InterPARES 3 Project

International Research on Permanent Authentic Records in Electronic Systems

in saeculis authenticus

Title: Case Study 08 – North Vancouver Museum and Archives (NVMA): Customizable Versions of Products

Brochure 2. Maintaining Digital Records: Business Edition

Status: Final (public)

Version: 1.0

Last Revised: October 2010

Author: The InterPARES 3 Project, TEAM Canada

Writer(s): Cindy McLellan
School of Library, Archival and Information Studies,
The University of British Columbia

Shamin Malmas
School of Library, Archival and Information Studies,
The University of British Columbia

Project Component: Knowledge Mobilization

URL: http://www.interpares.org/display_file.cfm?doc=ip3_canada_cs08_brochure-2.pdf

Document Control

Version history			
Version	Date	By	Version notes
1.0	2010-10-15	C. McLellan, S. Malmas	First public version.

Maintaining Digital Records: Business Edition

These guidelines have been developed to help businesses and small organizations with formalized structures understand and preserve their digital records. Keeping good records is an important part of being accountable to customers, government, members, and the public. The preservation of digital records requires more planning and periodic intervention than is necessary for traditional records. This guide offers practical advice and tips for preserving digital information that can be applied with minimal resources.

By following the steps outlined below, you are increasing the possibility that you will have accessible, authentic, usable digital records in the future. That is the immediate benefit. If your well-cared-for records find their way into an archival repository the community as a whole benefits.

Practical steps

Step 1: Appoint a trusted custodian

Depending on the size of the organization, this may be one person (secretary or records clerk) or a team of people (records department). The trusted custodian is responsible for the maintenance and care of essential records (for example, meeting minutes and financial records). It is necessary for the trusted custodian to build a good relationship with whomever you rely upon for IT expertise. The trusted custodian should communicate software and hardware needs and recordkeeping concerns to this individual.

Depending on the structure of the organization, it may be appropriate to add a clause requiring digital records preservation to its by-laws and/or policy and procedure documents.

Step 2: Understand the records

- Inventory the digital records and take note of how they are organized;
- Create a document explaining the record keeping system (this will most likely be a complex document detailing the hierarchical structure of how the documents are filed in folders, or how e-mails are distributed in directories);
  - Make sure this document is updated and known to at least one other trusted individual, and that it is formally approved by the top management.
  - Include information about retention schedules in this document.
- Know what legislation applies to the records you create. For some organizations the *Societies Act [R.S.B.C. 1996],* and/or *Personal Information Protection Act* will apply.
- Manage e-mail; it is necessary to develop criteria for keeping and maintaining e-mail over time. Records important to the operation of your organization may arise out of e-mail threads and need to be treated as such.

  - The nature of e-mail has blurred the boundaries between private correspondence and business records.
  - The management of e-mail requires unique solutions based on your specific business or organization. Effective and efficient e-mail management is part of good record keeping practices. Please refer to the brochure “Managing E-mail” for more information.

Step 3: Understand the technological properties of the records

- List the digital records formats you use and the media on which they are stored. Keep this document up to date.
- Keep the original documentation or manuals related to the software and hardware used.
- Make a plan for changes that should be made within the next few years (see *Step 5a: Preventing loss* for more information).
- If the business requires specialized software and/or hardware, be aware of changes in the industry.
- Think about where important digital records are stored:
  - Is there important information on floppy disks? How old are they? Is the information still accessible?
  - Is there important information stored on CDs? Are they gold standard?

Step 4: Plan for hardware and software obsolescence

Software and hardware typically become obsolete after five years. To avoid losing your records it is important to:

- Frequently upgrade the technology you use to create and maintain your records
  - This is necessary because backward compatibilities have limits. For example, the latest version of MS Word is only compatible back to 1997.
- Migrate files from obsolete media to current media
  - If your organization uses older storage media (such as 3.5 inch floppy disks), it is time to update these practices as the ability to move this information to current media storage is rapidly decreasing. As 3.5 inch floppy disks have become obsolete so will CDs.
- Consider saving records in a fixed form, which will help ensure stable content.

