

Digital Archives Preservation Strategy

1. Introduction

The digital preservation strategy of the Digital Archives of Georgia (DAG) relies on migration, emulation, and the use of analog preservation alternatives (namely microfilm) in combination with the promulgation of standards and best practices, and partnerships with other interested parties to ensure the preservation of the state's historical records.

This preservation strategy is written in support of the Georgia Archives digital preservation policies and details the types of activities that will be undertaken to ensure the reliable preservation of digital records. Like the policies, it will be updated and revised as the DAG develops and as technology changes. It should be emphasized that the Archives is employing a mix of strategies combined with responsible storage and maintenance decisions in acquisition and appraisal in order to reduce both risks of losing access to digital resources in the short-term and costs of preserving access to them in the long-term.

2. Preservation Strategies

2.1 Archival Storage of Digital Records

The Georgia Archives will employ the use of technology-neutral¹ specifications that will ensure the greatest flexibility in maintenance and retrieval of records and management of costs over time. Non-standard (proprietary) file formats that may be accepted for transfer outside of existing acceptable format policies will be converted at the time of transfer to a non-proprietary format wherever possible. A minimum of three copies of a digital object will be maintained within the DAG:

- The original bit stream,
- A preservation copy (in a non-proprietary file format), and
- A presentation copy (multiple presentation copies may be maintained to provide un-redacted access to agency staff and redacted access to the public)

The original bit stream of all digital records will be preserved as part of the preservation strategy to ensure that emulation of original software configurations remains a viable option for presenting records in the future (see section 2.3 for a discussion of Emulation). The selection of a preservation strategy – primarily migration or emulation – will be based on risk assessments conducted during ingest and again in the future when the preservation copy is converted to a new file format.

2.2 Migration

The migration of digital information refers to the periodic transfer of digital materials from one hardware/software configuration to another, or from one generation of computer technology to a subsequent generation. This term is sometimes used to refer to the transfer of information to non-digital media.

¹ Technology-neutral specifications are not predicated on any individual technology. The DAG storage solution will combine various technologies and vendor solutions to manage costs over time.

2.1.1 Migrating to Alternative File Formats

One approach to preserving access to digital information entails its migration to standard formats which are expected to be less volatile than the format in which the digital objects were originally created. However, it is important to understand that technical standards are in a state of flux and this strategy cannot be solely relied upon to ensure that digital information remains accessible. The selection of a format for preserving digital objects will depend upon what functionalities of the specific file format in question will be required in the future. For example, decisions need to be made as to whether there will be a need to process or edit a digital object in the future or if the visual presentation alone should be preserved. These decisions will be made initially at the time of ingest and again evaluated when the preservation copy of the record is converted to newer technology.

2.1.1.1 Reformatting and Conversion to Standard Formats

File formats, like storage media, are subject to rapid obsolescence and evolution, and the process of selection and assessment of options for preservation is largely one of risk reduction. Use of file formats which have been well documented, have undergone thorough testing, and are non-proprietary and usable on different hardware and software platforms minimizes the frequency of migration and reduces the risk and costs in their preservation. Similarly, utilizing formats which have been widely adopted minimizes risk as it is more likely that migration paths will be provided by the manufacturers and a degree of "backward compatibility" will be available between versions of the file format as it evolves.²

Although non-proprietary formats can be selected for many resource types, this is not universally the case. For many applications, such as Geographic Information Systems, only proprietary formats are available. In such cases a crucial factor will be the export formats supported to allow data to be moved out of (or into) these proprietary environments. Export formats will be identified and set as a technology standard within Georgia government as a means of enabling the preservation of Geographic Information System records.

To the extent possible, the Archives has identified file formats which are preferred for archival storage and will seek deposits in that form wherever a choice of formats exist. This list, included in Appendix 1, will be updated as the development of the DAG progresses.

