (i.e., position on the screen) of the content and data in the first saved manifestation of the material. The attributes that relate to the integrity of digital materials have to do with the maintenance of the materials, including the responsibility for their proper handling, such as overseeing and documenting any technological transformations or transfers of the materials to other systems.

The integrity metadata include:

- Names of handling person/office—the person or office using the materials to carry out business.
- Name of person or office with primary responsibility for keeping the materials—this may be the same as the handling person/office.
- Indication of annotations added to the materials, if applicable.
- Indication of any technical changes to the materials or to the application(s) responsible for managing and providing access to the materials—for example, change of encoding, wrapper or format, upgrading from one version to another of an application, conversion from several linked digital components to one component only (e.g., by embedding directly in the materials digital components that were previously only linked to the materials, such as audio, video, graphic or text elements like fonts).
- Access restriction code—indication of the person, position or office authorized to read the materials, if applicable.
- Access privileges code—indication of the person, position or office authorized to annotate the materials, delete them, or remove them from the system, if applicable.
- Vital record code—indication of the degree of importance of the record to continue the activity for which it was created or the business of the person/office that created it, if applicable.[18]
- *Planned disposition*—for example, removal from the live system to storage outside the system; transfer to the care of a *trusted custodian* (see Recommendation 10); scheduled deletion.

---

[17] Defined as: The quality of being complete and unaltered in all essential respects. With identity, a component of authenticity.

[18] The vital record code only pertains to specific communities of practices, such as legal and medical offices, who must identify the records that are vital to the continuance of their business in case of disaster and who would therefore exercise special protection measures on those records.

5. Organize digital materials into logical groupings.

The management and retrieval of your digital materials can be enhanced if you can handle them in large sets, rather than one by one. Therefore, it is important that you group your digital materials in some logical manner. The categories chosen may reflect the way you work, your activities, procedures, thematic areas, or some sort of structural organization. Separating your records from other digital materials is an important first step. The organization of your records may be based on the different types of records or the length of time for which certain kinds of records need to be kept. These groupings can be related to each other in a hierarchical or flat way, as best suits your needs. Generally, this structure should be consistent with the organization of any paper records you have (or records in other media), so that all records related to the same activity or subject, or of the same type, can be easily identified and retrieved as part of one conceptual grouping, as needed. Your organization scheme should be recorded in a document that shows all the groupings of materials, describes them in a brief sentence and indicates how they are related. In this document, which is called a classification scheme[19] or filing plan, each grouping of records can be assigned a code or a name that should be linked to each record belonging in the same grouping no matter what the medium or location: thus, the records assigned to each grouping will share such code or name, followed by a number that indicates their sequence. This identifier should be recorded among the identity metadata[20] of your digital records and on the face of your paper records belonging to the same grouping and should be unique for each record.

Identifying how long groupings of records need to be retained will facilitate their management while they are regularly needed and help ensure that records that need or merit long-term preservation are tagged early and given proper protection to ensure their survival.

You will find it easier and more efficient to assign a retention period—the length of time you want or need to keep materials—to a grouping of materials, rather than to individual items. Trying to ensure that some things are kept as long as needed while weeding out things that are no longer needed is simply too cumbersome at the individual item level. Although you may think that within a grouping some records should be kept longer than others, not only will you save time if you keep the whole grouping, but you will also have more complete information when you need to refer to the records. However, for some types

---

[19] Defined as: A plan for the systematic identification and arrangement of business activities and records into categories according to logically structured conventions, methods and procedural rules. (See also Recommendation 3.)

[20] Defined as: The properties or attributes conveying the identity of a digital object that is to be kept as a record. (See also Recommendation 3.)

of records, you can create subgroups within each given grouping on the basis of the retention period.

6. Use authentication techniques that foster the maintenance and preservation of digital materials.

The authenticity of digital materials is threatened whenever they are transmitted across space (i.e., when sent to an addressee or between systems or applications) or time (i.e., either when they are in storage, or when the hardware or software used to store, process or communicate them is updated or replaced). Because the acts of setting aside digital materials for future action or reference and of retrieving them inevitably entail moving them across significant technological boundaries (from display to storage subsystems and vice versa), the inference of the authenticity of digital materials must be further supported by evidence that they have been maintained using technologies and administrative procedures that either guarantee their continuing identity and integrity or at least minimize risks of change from the time the records were first set aside to the point at which they are subsequently accessed.

Technology-independent Authentication

Presumption of Authenticity. A presumption of authenticity is an inference that is drawn from known facts about the manner in which a document has been created and maintained. Adoption and consistent application of the recommendations presented in this document provide the best evidence to support such a presumption. The recommendations are cumulative: the higher the number of satisfied recommendations and the greater the degree to which an individual recommendation has been satisfied, the stronger the presumption of authenticity.

Successful implementation of the recommendations presented in this document is predicated on establishing and continuously applying effective administrative policies and procedures.[21] Ideally, you should strive to implement authentication techniques supported by administrative policies and procedures that are as technology-independent and/or neutral as possible.

Technology-dependent Authentication

Technology-dependent authentication techniques, such as cryptography, are used to provide a technological mechanism to guarantee the authenticity of digital materials. One such cryptographic technique is the digital signature, which can be used when transmitting documents between persons, systems or applications to declare their authenticity at a

---

[21] See Appendix 19, "A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records."

certain point in time. Such technologies have been given legal or regulatory value by some bodies, like the European Commission and the Securities and Exchange Commission.

Caution! Digital signatures are subject to obsolescence themselves and, by virtue of their purpose and inherent functionality, cannot be migrated to new or updated software applications together with the documents to which they are attached. In fact, the life of digital signatures and other authentication technologies may be much shorter than the length of time that even a temporary document not requiring migration may need to be maintained, because authentication technology is changing rapidly. Unless or until further development of digital signature technology enables such encrypted authentication information to be preserved over time with the document, you should, when you receive a document with an attached digital signature, detach the signature whenever possible and add information to the integrity metadata to indicate that the document had an attached digital signature when received and that the signature was verified, detached and deleted.