Avoid obscure formats!
If you currently use obscure (non-standard) formats be aware that this can be a preservation risk. Support for non-standard formats could disappear rapidly. As part of knowing your records make plans to move to standards or to well known and widely used computer file formats that are considered de facto standards, such as PDF, TIFF, DOCX, WAV, and AIFF.

Warning!
Heat, light, and moisture are all enemies of long term digital storage media.
Find a cool, dark, secure place to keep all your floppies, CD's, and other storage media, until you have a plan in place to deal with their contents.

Step 5: Preventing loss

If your hard drive crashes you could lose all of your records.

- Develop a back up strategy based on your organization's size and budget.
- Educate yourself on the best practices for your organization's records.

There are two main strategies for preserving digital records.

Strategy 1: Backup copy

A backup copy is a copy of all the systems, applications and records on your computer's hard drive. Backup is typically done using an external hard-drive or a mirroring system. The purpose of this copy is to enable you to reconstruct the entire configuration of your computer.

- Use a RAID (Redundant Array of Inexpensive Disks), or a mirroring hard-drive technology ($500-$800).

Strategy 2: Safety Copy

A safety copy is the copy of the records vital to the daily operations of the business organization. The purpose of the safety copy is to ensure the survival of the records that you deem to be the most important.

- Use one or more external hard drives ($150-$300)
- Use one or more USB keys ($20-$50)

Things to consider

Location of backup copy and safety copy: It may be appropriate to have two safety copies, one on an external hard drive and one on a USB key stored in two separate locations, such as in a safe deposit box or fire-proof safe.

Life of backup copy and safety copy: Technology does not remain stable. It is important to keep updating the back up and safety devices. USB Keys, CDs, and other storage devices may break and the information on them will degrade overtime.

Security: Digital records are very susceptible to accidental, unauthorized or malicious alteration. To help safeguard records against these concerns consider saving finalized documents in widely used stable, hard to modify, file formats like PDF, so they remain accessible over time and cannot be accidentally or intentionally changed.

Password protect all business computers and enforce security to protect the records of the business. Mobile devices, such as personal data devices (PDAs) and laptops, which often leave company facilities, are particularly susceptible to theft and accidental loss. Employee awareness and adherence to company policies will help mitigate this risk.

Avoid lossy compression: Some file formats use lossy compression to store items at a smaller file size than the original in the process losing some information, such as .JPEG. Instead, consider saving your photographs using TIFF.

Definitions

Backward compatibility: The ability of some software to correctly interpret and present digital components of records created with previous versions of the same software.

Fixed form: A file type that ensures the documentary appearance or presentation of the record is the same each time the record is retrieved. For example, PDF and TIFF.

Retention schedules: A timetable that specifies the length of time certain records are to be kept. Please see ARCS and ORCS, under "Additional resources" at the end of this guide, for more information.

Stable content: The quality of a record that makes the information and data contained in it immutable (it cannot be overwritten, deleted, added to or changed), and allows for changes to be made only by appending an update or creating a new version.

Trusted custodian: A preserver who will not alter the records or allow others to alter them. This person is responsible for ensuring the preservation of the records over time.

Additional resources

InterPARES 2 Project. *Creator Guidelines: Making and Maintaining Digital Materials: Guidelines for Individuals.* http://www.interpares.org

InterPARES 2 Project. *Preserver Guidelines: Preserving Digital Records: Guidelines for Organizations.* http://www.interpares.org

A copy of the Society Act [RSBC 1996] can be found by visiting http://www.bclaws.ca

For information about PIPA (Personal Information Protection Act) (in BC) visit the Web site of the Office of the Information & Privacy Commissioner, http://www.oipc.bc.ca/

Administrative Records Classification System (ARCS)
http://www.lcs.gov.bc.ca/CIMB/arcs/admin/main.asp

Operational Records Classification Systems (ORCS)
http://www.cio.gov.bc.ca/services/records/ORCS/default.asp

InterPARES 3 Project. *Consider donating your records to **[Institution name]***. **[Institution name]** brochure series.

InterPARES 3 Project. *Managing E-mail*. **[Institution name]** brochure series.

InterPARES 3 Project www.interpares.org

[Institution contact information]

InterPARES 3 Project
International Research on Permanent Authentic Records in Electronic Systems
TEAM Canada