2.1.2 Refreshing

The term "migration" also encompasses refreshing, that is, copying digital information onto new storage media without changing the original file format. However, while refreshing will overcome the problem of media instability, it usually isn't enough to prevent technological obsolescence³.

² It is important to note that backward compatibility is rarely maintained for more than one or two previous versions and that the "window of opportunity" to migrate is therefore relatively brief.

³ Technological obsolescence is the result of the evolution of technology: as newer technologies appear, older ones cease to be used. For example, new media for storing digital information rapidly replace older media and reading devices for these older media become no longer available. Newer versions of software constantly render older versions obsolete and the hardware required by this software also changes over time. Consequently, information which relies on obsolete technologies becomes inaccessible.

Two primary factors trigger a migration. Internally, the DAG may undergo a major technological change, such as a change to a new operating system, triggering a migration of the data and records within the DAG. Externally, a change in technology, enabling a better way of providing access to digital records, may trigger a migration. Below, is a table listing the advantages and disadvantages of using migration as a long-term preservation strategy. The table also includes key programmatic requirements that must be in place to ensure adequate documentation of the process and protect the reliability of the records.

| Advantages | Disadvantages | Programmatic Requirements |
|---|---|---|
| Procedures for simple migration are well established | Cost - requires special program to be written for complex migrations | Written policies and guidelines, including selection policy for materials to be migrated |
| Is currently the preferred strategy for most digital archives | May compromise the integrity of the originals unless stringent quality control procedures to ensure authenticity are in place | Written quality control procedures including testing the migration program with a sample of records or bit/byte or checksum comparisons of migrated and original data |
| May become simpler as technology advances and range of platforms diminishes | Likely to lose some functionality, look and feel of original | Rigorous documentation of migration procedure |
| | Can be time-consuming and complex | Preservation metadata and documentation |
| | More complex digital resources may be migrated with significant loss of functionality | Migration required whenever there is a software upgrade or a new software application is installed |
| | Needs to occur at regular intervals throughout the life of the object | |

2.3 Emulation

Emulation refers to the process of mimicking, in software, a piece of hardware or software so that other processes think the original equipment/function is still available in its original form. Emulation is essentially a way of preserving the functionality of and access to digital information which might otherwise be lost due to technological obsolescence. Because it is impossible for any organization to retain working examples of every computer and every piece of software, and because the cost of any attempts to do so would be prohibitive, emulation may offer a viable alternative strategy to ensure access to digital information in the future⁴.

One of the benefits of the emulation strategy compared with migration is that the original data need not be altered in any way. It is the emulation of the computer environment that will change with time. This should help maintain the integrity and "look and feel" of the material. Another advantage of implementing emulation is its possible efficiency. Once the data is archived with appropriate metadata and software, no other action is required apart from media refreshing until access is desired. One emulator can also be used as a solution for several data objects requiring the same operating environment.

⁴ Note: Emulation does not have as solid a track record as migration and the Georgia Archives will use it only as a last resort should migration prove unfeasible.

| Advantages | Disadvantages | Programmatic Requirements |
|---|--|--|
| Recreates the functionality, look and feel of the original | Is still in the research stage and requires further practical testing. May only be able to emulate part of the functionality, look and feel of the original | Appropriate storage and maintenance procedures |
| Avoids repeated costs associated with migration (though see also disadvantages) | Is likely to be very costly unless it has economies of scale. New emulators need to be built for major computer paradigm shifts; it is possible that these costs may even exceed the savings of repeated migration costs | Written policies and guidelines |
| May offer the best prospects for more complex digital resources | Software copyright issues need to be addressed and may be extremely complex | Preservation metadata |
| | There must be rigorous documentation of hardware and software requirements. These have rarely been documented to this level of detail in the past and would require concerted effort and resources | Detailed documentation on hardware and software specifications |