7. Protect digital materials from unauthorized action.

The accuracy and authenticity of digital materials cannot be presumed if there is any opportunity for modifying them without leaving a trace. You need to be able to demonstrate that it was impossible for anyone to tamper with or manipulate your digital materials without that person being identified. Security includes restricting physical access to places where computers are kept, as well as restricting access to the digital materials on the computers themselves. The latter can be accomplished through various means, including the use of passwords and/or biometric authentication to log on to the system.

It is also important to set up a structure of access permissions (also called access privileges—see discussion of integrity metadata in Recommendation 4) for all users of the system. For example, some users may only be able to read materials, while others may have permission to modify them. In any case, it should be impossible to modify any record once it has been filed according to the classification scheme or filing plan (see Recommendations 3 and 5), and only the person who has been given responsibility for recordkeeping and maintenance should be able to transfer or delete materials from the system. In addition, the system should maintain an audit trail to track access to the materials to control the administration and use of access privileges.

This recommendation may appear to be a tall order for individuals who may be working out of their homes, or even for those working in very small offices or communities of practice. But it is important to remember that if you cannot demonstrate that it was impossible for anyone to tamper with and manipulate your digital materials without being identified, your assertion that your records are de facto accurate and authentic becomes irrelevant. In this regard, it might be useful to keep copies of at least the most important digital materials offline and to establish some routine by which materials stored offline are randomly compared with their counterparts online on a periodic basis.

8. Protect digital materials from accidental loss and corruption.

Computers are not foolproof, and any of a number of factors can cause corruption or other accidental loss of records or data. The best way to ensure against accidental loss or corruption is to make backup copies regularly and often. If you store such copies off-site, additional protection is obtained against fire or theft of equipment. Many backup techniques, software packages, and services are available, including ones that automatically create the backup materials and then transmit them to a secure off-site location.

- *Develop a rigorous policy or routine that ensures your system is backed up daily*. Your system is only as good as its last backup, so you need to make sure it is backed up often, at least once daily, using proven methods that will ensure that if something goes wrong, you and/or your business will be able to recover quickly. Such regular backups should be destroyed on a rotational basis according to a strategy or schedule that is most appropriate for your requirements, since they do not contain records but only exist for recovery of the system if it fails. Note that we are talking here about a comprehensive *system backup*, which includes the operating system, the software applications and all the digital materials in your system. If, in addition to a system backup, you need to have a security copy of your digital materials in case your computer is stolen or some of your records become corrupted, then you should backup those materials only on another computer, an external hard drive or other portable digital media and store these security copies in an off-site location away from the computer with the "original" copies.
- *Choose and install the best backup technology for your situation*. Study the technology and services available, and choose what works best for your particular situation. Many different systems are available, ranging from those covering one-person operations to those able to back up very large systems. The backup system needs to include an audit trail, in case the system fails between backups and you need to recover the records or other digital materials created during the time for which there is no backup.

9. Take steps against hardware and software obsolescence.

The speed with which hardware and software become obsolete poses severe challenges to the maintenance and long-term preservation of digital material. One strategy to address this problem is to eliminate dependence on hardware by transferring hardware functionalities to software (i.e., use a software application to simulate the actions of a piece of hardware). This provides a more stable way to retain the function when the hardware becomes obsolete.

The rapidly changing technology environment means that both individuals and offices should regularly upgrade their digital systems as well as all the records within these systems and those that have been moved to another storage medium, such as CD, DVD or tape. In other words, when parts of the technological environment in which you are working begin to become obsolete, they should be upgraded to the most advanced technology available according to your particular requirements and constraints, and all digital materials inside and outside the system should be migrated to the new technology.

When replacing hardware, it is important for the replacement hardware to have capabilities at least equal to the hardware it is replacing. For example, a new monitor needs to display a graphic record in a way that retains the documentary form of the original record. Planning for regular technology upgrades on a rotational basis will help ensure that your technology does not become out of date and also help prevent large and unexpected technology expenses.

Sometimes digital records produced by or maintained in systems that are becoming obsolete need to be retained for a long time, but they are not expected to be accessed often. If such records are textual records and need to be read sequentially rather than randomly, you could convert them from their digital form to computer output microfilm. This will protect them from accidental loss or corruption better than any other measure. Another good protective measure is duplication—creating a second copy of groups of vital records and keeping it on another computer, on a second hard drive, on DVD, with another office or individual or in remote storage. When digital records or other entities are removed from a live system, for storage on magnetic or optical media outside the system, for example, it is essential that documentation about the system and about the digital materials (for example, the records' metadata) is also removed and kept with them. For more detailed information about the types of documentation in question here, see Recommendation 1, subsections D, E and F.

10. Consider issues surrounding long-term preservation.

Although the focus of this document has been on the creation and maintenance of all kinds of digital materials while they are needed on a regular basis by their creators, it is important to consider how best to preserve important digital materials for the long term. Typically, only a small percentage of materials need to be preserved for the long term, but the ability to provide ongoing, long-term care for materials, especially digital materials, is often beyond the capability or interest of individuals and small organizations. There are real costs—both financial and human—in retaining materials for the long term, but such preservation efforts are essential for establishing and maintaining our cultural heritage, for accountability purposes and for informing managerial decision-making.

To begin this process, you should identify someone who will take charge of your digital materials once they are no longer needed for regular personal or professional purposes. This person would take the role of trusted custodian.[22] A trusted custodian is a professional—or a collection of professionals, as in an archives or a community historical society—who is educated in recordkeeping and preservation, and who ideally has no stake

---

[22] Defined as: A preserver who can demonstrate that it has no reason to alter the preserved records or allow others to alter them and is capable of implementing all of the requirements for the authentic preservation of records.

in the content of the records and no interest in allowing others to manipulate or destroy the records.

In the case of small organizations or offices, this person could be the one responsible for keeping the records and organizing and storing them during their active use. In the case of individuals who manage their own recordkeeping, the person fulfilling the preservation function may be an archivist or a librarian in a documentation centre, or simply themselves. In either case, a preservation strategy should be established as soon as possible, because digital materials that have not been targeted for preservation early and taken care of in a proactive way will not be preserved. Close adherence to these guidelines will therefore facilitate long-term preservation.

Conclusion

This document has outlined a series of activities for individuals and small organizations to carry out to create and maintain digital materials that can be presumed to be authentic, accurate and reliable. For individuals the burden may seem great, but the alternative—loss of records or the emergence of corrupt and unverifiable data—would be an even greater problem in the long run. Small organizations will benefit by making a clear designation of the individual or individuals responsible for overseeing the maintenance of the organization's digital records. Bear in mind, however, that not all recommendations presented in this document need to be implemented in each circumstance; you should be able to select and adopt the measures that address your particular problems in the specific context in which you operate. There may also be cases in which additional measures are necessary because of legislative or regulatory requirements specific to your field, or because of the characteristics of the activity and hence of the records that it produces. In such cases, consultation with experts may be required. Among such experts are the archivists of city, provincial, state or national archives, as well as local archival associations. Individuals, offices and small organizations should not hesitate to contact such experts for advice on any issues relating to the creation and maintenance of their digital materials.

Finally, this set of guidelines is but one of the documents issued by the InterPARES Project, an international research project studying the long-term preservation of authentic digital records. Additional material that will support the understanding of the nature of digital records and the development of methods for their reliable creation and accurate and authentic maintenance and preservation can be found on the InterPARES Web site at www.interpares.org

Appendix D: Preserver Guidelines – Preserving Digital Records: Guidelines for Organizations[23]

Introduction

These guidelines have been developed to provide concrete advice to various groups that are responsible for the long-term preservation of digital records. They are not intended to be comprehensive but to highlight a number of areas that are particularly important to the preservation of authentic digital records and which experience has shown to be often overlooked in the rush to accept digital records into archival repositories.

As is widely recognized, digital records must be carefully managed throughout their entire existence to ensure that they are accessible and readable over time with their form, content and relationships intact to the extent necessary for their continuing trustworthiness as records. It is also widely recognized that management of digital records must proceed from a comprehensive understanding of all phases or stages of records' existence, from the time they are generated, through their maintenance by their creator, and during their appraisal, disposition and long-term preservation as authentic memorials of the actions and matters of which they are a part. From the perspective of long-term preservation, all the activities to manage records throughout their existence are linked, as in a chain, and interdependent. If a link in the chain fails, the chain cannot do its job. If certain activities and actions are not undertaken on records, their integrity (that is, their reliability and authenticity) and preservation are imperiled.

These guidelines focus on the preservation link in the chain of preservation and are organized according to the sequence of preservation activities presented in the InterPARES Chain of Preservation (COP) model,[24] which charts the many sequential steps in the creation, maintenance and preservation of authentic records. The alphanumeric number in parentheses following each section title in these Guidelines is a cross reference to the applicable preservation activity presented in the COP model.

The guidelines have been tailored to address the preservation needs of organizations or pro-grams whose records must be retained and consulted for long periods and those of archival institutions that take on the responsibility for the long-term preservation of the records of others and for their continuing accessibility to the public they serve. In both

---

[23] These Guidelines have also been issued in an illustrated booklet form that is freely available at http://www.interpares.org/display_file.cfm?doc=ip2(pub)preserver_guidelines_booklet.pdf. [Please note that these guidelines have been included here directly from the InterPARES website – appendices referenced in these Guidelines refer to the IP2 book – this will be clarified and fixed when the final delivery method and content are approved]

[24] Available at http://www.interpares.org/ip2/ip2_models.cfm.

these cases, human and financial resources as well as in-house technical expertise are frequently limited.

Institutions, organizations and programs with preservation responsibilities should also consult the *Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records* (a.k.a., Policy Framework)[25] developed by the InterPARES 2 Policy Cross-domain, which complement these Guidelines. Many of the recommendations of these Guidelines may also be applicable to the preservation of digital objects other than records, such as documents, publications or data.

1. Manage Chain of Preservation

This aspect involves determining framework requirements, and designing, implementing and maintaining a chain of preservation framework. A Chain of Preservation Framework includes all the elements of policy, strategy, methodology and so on.

1.1. Establish scope and objectives

Preservers must define the scope and objectives of their digital preservation program. In the arts, for example, they may wish to preserve the recording of the performance(s) of a work, or they may choose to undertake the more complex preservation of the components of a work of art that support its reproduction or re-performance. In the sciences, preservers may wish to preserve only the final report of the results of an experiment, or hold raw data, normalized data and/or aggregated data to document the methodology used and the result obtained, as well as to ensure the availability of the data for future uses. Preservers should also consider who the eventual users of the archives will be. Technically sophisticated users generally require less assistance in accessing even technologically complex digital materials, while the general public might require extremely user-friendly access mechanisms and materials transformed into a few simple, but widely available, formats. The scope of the preservation program will help define which preservation strategies (see Section 4 and Appendix 21c, Section B) a preserver might need to support.

In defining the digital preservation program, preservers should build on previous efforts. To develop appropriate policies and strategies, preservers should consult the InterPARES 2 Policy Framework for guidance applicable at organizational, sectoral, national, international and supranational levels. For the functions of the preservation program, preservers should consult the ISO Open Archival Information System (OAIS) standard[26] and should follow the InterPARES 2 Chain of Preservation model for an adaptation of the OAIS standard specifically intended for digital records. Plans should also reflect the Trustworthy Repositories Audit & Certification: Criteria and Checklist, a revised

---

[25] Available at http://www.interpares.org/public_documents/ip2(pub)policy_framework_document.pdf.
[26] International Organization for Standardization, ISO 14721: 2003 - Space data and information transfer systems—Open archival information system—Reference model.

and expanded version of the Audit Checklist for Certifying Digital Repositories originally developed by the NARA/RLG Digital Repository Task Force.[27]

1.2. Acquire resources

Digital preservation requires substantial resources in funding, technological capabilities and expertise. An organization responsible for digital preservation has several options, including: a) acquire new resources, b) reallocate existing resources and/or c) leverage other resources.

Regardless of the option(s) chosen, a fundamental requirement is that resources must be sustainable. One-time resources, such as grants, may be appropriate for specific finite tasks, such as establishing the preservation program or processing a given body of records, but a reliable source of sustained resources is a sine qua non for any preservation program.

Acquiring new financial resources will require a sound plan for the program and a matching communications plan to convince funding sources and stakeholders that preservers are likely to consult that the program should be funded. A viable strategy for a new program may be to start small and plan on short-term successes to convince funding sources to incrementally increase resources for the program. An incremental strategy should evaluate whether funding sources are more likely to be influenced by short-term success in basic program objectives or in areas of more particular concern to the funding sources and stakeholders. For example, funders and stakeholders may be more swayed by demonstrations of technological capabilities than by a sound and comprehensive plan for appraising digital records.