2.3 Analog Preservation Alternatives

Migration and emulation dominate current options for preserving digital resources long-term. Both have champions and detractors, both have acknowledged difficulties. The need for both may also be deferred and/or simplified if appropriate preventive preservation procedures, such as storage and maintenance and selected secondary preservation strategies, have been used. On such secondary preservation strategy, transfer to an analog preservation format, such as paper or microfilm, differs from the other strategies in two important ways:

1. It can only be considered for a relatively small category of digital objects (namely digital images, word processing files, and spreadsheets) and is patently inappropriate for the increasing numbers of more complex digital objects being created.
2. By its nature, it loses the digital characteristics of the objects converted and is therefore a *preservation strategy for digital resources*, as opposed to a *digital preservation strategy*, where the essential aim is to retain the digital characteristics of the object. This latter is preferred.

| Advantages | Disadvantages | Programmatic Requirements |
|---|--|--|
| Is no longer vulnerable to technological obsolescence assuming preservation quality microfilm or permanent paper is used | Loses functionality of original digital resource | Policies and guidelines clearly documenting rationale for adopting strategy and category of resources it may be used for |
| Should be a "once only" cost for conversion | Can only sensibly be considered as an option for digital resources which do not utilize or require the full functionality of digital technology | N/A |
| Will guarantee accessibility for hundreds of years provided it is converted to an archival standard and stored in archival conditions | Costs of conversion to archival standard and storage in archival conditions (the latter cost will be recurrent and the cumulative cost will be significant over time) | N/A |
| May be a pragmatic interim strategy pending the development of infrastructure for more appropriate digital preservation strategies | Cannot be considered for more complex digital resources where loss of functionality would at best diminish, if not destroy, the usefulness and integrity of the resource | N/A |
| May be appropriate for vast majority of current digital objects (which are not interactive) | Loses functionality of original digital resource | N/A |

While acknowledging that the use of analog preservation formats are not the preferred method for preserving digital records, the Georgia Archives also acknowledges that loss of historical records is not an option. The use of such alternative preservation strategies is meant as a failsafe, particularly during the early years of program development.

2.4 Standards Compliance

Adherence to stable and widely adopted open standards when creating and archiving digital resources may also be desirable. These standards are not tied to specific hardware/software platforms and can prevent or delay the loss of digital objects due to technological obsolescence. Identification of best practices within each standard demonstrates the benefits of standards adherence and encourages compliance by government agencies.

| Advantages | Disadvantages | Programmatic Requirements |
|--|--|--|
| Using stable open standards will delay the time when more costly strategies are needed | Proprietary extensions are relatively common and generally not as well documented as the standard itself | Written guidelines on preferred and acceptable standards |
| Using stable standards will reduce the complexity, and therefore costs, of longer-term preservation strategies | Dependent on creators being able and/or willing to comply or later conversion by the archive | Knowledge of all relevant standards for all categories of digital resources must be maintained |
| Can simplify migration and achieve economies of scale in migrating similar items | Stable standards are not available for some formats | Close partnership and involvement in standards process at the Georgia Technology Authority |
| | Even when stable standards do exist, they are themselves subject to inevitable change as they evolve into new versions | |

2.5 Collaborations and Partnerships to Preserve Digital Records

The final preservation strategy of the Digital Archives is not a procedure or process but a program initiative. The Georgia Archives is one of many players with an interest in ensuring that the state's documentary heritage is preserved and accessible. Others with such an interest may include local, state and municipal agencies, libraries, universities, and organizational archival/historical agencies. The Archives seeks to work with others who are taking or could take responsibility for preserving and providing access to Georgia's digital information resources. In working with such partners the Archives wishes to:

- Identify appropriate partners and stakeholders able to contribute to the statewide effort
- Establish agreements on responsibilities and roles
- Pursue agreements that provide a reliable basis for ongoing accessibility over time
- Help identify and develop policies, procedures and tools to support such an aim
- Work with creators, publishers and re-users of digital content to encourage practices that will enable, rather than hinder, preservation
- Work with government agencies and officials to develop legislative and funding frameworks that will enable cost-effective preservation.