For most organizations, reallocating resources to digital preservation is likely to entail painful choices. As with seeking new funds, an incremental approach may be best. Furthermore, ongoing adjustments can be made to the plan, based on the experience gained during each phase of implementation. If the digital preservation program is to be established in a larger institution, it would be helpful to address digital preservation as part of the overall strategic plan rather than as a special initiative.

Even when a preserver successfully acquires new resources or is able to reallocate existing resources to digital preservation, it is unlikely it will have sufficient resources to address all the challenges. Therefore, preservers should capitalize on opportunities for leveraging outside resources. There are a variety of paths for doing this. For example, rather than trying to hire technical experts on a permanent basis or training staff in all requisite technical knowledge and skills, preservers might engage outside experts on a consultative or task basis. They should not exclude options to contract for both basic and ad hoc services. On a basic level, preservers should evaluate the possibility of using a computer service

---

[27] See Online Computer Library Center, Center for Research Libraries (2007), "Trustworthy Repositories Audit & Certification: Criteria and Checklist," v. 1.0, February 2007. Available at http://www.crl.edu/PDF/trac.pdf.

provider rather than acquiring a dedicated preservation system. Ad hoc options include engaging specialized companies for tasks such as re-copying from obsolete digital media or converting rare formats. Another option is to participate—actively or passively—in open-source communities developing technologies needed for digital preservation (e.g., FEDORA,[28] Global Registry of Digital Formats[29]).

Finally, preservers in an organization lacking the required resources to support a digital preservation program should investigate the possibility of establishing collaborative partnerships or consortia to develop and finance a program that meets a minimum acceptable standard.

1.3. Focus on digital records

Preservers must ensure that digital preservation resources are primarily deployed to protect authoritative copies[30] of digital records, rather than to preserve digitized copies of surviving analogue records. The rationale for this is that most analogue records will survive without digitization, whereas digital records will be lost without a digital preservation program.

1.4. Offer advice

Because the chain of preservation of digital records begins at creation, preservers should provide advice on digital records creation and maintenance. Depending on the mandate of the preserver, this may be quite specifically targeted to, for example, employees in the preserver's organization or, as in the case of national archives, other government institutions. In other cases, the advice may be disseminated widely to special interest groups or to the general public, with the purpose of reaching the person(s) or organization(s) whose records fall under the mandate of the preserver.

1.5. Set a good example

Preservers must establish, within their own organization, a record-making and a recordkeeping environment such that their own control records produced in the course of their preservation function will be created and maintained in a way that satisfies the InterPARES 1 Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records.[31] Not only is this an essential requirement for any organization

---

[28] See http://hul.harvard.edu/formatregistry/.

[29] See http://www.fedora.info/.

[30] Authoritative copy is defined as "The instantiation of a record that is considered by the creator to be its official record and is usually subject to procedural controls that are not required for other instantiations" (InterPARES 2 Terminology Database. Available at http://www.interpares.org/ip2/ip2_terminology_db.cfm).

[31] See Authenticity Task Force (2002), "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records," in *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Italy: Archilab, 2005), 204-219.

undertaking long-term preservation, but the development of this type of in-house environment will also provide:

- hands-on training to archivists in the technologies they are championing to records creators;
- an invaluable "user's eye view" of actual recordkeeping solutions and how they really work in a day-to-day operational environment;
- a testbed where upgrades and innovations can be introduced and evaluated; and
- a working prototype that can be used in demonstrations.

1.6. Develop procedures

Preservers must establish controls over records transfer, maintenance and reproduction, including the procedures and system(s) used to transfer records to their own organization or program within the organization; maintain them; and reproduce them in a way that satisfies the InterPARES 1 Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records.[32] These procedures must embody adequate and effective controls to guarantee the records' identity[33] and integrity,[34] and specifically that:

- unbroken custody of the records is maintained;
- security and control procedures are implemented and monitored;
- the content of the records and the required annotations and elements of documentary form remain unchanged after reproduction.

1.7. Implement maintenance strategies

Although much attention is paid to the development of complex long-term preservation strategies, such strategies are inapplicable if the records for which they are to be used are not properly maintained and protected in the recordkeeping and/or record preservation systems that contain them. A complete version of the eight primary maintenance strategies is available in Appendix 21c, Section A. Briefly, they include:

Online reprint available at http://www.interpares.org/book/interpares_book_k_app02.pdf. See Appendix 21a for an abridged version.

[32] Ibid. See Appendix 21b for an abridged version.

[33] Identity is defined as "The whole of the characteristics of a document or a record that uniquely identify it and distinguish it from any other document or record. With integrity, a component of authenticity" (InterPARES 2 Terminology Database, op. cit.).

[34] Integrity is defined as "The quality of being complete and unaltered in all essential respects. With identity, a component of authenticity" (Ibid.).

A1. Clear allocation of responsibilities

A2. Provision of appropriate technical infrastructure

A3. Implementation of a plan for system maintenance, support and replacement

A4. Implementation of a plan for the transfer of records to new storage media on a regular basis

A5. Adherence to appropriate storage and handling conditions for storage media

A6. Redundancy and regular backup of the digital objects

A7. Establishment of system security

A8. Disaster planning

2. Appraise Records for Permanent Preservation (A4.2)

In cases where, as recommended in the InterPARES 2 Chain of Preservation model, retention scheduling is employed, decisions on the disposition of records will regularly be made as part of the management of a recordkeeping system. In some cases, appraisals may be conducted when it is determined that records in a longstanding system need to reach a disposition. Eight important aspects of the appraisal process are discussed below.

2.1. Appraise early

Given the technical difficulties involved in the preservation of digital records, the identification of what records need to be preserved for the long term should be carried out at the earliest possible opportunity. Performing appraisal, establishing transfer methods and even identifying potential preservation strategies with the records creator will improve the likelihood of success. This process may also provide the preserver with an opportunity to offer records creation and maintenance advice (see Section 1.4).

Professional preservers, such as archivists, are frequently encouraged to participate in the actual design of computer applications being developed by organizations with which they have a donor-preserver relationship. This approach will help integrate appropriate recordkeeping and preservation practices. Preservers who have joined system design teams have learned that it is an enormously time-consuming practice that requires a far more detailed understanding of the organization's internal workflows and procedures than an archivist normally acquires during an appraisal. Furthermore, system specifications are rarely an accurate depiction of the application that will eventually be implemented. An appraisal will still have to be conducted once the system is operational and is meeting organizational requirements. It may be more reasonable for archivists to contribute to system design as part of the advice function discussed in Section 1.4. Sharing high level strategies, principles and guidelines developed by the archival profession may prove to be a more realistic goal.[35]

---

[35] Many aspects relating to the creation of effective digital preservation programs have been studied in recent years. Among the Web sites containing useful information or examples are: the InterPARES Project at http://www.interpares.org; Model Requirements for the Management of Electronic

2.2. Locate multiple owners

In cases where the intellectual components of a digital object have multiple owners, these owners must be identified during the appraisal process to assess the ramifications of this situation for long-term preservation. This can occur, for example, where institutions at various levels of government contribute, and share access to, data resources. Another example is illustrated by Web sites that access and use resources located outside their span of control. Although access agreements are frequently negotiated in these circumstances, they rarely include provisions for long-term preservation of all significant digital components.

2.3. Assess authenticity

The assessment of authenticity has always formed part of the traditional archival appraisal process. In the first instance, it has relied on confirming the existence of an unbroken chain of custody from the time of the records' creation to their transfer to the archival entity responsible for their long-term preservation. Periods when records were not subject to some form of protective measures by the records creator or by a successor institution with a vested interest in maintaining the accuracy and completeness of the records can cast significant doubt on the authenticity of the records.

The assessment of authenticity has also depended on the archivist's knowledge of recordkeeping practices, both historically and in relation to the record types and administrative procedures of a specific creator. The general framework for this assessment was originally codified in diplomatics.[36] A third, less frequently used method to confirm the identity and integrity of records is based on comparison. Records within a fonds are compared to copies forwarded to and held by external sources in the normal course of the creator's business.

Records created and maintained using digital technology present additional difficulties, and archivists have not yet developed standard practices to assess authenticity in this environment. Issues revolve around the fact that digital objects are easily duplicated, distributed, re-named, re-formatted or converted, as well as to the ease with which they can be falsified without leaving a trace. The following examples illustrate the extent of the loss to archivists, historians, lawyers and others who require authentic records in their work:

Records (MoReq) at http://www.cornwell.co.uk/edrm/moreq.asp; the Metadata Encoding and Transmission Standard (METS) at http://www.loc.gov/standards/mets/; the Electronic Records from Office Systems (EROS) at the National Archives of the United Kingdom at http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm; and the Australian DIRKS (Designing and Implementing Recordkeeping Systems) manual at http://www.records.nsw.gov.au/recordkeeping/dirks-manual_4226.asp.

[36] See discussion of diplomatics in Luciana Duranti and Kenneth Thibodeau (2006), "The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES," *Archival Science* 6(1): 15-21.

- The physical support on which digital documents are stored has largely lost its significance in confirming the date of a record or its place of manufacture. Anyone with access to functioning, obsolete equipment and storage media has the capability to copy digital files to, for example, 9-track tape or 5-1/4" diskettes.
- The date stamp on any digital file can be modified by adjusting the system clock.
- Few institutions understood what their employees would do once entrusted with word processing software. Standard document forms, such as memos and correspondence on letterhead, disappeared under the onslaught of new, individualized record forms, which rapidly included personalized colour, graphics and even sound effects, as well as the attribution of new meaning to capitalization, colour and the development of emoticons. The degree of erosion of standard records creation practices varied enormously across types and sizes of corporate and government organizations.
- The introduction of e-mail networks allowed records to travel by many new routes among staff, rather than according to the well-established distribution routes of traditional office procedures.
- The severe reductions in records management personnel in most organizations, fuelled by an assumption that digital objects somehow did not need to be managed, played havoc with the holdings of the Records Office, which largely stopped receiving records created and transmitted in digital form.

When appraising records created in a digital environment, the assessment of the authenticity of records must become a more overt, visible process performed and documented by the preserver. Unbroken chain of custody, knowledge of recordkeeping practices, and verification may still offer some assurances of authenticity. To these must now be added the verification of compliance with each of the benchmark requirements for authenticity listed in Section 2.4.

2.4. Document the assessment of authenticity

The appraisal report should document the controls put in place by the creator to guarantee the identity and integrity of the records and thus the presumption of their authenticity. These controls include each of the benchmark requirements supporting the presumption of authenticity.[37] Briefly, these include:

A.1 Expression of Record Attributes and Linkage to Record (e.g., identity and integrity metadata)
A.2 Access Privileges
A.3 Protective Procedures against Loss and Corruption of Records
A.4 Protective Procedures against Media Deterioration and Technological Change
A.5 Establishment of Documentary Forms
A.6 Authentication of Records

---

[37] See Appendix 21a.

A.7 Identification of Authoritative Record

A.8 Removal and Transfer of Relevant Documentation

2.5. Monitor records identified for long-term preservation

Once the appraisal is completed, the records identified for preservation must be monitored at regular intervals until such time as they will be transferred to the preserver. Monitoring involves confirming with the records creator that nothing has changed with regard to how classes of records identified for transfer are being created or maintained or, if changes have occurred, that they have not affected the nature and attributes of the records, their value, their authenticity or the feasibility of their preservation.

Many changes within an organization can affect the ongoing survival of digital records. The possibility that records will be destroyed in an instant is much higher than for traditional records. This danger is somewhat offset by the tendency to duplicate material in an uncontrolled fashion. Unfortunately, if the production of copies is uncontrolled, it is unlikely that anyone will realize when the last copy of a record is destroyed.

The simplest scenario may involve a system upgrade either to the hardware or to the software, which will affect the archives' ability to accept the records. An upgrade could also result in even minor system redesign that could remove the ability to separate temporary records from those that must be removed for transfer to the preserver.