3. Implementing a Digital Preservation Program

As stated in the introduction, the digital preservation strategy of the DAG relies on a combination of preservation strategies. At its base, the promulgation of key standards guides the creation and maintenance of digital records in the agency. Once in the custody of the Archives, the preservation strategy will be implemented as part of a well-defined process. Types of activities undertaken to ensure the preservation of digital records include:

1. Assessing the risks for loss of content.
2. Evaluating digital records to determine what type and degree of format conversion or other preservation actions should be applied.
3. Ensuring continued access to digital objects.

3.1 Risk Assessment

3.1.1 Technology Risk Assessment

The certainty that there will be frequent technological change poses a major challenge. Precautions can, and should, be taken which will greatly reduce the risk of inadvertently losing access to a resource because of changes in technology. These include:

- Using standard file and media formats, as recommended by reputable sources, particularly those approved by a formal standards-making body.
- Providing detailed documentation to enable the context to be determined and also to facilitate successful management.

A technology risk assessment attempts to detect the timing and likelihood of changes in technology environments and file formats that will affect the accessibility and long-term preservation of digital records. Risks may vary according to:

- The content of the record;
- The formats in which the record has been created;
- The ability to support hardware and software necessary to render the record usable;
- The needs of the agency creator and users for the records;
- DAG budgetary constraints, and;
- The organization of management activities in the DAG.

The completion of a risk assessment of technology and file formats determines what environments are needed for the most reliable access to the records and what actions need to be taken on a regular basis to ensure preservation of digital records. This risk assessment will take into account the content of the digital record and the needs of the agency creator. The technology environments and the preservation action plans provide alternatives for future accessibility of the digital records.

A technology environment is a set of applications, operating systems, and hardware needed to render the content of a digital record. Technology environments for all digital records accepted into the DAG will encompass:

- The current environment in which the record was created/rendered, and
- A preservation environment into which the record will be moved as technology changes or becomes obsolete. To the extent possible, the preservation environment will be based on open-source technology specifications.

As changes in the technology environment occur, the preservation action plans may recommend changes to, or emulation of, the current environment and/or migration of the data to a new file format.

3.1.2 Records Risk Assessment

A records risk assessment evaluates the probability that work processes of the DAG will fail to preserve the original bit stream (because of the use of a proprietary format for instance) or will compromise the reliability of the record (because of inadequate security protecting the DAG, for

example). A risk assessment will provide staff with a decision making tool that will be used in evaluating the proper time to convert data to a new physical storage medium or to a different software platform. This risk assessment will take place each time media renewal and error checking processes are completed for the original bit stream storage media.

3.2 Evaluating Digital Records

3.2.1 Options for Transfer and Accessioning

To the extent possible within Georgia's government culture, the Archives will limit the range of file formats and storage media accepted in the DAG. Procedures for the transfer of physical media (CDs) and for the transfer of data via File Transfer Protocol (FTP) have been issued separately for use by agencies (See http://www.sos.ga.gov/archives/who_are_we/rims/digital_History/default.htm). A table outlining options, issues and requirements that was compiled to assist in making this decision is included in Appendix 2.

3.2.2 Quality Assurance

Quality assurance checks will be carried out at the time of transfer on the medium, content and structure of deposited digital objects, and on any accompanying documentation. Quality assurance procedures may be adapted in the light of the volumes of material and staff resources available. Where possible, procedures will be automated but others can only be undertaken manually. Such checks may include:

- Scanning for computer viruses.
- Checking media and files can be read.
- Checking completeness and accuracy of paper based or digital documentation.
- Checking description and intellectual content of the resource.
- Checking structure and formatting of the resource.
- Procedures for documenting validation checks and any discrepancies encountered.
- Procedures for checking and if possible resolving discrepancies with the supplier.