A second scenario can involve changes in an organization's mandate or functions. This can easily lead to changes in how computer applications are used, and the nature and amount of data that they contain. People responsible for system re-design may not be aware of the requirement for transfer of the existing records to the designated preserver before the system can be modified. Without intervention, even documentation about the original application and backup tapes will move inexorably toward a scheduled destruction date.

Finally, the widespread collapse of proper records management practices in most organizations means that records are poorly identified and incorrectly stored in unsecured locations. Managers, and even records managers, may not understand the details of the technical infrastructure, while IT staff may be unfamiliar with either the history of an organization or the relative importance of older records in various data stores. Hard drives may be wiped, user accounts and all the files they contain may be deleted, tapes and discs may be recycled or destroyed, and obsolete playback technology may be disposed of to meet day-to-day operational requirements of speed and efficiency, with no understanding of the impact of such actions on an organization's records or on pre-existing transfer agreements designed to ensure their long-term preservation.

2.6. Update appraisals

Appraisals also need to be updated at regular intervals, though less frequently than records identified for transfer need to be monitored. Information gathered during a monitoring visit may provide the first indication that a new appraisal is required. Change within

organizations and within their record-making and recordkeeping systems is inevitable. Organizational mandates and responsibilities may change, as well as the way those responsibilities are carried out, and data accumulated in existing systems may be put to new uses, which might increase their long-term value. At the simplest level, systems that did not initially contain records may be upgraded to do so. This is particularly true during this period of "hybrid" recordkeeping systems, where paper-based record systems continue to co-exist with the early stages of digital information, document or record systems.

2.7. Identify all digital components[38]

Paper records kept in traditional recordkeeping systems generally offer a tightly-wrapped package, where the content of the record is firmly attached to its paper support and the record itself is contextually filed with the related records. This seamless system began to break down with the introduction of technology when, for example, photographic negatives had to be processed to produce prints and moving images resulted from multiple layers of sound and images, combined and re-combined to produce the final composite print that is screened in cinemas or broadcast on television.

Digital technology has further dismantled the record into a series of components. To successfully extract digital records from the system in which they were created, or even from a secondary maintenance system, the preserver must ensure that all essential digital components are identified and that implicit relationships are made explicit in the metadata before the whole construct is transferred. One of the most common examples of a digital component is the library of fonts, any number of which can be selected by the creator to be used in the presentation of a word-processed document. In Windows, these are stored in '.dll' (or dynamic link library) files. For the preserver to be able to reproduce this record to reflect the creator's original intentions, both the digital component containing the text and the digital component containing the font must have been preserved, as well as the link between them established in such a way that the software attempting to display the content of the text file can find the appropriate font library.[39]

2.8. Determine the feasibility of preservation

Although not part of the assessment of the value of the records, the appraisal process must be completed by a careful investigation of the technical preservation requirements for

---

[38] A digital component is defined as "A digital object that is part of one or more digital documents, and the metadata necessary to order, structure or manifest its content and form, requiring a given preservation action" (InterPARES 2 Terminology Database, op. cit.).

[39] A more detailed description of the "digital component," with additional examples illustrating the concept, is available in Preservation Task Force (2001), "Appendix 6: How to Preserve Authentic Electronic Records," in Duranti, *Long-term Preservation*, op. cit., 293–328. Online reprint available at http://www.interpares.org/book/interpares_book_o_app06.pdf.

preservation. Different preservation strategies (see Appendix 21c, Section B) can vary widely in cost and can produce very different results. A textual record stripped of all its formatting may be acceptable in a situation where the preserver is interested in carrying forward only the content of the record. However, where meaning is conveyed by the documentary form and the display characteristics of the record, a more complex preservation solution will be required.

A determination of the feasibility of preservation is essential if the preserving body is to clearly understand the cost of the acquisition and preservation to which it is committing. This is not a new activity; it is simply the extension to the digital realm of the identification of the resources needed to preserve, for example, paper records that are mouldy or moving image reels that are badly shrunken. The current state of digital preservation does mean, however, that preservation costs must be viewed as recurrent. Re-copying holdings from one physical carrier to another will be required as often as the selected format becomes obsolete. Conversion of file formats will be required when logical obsolescence threatens to make the content unreadable. In addition, the digital records considered for long-term preservation may require measures far too complex for the technological environment and the knowledge resources of the preserving organization, and this might imply a postponement of the transfer.

3. Acquire Selected Records for Permanent Preservation

The activity of the preserver acquiring selected records, and all the activities of preservation that follow from that, have as their goal the continued authenticity and accessibility of those records that are selected for continuing preservation. This movement of records from the creator's (or legitimate successor's) custody to the preserver's custody is a critical juncture in the chain of preservation and must be done with great care to ensure that nothing goes awry in the transfer process.

3.1. Develop shared plan for transfer

A successful transfer from the current custodian of the records (be it original creator or legitimate successor) to the organization or program taking on responsibility for long-term preservation requires a plan agreed upon by both parties. Re-accessing obsolete systems or extracting inactive records from operational systems will definitely involve human resource costs for copying time and, potentially, for programming time. Special hardware and software may also be required. The logical and physical (or virtual) formats used for the transfer must be agreeable to both parties. As a general rule, the transfer plan should be developed when the technical feasibility of acquisition and preservation are undertaken. If the two parties cannot agree on a transfer process, the appraisal decision may have to be re-visited. Again, in this period of hybrid recordkeeping, paper and microfilm-based options may still exist. Alternatively, the preserver might encourage the records creator to adopt upgrades to the record system that will allow for easier regular transfers.

3.2. Enforce standardized procedures

The controls over the transfer of digital records from the creator's to the preserver's custody must include:

- establishing, implementing, and monitoring procedures for registering the records transfer;
- verifying the authority for transfer;
- examining the records to determine whether they correspond to the records that are designated for transfer; and
- accessioning the records.

As part of the transfer process, the authenticity of the creator's records, which was assessed as part of the appraisal process, should be verified. This includes verifying that the metadata relating to the records' identity and integrity have been transferred together with the related records and are linked to them, and that the records are accompanied by any relevant documentation of the technical and administrative environment in which they were created and maintained.

3.3. Keep the oldest available logical format

The logical format[40] in which the records were originally created, or in which they are held by the creator at the time of transfer, should, whenever feasible, be maintained by the preserver, in addition to any preservation or reference copies generated after the transfer. Should selected preservation strategies, such as a specific conversion path, fail over time, continued custody of the initial logical format will allow the preserver to essentially re-start the preservation process with the most authoritative copy of the records, by applying a different preservation strategy to the records. Over the long periods during which preservers hold records, experience may show that other preservation strategies are more stable over time or can more easily be carried forward over the long-term. Alternately, new methods of preservation may have been developed following the acquisition and initial processing of the records.

3.4. Avoid duplicates

Because of the ease of replication of digital records, the preserver must put in place procedures to ensure that digital records from a specific series are transferred by a specific creator to the preserver only once. Accurate identity information is an important first step in avoiding duplication of effort by the creator and the preserver. Also, if reference copies are provided by the preserver to the creator after the transfer of the records, they should be clearly identified and marked as such to prevent accidental re-transfer.

---

[40] Logical format is defined as "The organized arrangement of data on electronic media that ensures file and data control structures are recognizable and recoverable by the host computer operating system" (InterPARES 2 Terminology Database, op. cit.). Two common logical formats for files and directories are ISO 9660 for CD-ROMs, and Universal Disk Format (UDF) for DVDs.

3.5. Document all processing

Initial processes applied during and immediately after transfer may or may not be related to preservation per se. Confirming the identity of the transferred material, checking for viruses and confirming completeness of files tend to leave the transferred file unchanged. File conversion, renaming digital objects and encapsulating files are more intrusive activities. In both cases, preservers must document all processing of digital records and the effects of processing while records are in their custody (see Appendix 21b, Requirement B.2). This documentation should include information such as:

- why certain processes were applied to the records;
- what records were processed;
- the date when the process was performed;
- the names of persons performing and documenting the various steps of the process(es);
- the impact of the process performed on the records' form, content, accessibility and use; and
- the description of any damage, loss or other problems encountered as a result of the processing, including any effect on the elements expressing the records' identity and integrity.

Should the preserver produce copies of the acquired records, it is important to remember that, as discussed in Section 1.5, these copies should be produced in an environment that satisfies the relevant requirements[41] from the InterPARES 1 Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records.

4. Preserve Accessioned Records

The designated records preserver is the entity responsible for taking physical and legal custody of, and preserving (i.e., protecting and ensuring continuous access to), a creator's records. Be it an outside organization or an in-house unit, the role of the designated preserver should be that of a trusted custodian[42] for a creator's records. The authentic copies of the creator's records are kept by the trusted custodian in a *trusted preservation system* (see Appendix 21c), which should include in its design a description and a retrieval system. This trusted preservation system must also have in place rules and procedures for

---

[41] Requirement A.5 (Establishment of Documentary Forms), where the creator establishes the documentary form of the record, would usually not apply to the preserver, except if the original documentary form of the record has been lost and the preserver must specify a substitute to permit access.

[42] A trusted custodian is defined in the InterPARES 2 Terminology Database as "A preserver who can demonstrate that it has no reason to alter the preserved records or allow others to alter them and is capable of implementing all of the requirements for the authentic preservation of records" (InterPARES 2 Terminology Database, op. cit.).

the ongoing production of authentic copies as the existing system becomes obsolete and the technology is upgraded.

4.1. Describe the records

The information about the records and their contexts collected during the appraisal and processing stages should form part of the archival description of the fonds or series in which the records belong (see Appendix 21b, Requirement B.3). This should also include information about intellectual property rights or privacy concerns.

The archival description of the fonds or series containing the digital records should include—in addition to information about the records' juridical-administrative, provenancial, procedural, and documentary contexts—information about changes the digital records of the creator have undergone since they were first created. The description should also include an overview of the transfer and preservation processes based on the documentation discussed in Section 3.5 and the explanation of the relationships among digital components discussed in Section 2.7.

4.2. Identify legal ramifications of preservation actions

When a preservation strategy is selected, its legal implications should be reviewed. For example, format conversion out of a proprietary environment could involve the preserver in illegal actions. In the United States, the *Digital Millennium Copyright Act* has made it a criminal offence to produce tools that can circumvent copyright protection measures. Internationally, the World Intellectual Property Organization Copyright Treaty (WIPO WCT) contains provisions that include copyright protection for software as well as digital works and that introduce criminal penalties for infringement, which ranges from unauthorized copying of material placed on a Web site to the removal or alteration of rights management controls from digital works. Most software packages also include some type of similar restrictions, which users must agree to during the installation process.

4.3. Confirm the effectiveness of the selected preservation strategy

As discussed in Section 2.8, there are now a number of preservation strategies available. Ideally, the selected preservation strategy should be tested on the records prior to the formal transfer to the preserver, to ensure that it will perform as expected. Realistically, most preserving organizations or programs can only fund this type of testing on an exceptional basis. Just as traditional conservators carefully test proposed treatments before applying them wholesale to analogue records, digital preservers must be constantly alert to the impact that each preservation process may have on the records and ensure that it is the appropriate choice for preserving authentic records. Flaws in application software and variations in the functionality of versions over time can result in unexpected consequences when applied to a new group of records.

Part of this process includes a constant awareness of the need to track the presence and the performance of all digital components. A change in one component may have unexpected

results on a second component, or it may affect how the relationship functions between any two essential components of the record or affect these components' ability to interact. A different relationship that could be affected is that which exists among the members of a related group of records, such as a dossier or series, and the presentation of that aggregate in the correct order (e.g., alphabetical, chronological or hierarchical). If the original order has been lost, corrective measures will have to be taken.

4.4. Maintain proper storage

It is a widely accepted archival preservation principle that maintaining an appropriate and consistent storage environment (temperature and relative humidity) for the material being stored is the most cost-effective contribution to the long-term preservation of records. Manufacturers of magnetic or optical storage media generally offer advice on optimum storage conditions. The environment must be monitored constantly and the readings checked on a regular basis. This recommendation is one of the eight mandatory maintenance strategies outlined in Section 1.7 and discussed in Appendix 21c, Section A.

5. Output Records

As noted earlier, continued accessibility (i.e., use) is an integral part of the archival process. Consequently, providing access to preserved records is an essential component in the chain of preservation. It should be managed by the preserver with the same sense of responsibility and degree of technical and professional competence imparted to records appraisal, acquisition/ transfer, description and storage.