3.2.3 Preservation Action Plans

Decisions regarding the use of a particular preservation strategy and about what aspects of the material to be preserved (e.g. functionality, presentation) will be made through the development and use of preservation action plans. Such plans will be developed for selected file formats that are determined, through formal risk assessments, to be at risk of loss or corruption. The plans will document the preservation approach, including actions that are considered necessary for immediate, short-term, and long-term preservation. All preservation plans will consider the production of microfilm as an analogue preservation medium and will evaluate its practicality. Each plan will be based in part on risk assessments and costs analysis.

3.2.4 Preservation Metadata⁵

⁵ Other metadata which may be necessary, for example, to provide access, are not addressed in this policy.
Rev. 08/23/2007

Preservation metadata is information that supports and documents the long-term preservation of digital records. It addresses the record's provenance and custodial history, and forms the basis for authenticating and validating a historical digital record. The challenge in developing a preservation metadata schema is to anticipate what information will actually be needed to support a particular digital preservation activity and particular preservation goals. The Archives will base its preservation metadata schema first on the high-level information recommended by the Open Archival Information System (OAIS) model and secondly on the work completed within the Preservation Metadata Implementation Strategies project (PREMIS) of the Online Computer Library Center (OCLC) and the Research Libraries Group (RLG). The categories of metadata gathered will include:

- Representation information
- Preservation description information (which can be broken down into reference, context, provenance, and fixity information)
- Packaging information
- Descriptive information

As the DAG program expands, the metadata schema(s) will be evaluated to ensure that the appropriate metadata has been and is being collected.

3.3 Access Continuity Assurances

3.3.1 Backup

Backups are created and maintained locally and offsite according to the following guidelines:

- New and changed content and metadata are immediately and redundantly logged to disk
- Recurring backups to non-disk media occur at systematic intervals throughout each day and are stored locally
- Daily incremental backups are maintained for an extended period of time and stored locally
- Weekly full system backups are stored at offsite facilities located a minimum of ten (10) miles from the DAG main facility.

In the event of a failure, the potential data loss depends on the nature of the failure. Two potential failures that could occur and their outcomes are listed below:

- A localized system failure could result in a loss of data that had not yet been backed up via a recurring backup to tape. This loss would be a few hours of data.
- A worst case catastrophic local disaster could result in the potential loss of several days' worth of data (data that had been transferred to the FTP site but not ingested into the DAG). Data within the DAG would have to be restored from weekly offsite backups. The recovery time frame in any disaster involving retrieved backups depends on the nature of the failure, the quantity of data involved, and whether restoration is from on-site or offsite copies of data.

3.3.2 Disaster Prevention and Recovery

The goal of a disaster plan is to safeguard the data (content and metadata) in the Digital Archives and to safeguard the DAG's software and systems. For the purposes of disaster planning, all data is considered of equal value.

There are manual and automatic system restart and recovery processes in place for the Digital Archives in case of unintended power failures, and node, server, individual process or other outages. Failover capabilities (redundancies) exist at three levels: network, host, and disk. The DAG will maintain a business continuity solution via a remote site that provides hardware and software to run services (primarily web-based services)⁶. Regular tests will be carried out with that facility. If all major Georgia Archives systems go down in a disaster situation, other systems may be restored before the DAG. If other systems are restored first, the DAG system functions will be restored within forty-eight hours thereafter. It may take up to several weeks to restore access to DAG content stored before the disaster occurred.

3.3.3 Succession Plan

One of the attributes of a trusted digital repository is organizational viability. Preservation of digital objects in the DAG is the responsibility of the Georgia Archives. Should the Georgia Archives discontinue the DAG for any reason, the following options will occur:

- The contents will be returned to the agencies in an agreed upon manner, or;
- A partner digital archive program will be asked to assume responsibility for the contents, or;
- Content capable of being preserved as microfilm or printed out on paper will be preserved in an alternate media.

⁶ Note: Presentation copies may remain available as the DAG itself is recovered.
Rev. 08/23/2007

Appendix 1

File Formats for Preservation

Narrowing the range of file formats handled will streamline the management process and reduce preservation costs. It will also reduce the ongoing cost of software licenses required by the Archives. In considering storage and preservation it is helpful to recognize that it can be a desirable strategy to distinguish between formats (or versions) used for archiving and access on the basis of different requirements. E.g. it would be appropriate to store a high resolution image as a TIFF master file (archival format), but to distribute the image as a JPEG file (access format) of smaller size for transmission over a network. It would not be appropriate to store the JPEG image as both the access and archival format because of the irretrievable data loss this would involve.

The speed with which many file formats evolve and the degree to which even well documented standard formats can be extended by proprietary additions or modified/adapted for specific applications by users also has significant implications for preservation, and in particular for good preservation metadata and system documentation

| Media | High Confidence Level | Medium Confidence Level | Low Confidence Level |
|--------------|---|---|---|
| Text | <ul style="list-style-type: none"> -Plan text (encoding: US-ASCII, UTF-8, UTF-16 with BOM) -XML/XSL/XHTML, etc: with included or accessible schema and character encoding explicitly specified) -PDF-A-1 (ISO 19005-1) | <ul style="list-style-type: none"> -Cascading Style Sheets (CSS) -DTD -Plain text (ISO 8859-1 encoding) -PDF (embedded fonts) Rich Text Format 1.x -HTML 4.x (include a DOCTYPE declaration) -SGML -Open Office -Office Open XML | <ul style="list-style-type: none"> -PDF (encrypted) -Microsoft Word -WordPerfect -DVI -All other text formats not listed here |
| Raster Image | <ul style="list-style-type: none"> -TIFF (uncompressed) -PNG | <ul style="list-style-type: none"> -BMP -JPEG/JFIF -JPEG2000 (prefer lossless or uncompressed) -TIFF (compressed) -GIF | <ul style="list-style-type: none"> -MrSID -TIFF (in Planar format) -FlashPix -PhotoShop -All other raster format not listed here |
| Media | High Confidence Level | Medium Confidence Level | Low Confidence Level |
| | | | |

| | | | |
|----------------------|--|--|---|
| Vector Graphics | -SVG 1.1 (no Java binding) | -Computer Graphic Metafile (CGM, WebCGM) | -Encapsulated Postscript -Macromedia Flash -All other vector image formats not listed here |
| Audio | -AIFF (PCM) -WAV (PCM) | -SUN audio (uncompressed) -Standards MIDI -Ogg Vorbis -Free Lossless Audio Codec -Advance Audio Coding -MP3 (MPEG-1/2, Layer 3) | -AIFC (compressed) -NeXT SND --RealNetworks 'Real Audio' -Windows Media Audio -WAV (compressed) -All other audio formats not listed here |
| Video | -Motion JPEG2000 (ISO/IEC 15444-4) -AVI (uncompressed) -QuickTime Movie (uncompressed) -Motion JPEG2000 | -Ogg Theora -MPEG-1, MPEG-2 -MPEG-4 | -AVI (compressed) -QuickTime Movie (compressed) -RealNetworks 'Real Video' -Windows Media Video -All other video formats not listed here |
| Spreadsheet/Database | -Delimited Text -SQL DDL | -DBF -OpenOffice -Office Open XML | -Excel -all other spreadsheet/database formats not listed here |
| Presentations | | -OpenOffice -Office Open XML | -PowerPoint -All other presentation formats no listed here |

1. File formats listed as high confidence will be used as preservation formats.
2. No files with viruses will be accepted (refers especially to these file formats: DOC, XLS, MDB, PPT, ZIP, EXE). Files should be scanned for viruses with up-to-date virus scanners before being transferred.
3. No fully encrypted files will be accepted.
4. No compressed files will be accepted.