5.1. Explain how the reference copies were made

The relationship between the records acquired from the creator and any copies produced by the preserver must be clearly described and readily accessible to users (see Appendix 21b, Requirement B.2.b). This should also include documenting how the reproduction process control measures that are in place were established and implemented and how they are monitored to ensure that the content of the reproduced records is not changed in the course of reproduction. Copies of records in the preserver's preservation system may not be designated authentic if the preserver has made them for purposes other than preservation; for example, a copy from which personal identifiers are removed may be made for access purposes.

Documenting the records reproduction process and its effects is an essential means of demonstrating that the reproduction process is transparent (i.e., free from pretence or deceit). Such transparency is necessary to the effective fulfillment of the preserver's role as a trusted custodian of the records. It also provides users of the records with a critical tool for assessing and interpreting the records by demonstrating the continuing authenticity of the records and by providing a complete history of the records, of which the history of reproduction is an essential part.

5.2. Explain the technical requirements for access

As mentioned in Section 1.1, different preservers provide reference services to different types of users. This will affect the reference formats and mechanisms adopted by the preserving organization or program, with simpler methods required for members of the general public who may not even own a computer or who may own a fairly simple machine with a few standard pieces of software. To meet the needs of these users, the preserver may have to undertake additional processing or create specialized tools to assist the researchers. More technologically

adept users, such as statisticians doing data analysis or forensic accountants conducting fraud investigations, are more likely to apply their own software tools to copies of the records.

Conclusion

This document has outlined a series of guidelines for institutions, organizations and programs with preservation responsibilities for digital records that can be presumed to be authentic and accurate while in the custody of the preserver. For individual preservers and small preservation organizations, the burden may seem great, but the alternative—loss of records or the emergence of corrupt and inauthentic records—would be an even greater problem in the long run. Small organizations will benefit by making a clear designation of the individual or individuals responsible for overseeing the preservation of the organization's digital records. Bear in mind, however, that not all recommendations presented in this document need to be implemented in each circumstance; each preserver should be able to select and adopt the measures that address its particular problems in the specific context in which it operates. There may also be cases in which additional measures are necessary because of legislative or regulatory requirements specific to the preserver's administrative or cultural jurisdiction. In such cases, consultation with legal experts may be required. Individuals, offices and small organizations responsible for preservation should not hesitate to contact such experts for advice on any issues relating to the preservation of the digital records in their custody and under their control.

Appendix E:
Template for mapping authenticity requirements to policy elements

Review the elements required for authenticity and long-term preservation of digital records in the first column. Map each element to a clause or paragraph in your existing records policies (column 2). Identify and elements that must be included in the digital preservation policy under development in order to ensure that all necessary elements are included.

Necessary elements for Authenticity	Accounted for in existing policies	Required in new policy under development
Accessibility • Choose software and hardware for interoperability; • Choose software that is backwards compatible; • Adopt official or *de facto* software standards; • Fully document all choices and any customization; • Choose widely used, non-proprietary, platform independent, uncompressed formats with freely available specifications where possible; • Choose lossless compression when compression is required		
Fixity • Digital records should have fixed form; stable content; • Documentary form must be retained as original (fixed within the confines of the system); • Endow records with bounded variability (established rules for the selection of content and documentary form that allow known, stable variations); • Establish essential intrinsic and extrinsic elements of each documentary presentation or form.		
Identity • Ensure the completeness of identity metadata:		

• Names of persons (author, writer, originator, addressee, recipient); • Title/subject (action or matter); • Documentary form (letter, report, etc.); • Digital presentation (format, wrapper, encoding, etc.); • Dates of creation and transmission; • Expression of documentary context (e.g., classification code, folder or directory, etc.); • Indication of attachments (if applicable); • Indication of copyright or other intellectual rights (if applicable); • Indication of the presence or removal of digital signatures; • Indication of other forms of authentication (e.g., corroboration, attestation, etc.) • Draft or version number (if applicable); • Existence and location of duplicate materials outside of the system (indicate which is the authoritative copy)		
Integrity • Ensure that digital materials carry information that will help verify their integrity; • Ensure the completeness of integrity metadata: • Name of handling persons/office; • Name of office/person with primary responsibility for keeping (may be same as handling); • Indication of annotations; • Indication of technical changes to either material or application; • Access restrictions (if applicable); • Access privileges (if applicable); • Vital record (if applicable); • Planned disposition.		
Organization • Organize digital materials into logical groupings (classification scheme, identity metadata).		
Authentication • Use authentication techniques that foster		

maintenance and preservation of digital materials; • Technology-independent vs. technology-dependent.		
Protection • Protect digital materials from unauthorized action.		
Backup • Protect digital materials from accidental loss and corruption; • Develop a rigorous policy or routine that ensures your system is backed up daily; • Choose and install the best backup technology for your situation.		
Obsolescence • Take steps against hardware and software obsolescence.		
Awareness		

Appendix F: Exercise #1 Discussion Points

Strengths

- Language is clear and concise.
- The policy is grounded in its administrative and juridical contexts, by referencing relevant university policies and legislation.

Weaknesses

- The Scope section only declared what records are subject to the policy, but does not specify what individuals or departments are subject to the policy.
- The Policy Statement section includes information that is technology-dependent and better contained within a guidance or procedural document.
- Lacks information that should be contained in the following sections: Definitions, Contact Information and Version Control.

Appendix G: Exercise #2 Discussion Points

Policy or guideline? This document is identified as a policy and a guideline, and is ambiguous in its purpose. As it is written, it is not enforceable.

Roles and responsibilities:

Section 1.1 states that the "guideline" is for records owners, IT managers and action officers/users. How does this policy define record owners? Records owners and IT managers do not have the same responsibilities and these should be outlined separately. The roles and responsibilities section omits any reference to action officers/users. What is their role in implementing this policy? All stakeholders responsible for implementing the policy need to be identified and their roles and responsibilities outlined.

Definitions: The definition section as it exists currently is not comprehensive enough to ensure that the policy can be followed and enforced. Concepts of metadata, appraisal, destruction, authenticity and archival value, business information systems and recordkeeping systems should be included in the definition section.

Scope section: Clarify the scope of the policy – identify the extent of records covered by the policy and the stakeholder groups responsible for its implementation.