5. No files using Digital Rights Management controls will be accepted.
6. It is acceptable to transfer files in the unencrypted ZIP (*.zip) format to the DAG. Upon receipt at the Georgia Archives, the ZIP files will be restored to their original formats and archived accordingly.
7. As a general rule, use platform-independent, vendor-independent, non-proprietary, stable, open, and well-support formats.

Appendix 2

Options for Transfer and Accessioning of File Formats and Storage Media

| Options | Issue | Requirements |
|--|---|--|
| | | Policy on storage formats |
| | | Watch technologies for developments in storage formats (all options) |
| <p>Limit range of file formats received</p> <p>Limit range of media received (most cost-effective long-term option)</p> | <ul style="list-style-type: none"> ▪ Simplifies management and reduces overall costs ▪ Agency may lack resource or expertise to comply ▪ Wide variety of file formats used and proprietary extensions to open standards ▪ Media used for transfer potentially can be used for long-term storage | <ul style="list-style-type: none"> ▪ Guidelines on preferred formats ▪ Degree of influence over transfer ▪ Outreach and collaboration strategies to achieve desired outcomes ▪ Guidelines on preferred transfer media and transfer procedures |
| <p>Accept as received but convert to standard file format</p> <p>Accept as received but convert to standard storage media format</p> | <ul style="list-style-type: none"> ▪ Simplifies management and reduces longer term costs ▪ May not be technically feasible to convert to standard format ▪ It will be necessary to check that accidental loss of data has not occurred | <ul style="list-style-type: none"> ▪ Archives must have statutory preservation rights. ▪ Resources and technical expertise of Archives ▪ Election of preferred formats ▪ Documentation of native formats to allow conversion ▪ Integrity checks for conversion process. |

| | | |
|---|---|--|
| <p>Accept and store as received (least cost-effective option long-term despite lower initial costs)</p> | <ul style="list-style-type: none"> ▪ Complicates management and increases cost of managing resources over time ▪ High risk options, particularly if large numbers of digital objects are being collected ▪ A choice of file formats may be available. That deposited may not be most suitable for preservation ▪ Storage media may be of unknown quality and suitability for long-term preservation ▪ Formats may be obsolete or not supported | <ul style="list-style-type: none"> ▪ Clearly defined priorities for both short and long-term preservation ▪ Ability to address issues such as encryption, proprietary software etc in received items ▪ Ability to ensure future access to information contained in the item |
|---|---|--|

Appendix 3 Bibliography and Sources

Digital Preservation Coalition, Handbook on Digital Preservation. Available at <http://www.dpconline.org/graphics/digpres/index.html>.

Lavoie, Brian and Richard Gartner, Technology Watch Report: Preservation Metadata, published by Digital Preservation Coalition. Available at: <http://www.dpconline.org/docs/reports/dpctw05-01.pdf>.

Council on Library and Information Resources, Report 92, “Authenticity in a Digital Environment,” May 2000. Available at <http://www.clir.org/pubs/reports/strategies.html>.

National Library of Australia, Preserving Access to Digital Information (PADI) Initiative, “Digital Preservation Strategies.” Available at <http://www.nla.gov.au/padi/topics/18.html>.

The National Archives, United Kingdom, “Sustainable Electronic Records, Strategies for Maintenance and Preservation of Electronic Records and Documents in the Transition to 2004,” Version 1.0, August 2001. Available at http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/preservation_toolkit.pdf

Digital Curation Centre (DCC), Digital Curation Manual. Available at <http://www.dcc.ac.uk/resource/curation-manual/>.

International Council on Archives, Electronic Records: A Workbook for Archivists (ICA Study 16) , 2005. Available at www.ica.org.

Preservation Metadata Implementation Strategies Working Group (PREMIS), Final Report, May 2005. Available at www.oclc.org/research/projects/pmwg/premis-final.pdf.

Recommended Data Formats for Preservation Purposes in the Florida Center for Library Automation Digital Archive. Available at:
<http://www.fcla.edu/digitalArchive/pdfs/recFormats.pdf>